Rutery. Wstęp teoretyczny, praktyczne aspekty konfiguracji, instrukcja do laboratorium.

Autor: Piotr Piskor IVFDS

STRESZCZENIE

Niniejsze opracowanie ma na celu zapoznanie z budową, funkcjonowaniem i konfiguracją podstawowych funkcji udostępnianych przez rutery Cisco.
Przedstawione tu zostały także zagadnienia związane z przeznaczeniem poszczególnych interfejsów rutera, sposobem podłączenia terminala i metodami konfiguracji urządzenia. Opracowanie zawiera opis sposobu pracy z interfejsem udostępnianym przez oprogramowanie IOS rutera, omówienie ważniejszych poleceń konfiguracyjnych oraz poleceń diagnostycznych, pozwalających sprawdzać status rutera. W rozdziałach dotyczących rutingu przedstawione zostały sposoby realizacji różnych metod rutowania, na przykładzie konkretnej sieci. Ostatni rozdział zawiera zestaw przykładowych tematów, które mogą służyć jako materiał do realizacji w laboratorium.

SPIS TREŚCI

1. WSTĘP TEORETYCZNY

1.1 Definicja rutera

Router to urządzenie, które kieruje ruchem pakietów w sieci na podstawie informacji warstwy trzeciej modelu ISO/OSI. Posługując się w tym celu protokołami tras, buduje tablice określające trasę, którą powinien przebyć pakiet, aby dotrzeć do celu.
Mosty lub przełączniki łączą dwie lub więcej fizycznych sieci w jedną sieć logiczną, podczas gdy ruter łączy sieci logiczne i wyznacza trasę między nimi, wykorzystując informacje zgromadzone przez protokoły tras w tablicach rutingu.[2]

1.2 Budowa rutera [1]

Najważniejsze elementy jakie można wyróżnić w budowie rutera, to:

- Jednostka centralna
- Blok pamięci – zawiera pamięć operacyjną RAM i DRAM. Służy ona do przechowywania tablic rutingu, kopii systemu operacyjnego, realizacji pamięci tymczasowej. Jest ona również wykorzystywana jako pamięć podręczna ARP. Zawartość tej pamięci ulega skasowaniu po wyłączeniu lub restarcie rutera.

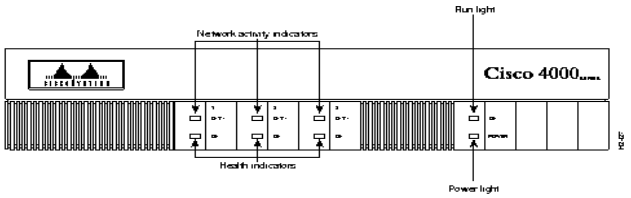
  Pamięć nie ulotna NVRAM przechowuje pliki konfiguracyjne.

  Pamięć nie ulotna Flash – przechowuje kod systemu operacyjnego. Można w niej przechowywać wiele kopii oprogramowania Cisco IOS oraz kopie procedur uruchomieniowych.

  W pamięci ROM zawarte są procedury diagnostyczne, programy rozruchowe i oprogramowanie systemu operacyjnego. Po włączeniu rutera, z pamięci ROM wykonywany jest program uruchomieniowy. Wykonuje on różnego rodzaju testy i wczytuje do pamięci RAM oprogramowanie Cisco IOS
- Wewnętrzne magistrale
- Grupa interfejsów sieciowych – do nich podłączane są inne urządzenia sieciowe. Mogą to być interfejsy: szeregowe, synchroniczne, asynchroniczne, Ethernet, ATM.

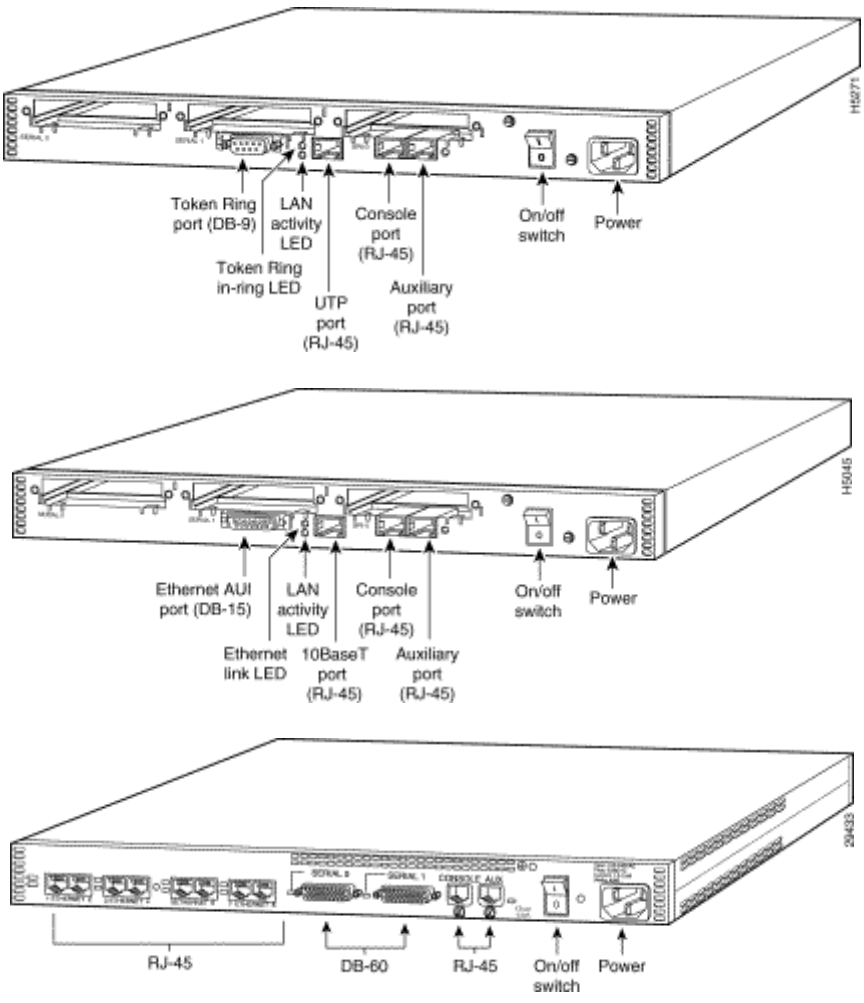
2. INSTALACJA I KOMUNIKACJA Z RUTEREM

Po włączeniu rutera rozpoczyna on swoje działanie sygnalizując to odpowiednimi diodami stanu, dostępnymi na panelu czołowym lub umieszczonymi na ściance tylnej (np. rutery serii 2500).[3]
Ścianka czołowa rutera zwykle nie zawiera niczego więcej poza elementami sygnalizacyjnymi i wyłącznikiem zasilania.



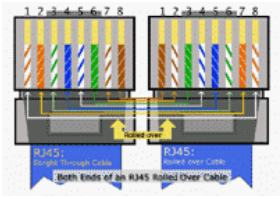
Rys 2.1 Wygląd ścianki czołowej rutera[3]

Ścianka tylna urządzenia posiada interfejsy sieciowe, interfejsy do komunikacji z terminalem, gniazdko zasilania, a także w przypadku większości obecnie oferowanych przez Cisco ruterów, elementy sygnalizacyjne i wyłącznik zasilania. Interfejsy sieciowe mogą być zrealizowane w postaci gniazdek RJ-45, pozwalając w ten sposób na bezpośrednie przyłączenie kabla skrętkowego, zakończonego wtykiem RJ45. Nie jest to jednak jedyny typ interfejsu. Oprócz RJ-45 stosowane są gniazda DB9, DB15 i DB60 (zwykle są dwa porty DB60 opisane jako S*erial* i *Serial2*). Aby w przypadku takich gniazdek można stosować wtyki RJ-45 dostępne są odpowiednie przejściówki, np. DB60 –RJ45.[3] Na rysunkach poniżej przedstawione zostały ścianki tylne różnych typów ruterów, wyposażone w różne rodzaje interfejsów:



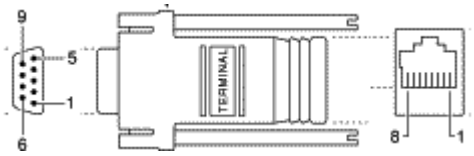
Rys 2.2 Wygląd ścianek tylnych w różnych typach ruterów [3]

Wszystkie rutery Cisco wyposażone są w porty konsoli, umożliwiające dostęp do rutera za pomocą terminala. Zwykle są to porty RJ-45 lub RS232, oznaczane jako *„Console”, „Aux” lub „Auxiliary Port”*. Do portu konsoli przyłącza się dedykowany terminal lub komputer osobisty wyposażony w emulator terminala[2].
Podłączenie terminala za pośrednictwem portu RJ-45 wymaga specjalnego rodzaju kabla, określanego jako *rollover cable*. Kabel taki ma odwróconą kolejność przewodów, tak jak pokazano to poniżej:

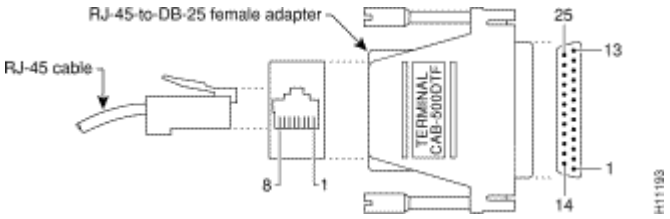


Rys 2.3 Kabel *rollover* [3]

Jeśli połączenie z komputerem odbywa się przez port szeregowy, zwykle wymagana jest specjalna przejściówka. Dostępne są dwa rodzaje takich przejściówek: *DB-9* oraz *DB-25*.[2]
Obydwa rodzaje pokazano na rysunkach poniżej:

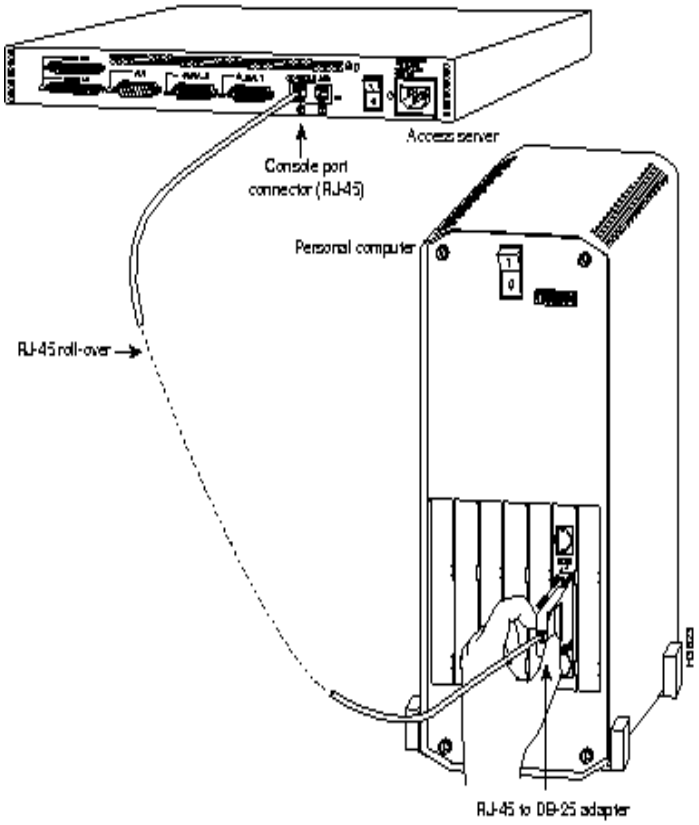


Rys 2.4 Przejściówka DB9-RJ45 [3]



Rys 2.5 Przejściówka DB25-RJ45 [3]

Sposób przyłączenia konsoli (w tym przypadku jest to komputer osobisty z zainstalowanym programem emulującym terminal) za pośrednictwem *RJ-45* pokazany został poniżej:



Rys 2.6 Podłączenie konsoli [3]

Do komunikacji z ruterem można użyć programu *Hyper terminal*. Należy zwrócić uwagę na poprawne ustawienie parametrów komunikacyjnych. Domyślnie są one następujące:

- emulacja VT100
- 9600 bodów
- brak kontroli parzystości
- 8b danych
- 1b stopu

Po ustawieniu parametrów komunikacyjnych można włączyć ruter. Jeśli wszystko jest w porządku, na ekranie terminala powinny zostać wyświetlone informacje generowane przez ruter i wyświetlony powinien zostać znak zachęty *Router*>.[2]

3. WYBRANE ASPEKTY KONFIGURACJI RUTERA

3.1 Tryby pracy rutera [1]

Ruter może pracować w kilku trybach. Różnią się one listą dostępnych poleceń konfiguracyjnych . Poniżej przedstawione zostały tryby pracy rutera wraz z opisem udostępnianych możliwości:

- Tryb użytkownika EXEC – umożliwia przeglądanie informacji dotyczących rutera, bez możliwości ich zmiany. Znak zachęty w tym trybie ma postać: *Router>*
- Tryb uprzywilejowany EXEC – obejmuje polecenia wykrywania błędów i testowania pracy rutera, modyfikowania plików konfiguracyjnych i dostęp do trybu konfiguracji. Znak zachęty w tym trybie ma postać: *Router#*
- Tryb konfiguracji – ma postać dialogu umożliwiającego nowemu użytkownikowi wprowadzanie z konsoli parametrów początkowej konfiguracji rutera.
- Tryb globalnej konfiguracji – umożliwia wykonywanie prostych zadań konfiguracyjnych. Znak zachęty w tym trybie: *Router(config)#*
- Inne tryby konfiguracji – pozwalają na wykonywanie bardziej złożonych zadań konfiguracyjnych, złożonych z wielu wierszy poleceń. Tryby te używają znaku zachęty *Router(config-mode)#*

Często tryb uprzywilejowany jest chroniony hasłem. Przełączenie do trybu uprzywilejowanego odbywa się za pomocą komend:

Router> enable
*Password: *******
Router #

Powrót do trybu nieuprzywilejowanego można wykonać za pomocą polecenia:

Router# exit

3.2 Sposoby konfiguracji rutera [1] [2]

Ruter można konfigurować na kilka sposobów. Każdy z nich wymaga jednak wcześniejszego przejścia w tryb uprzywilejowany, a następnie użycia polecenia *configure*. Polecenie *configure* można wywoływać z trzema opcjami:

- *configure termial* lub *conf term* – konfiguracja za pomocą terminala przyłączonego do routera
- *configure memory* – wczytuje konfigurację z pamięci NVRAM
- *copy tftp running-config* – wczytuje informacje konfiguracyjne z pliku przechowywanego na serwerze TFTP. Po wpisaniu polecenia *copy tftp running-config* należy podać IP hosta, z którego ma zostać pobrany plik konfiguracyjny. Następnie podaje się nazwę pliku i akceptuje wprowadzone zmiany.

Bieżąca konfiguracja (*ang. running config*) przechowywana jest w pamięci RAM, która jest wymazywana po wyłączeniu zasilania lub restarcie. Aktualną konfigurację da się jednak zapisać w pamięci NVRAM, gdzie zyska ona status konfiguracji startowej (*ang. startup config*). Do zapisu bieżącej konfiguracji w pamięci NVRAM służy polecenie:

copy running-config startup-config

Jeśli wprowadzimy błędne ustawienia, to zawsze istnieje możliwość naprawienia takiej sytuacji poprzez odtworzenie konfiguracji startowej. Odbywa się to przez skopiowanie konfiguracji startowej do konfiguracji bieżącej poleceniem:

copy startup-config running-config

Bieżącą konfigurację rutera można także skopiować do pliku na serwerze TFTP wykonując następujące operacje:

- copy running-config tftp
- Podać adres IP komputera na którym ma być przechowywany plik konfiguracyjny
- Podać nazwę pliku
- Potwierdzić wprowadzone zmiany wybierając opcję *yes*.

Do wymazania konfiguracji startowej służy polecenie:

erase startup-config

3.3 Interfejs użytkownika [1]

Rutery posiadają wbudowane oprogramowanie IOS, które pełni rolę systemu operacyjnego. IOS udostępnia listę poleceń, za pomocą których użytkownik podłączony za pośrednictwem konsoli komunikuje się z ruterem.
Zakres dostępnych poleceń jest różny w zależności od trybu pracy rutera. Napisanie znaku ? powoduje wyświetlenie listy dostępnych poleceń.
Interfejs użytkownika pomaga również w usuwaniu błędów, przez umieszczenie znaku ^ w miejscu gdzie wprowadzony był błędny symbol.
Interfejs użytkownika zawiera ponadto zaawansowany tryb edycji, udostępniający podstawowe funkcje edycji. Jest on automatycznie dostępny w obecnych wersjach oprogramowania. Tryb zaawansowanej edycji może zostać wyłączony, co jest przydatne w sytuacji kiedy mamy skrypty startowe nie działające prawidłowo w zaawansowanym trybie edycji. Ważniejsze polecenia edycyjne zostały przedstawione poniżej:

Ctrl + A – przejście na początek wiersza poleceń
Ctrl + E – przejście na koniec wiersza poleceń
Esc + B - jedno słowo do tyłu
Ctrl + F - jeden znak do przodu
Ctrl + B - jeden znak do tyłu
Esc + F - jedno słowo do przodu

Interfejs użytkownika pozwala na przeglądanie historii poleceń za pomocą klawiszy:

Ctrl + *P* lub strzałka w dół – przywołanie kilku ostatnich poleceń
show history – wyświetla zawartość bufora poleceń
no terminal editing – wyłącza zaawansowane funkcje edycji
terminal editing - włącza zaawansowane funkcje edycji

3.4 Polecenia sprawdzające status rutera

Polecenia te pozwalają sprawdzić bieżący status rutera i usunąć problemy związane z jego funkcjonowaniem . Poniżej zebrane zostały ważniejsze polecenia sprawdzające[1]:

- *show version* - wyświetla konfigurację sprzętową systemu, wersję oprogramowania, nazwy i pochodzenie plików konfiguracyjnych, obrazy procedur startowych oraz przyczynę ostatniego restartowania systemu.
- *show process* – wyświetla informacje o aktywnych procesach
- *show protocols* – wyświetla skonfigurowane protokoły, dla każdego protokołu w warstwie sieci.
- *show memory* – wyświetla informacje o pamięci rutera, w tym o wolnej pamięci.
- *show stack* – monitoruje wykorzystanie stosu przez procesy i procedury przerwań.
- *show buffers* – informacje o buforach rutera
- *show flash* – informacje o pamięci Flash rutera
- *show running-config* – wyświetla zawartość aktywnego pliku konfiguracyjnego(konfiguracja aktualnie działająca)
- *show run* – jak wyżej
- *show config* – konfiguracja zapisana w NVRAM
- *show conf* - jak wyżej
- *show startup-config* – jak wyżej
- *show interfaces* – informacje o wszystkich interfejsach skonfigurowanych w ruterze. Polecenia tego należy używać w trybie nieuprzywilejowanym.

3.5 Konfiguracja interfejsów rutera

Każdy interfejs w urządzeniach Cisco nazywany jest portem. Porty zwykle oznaczane są kolejno bez podawania gniazda. Np. w ruterze 2500 mającym jeden interfejs ethernet i dwa interfejsy szeregowe, są one oznaczane jako *ethernet0*, *serial0* i *serial1*. Jeśli urządzenie ma budowę modułową i wymienne karty interfejsów, wówczas interfejsy określane są według składni gniazdo/port. Np. interfejs znajdujący się w gnieździe 1 i porcie 2 jest oznaczany jako *ethernet1/2*.[2]
Do konfiguracji interfejsów służy polecenie *interface*, po którym należy podać numer portu. Polecenie to służy do konfiguracji wszystkich portów rutera (Ethernet, Token Ring, interfejsów szeregowych, itd.). Dla przykładu, parametry portu szeregowego można ustawić za pomocą poleceń [2]:

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0
Router(config-if)#clock rate 56000
Router(config-if)#end
```

Stan interfejsów można sprawdzić za pomocą komendy:

```
Router# show interfaces
```

3.5.1 Włączanie i wyłączanie interfejsów

Interfejsy można włączać i wyłączać z poziomu administratora, odpowiednio za pomocą poleceń [1]:

```
Router(config-if)# shutdown
Router(config-if)# no shutdown
```

3.5.2 Przypisywanie adresów IP [1] [2]

Do przypisania adresów IP do interfejsów rutera służy polecenie

```
Router(config-if)# ip address adres maska
```

Maska podsieci może być podana w trzech notacjach: bitowej, dziesiętnej z kropką oraz heksadecymalnej. Przykład poniżej pokazuje sposób konfiguracji adresu IP dla interfejsu eth0:

```
Router> en
Router# conf term
Router(config)# int eth0
Router(config-if)# ip address 192.168.20.1 255.255.255.0
```

Po dokonaniu zmian w ustawieniach interfejsu zawsze warto sprawdzić jego ustawienia za pomocą komendy:

```
Router> sh interface eth0
```

```
Ethernet0 is administratively down, line protocol is down
  Hardware is Lance, address is 000C.9240.1316 (bia 000C.9240.1316)
  Internet address is 192.168.20.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of show interface counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 2 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, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Rys 3.5.2.1 Wygląd ekranu terminala po wykonaniu polecenia sh interface eth0

Jak widać interfejs posiada adres IP dokładnie taki jaki został podany, ale jest wyłączony (świadczy o tym pierwsza linia).
Włączamy więc ten interfejs za pomocą komendy:

Router# conf term
Router(config)# int eth0
Router(config-if)# no shutdown

Sprawdzamy ponownie stan interfejsu poleceniem *sh interface eth0*. W pierwszej linii wyświetlanego raportu powinna teraz pojawić się informacja:

```
Ethernet0 is up, line protocol is up
```

Bardziej zwięzły opis interfejsów rutera można uzyskać za pomocą komendy

show ip interface brief

```
Interface              IP-Address      OK? Method Status                Protoco
Serial0                unassigned      YES unset  administratively down down
Serial1                unassigned      YES unset  administratively down down
Ethernet0              192.168.0.2     YES unset  up                    up
Ethernet1              192.168.2.1     YES unset  up                    up
```

Rys 3.5.2.2 Wygląd ekranu terminala po wykonaniu polecenia show ip interface brief

Istnieje możliwość dołączania krótkich opisów do interfejsu, mogących krótko charakteryzować, do czego dany interfejs służy. Wykorzystuje się w tym celu polecenie *description*. Sposób jego użycia pokazany został w przykładzie poniżej:

```
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int e0
Router(config-if)#description Podlaczenie do routera nr1
Router(config-if)#end
Router#
```

3.6 Podstawowe informacje o konfiguracji rutingu

Jedną z podstawowych funkcji protokołu IP jest rutowanie. Umożliwia ono przesyłanie datagramów poprzez wiele sieci do miejsca przeznaczenia. Rutowanie polega więc na ustaleniu ścieżki połączeń między kolejnymi ruterami, do miejsca przeznaczenia pakietu.[2]
Jeśli urządzenie sieciowe ma wysłać pakiet do innego urządzenia sieciowego, wówczas mogą zajść następujące przypadki [4]:

- Węzeł sieci, do którego skierowany jest pakiet, jest albo bezpośrednio połączony z urządzeniem sieciowym mającym wysłać ten pakiet, albo znajduje się w tej samej sieci co wspomniane urządzenie sieciowe. W obu tych sytuacjach pakiet może być bezpośrednio przesłany do węzła docelowego.
- Węzeł sieci, do którego skierowany jest pakiet, nie znajduje się w tej samej sieci/podsieci co urządzenie sieciowe mające wysyłać pakiety. W tej sytuacji urządzenie powinno podjąć decyzję o wyborze adresu urządzenia sieciowego, które przejmie odpowiedzialność za dalsze przesłanie pakietu.

Jeśli urządzeniem sieciowym wysyłającym pakiet jest, np. komputer, to w sytuacji drugiej pakiet wysyłany jest do najbliższego rutera, którego adres określony jest w konfiguracji interfejsu sieciowego tego komputera jako gateway. Jeśli natomiast urządzeniem tym jest ruter, to musi on podjąć decyzję o dalszej drodze pakietu na podstawie posiadanych przez siebie informacji. Informacje te w ruterze zawarte są w tablicy rutowania [4].

Do włączenia rutingu IP używa się globalnego polecenia konfiguracyjnego *ip routing*.
Ruter domyślnie jest skonfigurowany do obsługi rutingu IP. Jeśli jednak z jakichś powodów ruting nie jest domyślnie uaktywniony, wówczas można go włączyć poleceniem [2]:

```
Router> en
Router# conf term
Router(config)# ip routing
```

Po włączeniu rutingu można zbudować tablicę rutowania. Domyślnie kiedy interfejs ma przypisany adres IP i jest włączony, jego adres sieciowy jest umieszczany w tablicy rutingu.

W przypadku rutingu statycznego informacja o trasach zapisywana jest przez administratora w tablicy rutowania. Ruting statyczny jest prostym i nie obciążającym dodatkowo sieci sposobem konfiguracji ruterów.
Ruter skonfigurowany statycznie jest pasywny – nie komunikuje się z innymi ruterami w celu uzyskania informacji o dostępnych odległych sieciach lub bieżącym stanie już znanych mu tras. Wpisywanie ręczne tras jest uciążliwe przy dużych rozmiarach sieci. Rutery statyczne nie rekonfigurują się w przypadku awarii łącza. Wszelkie zmiany topologii sieci administrator musi nanieść ręcznie. W przypadku rutowania statycznego zawsze znana jest droga jaką pakiet podąża do celu. Rutowanie statyczne nie umożliwia wykorzystania połączeń zapasowych [4].

Nowe informacje do tablicy rutowania wprowadza się podkomendą:

ip route adres_ sieci adres_interfejsu
gdzie:

adres_sieci - jest adresem IP docelowej sieci
adres_interfejsu - jest adresem interfejsu rutera znajdującego się na ścieżce prowadzącej do sieci docelowej; interfejs ten należy do sieci mającej styczność z konfigurowanym ruterem.

Informacja o adresie docelowym może przybrać następujące formy[4]:

- konkretny adres IP następnego rutera na trasie
- adres sieci dla innej trasy w tablicy rutowania, do której należy przekazać pakiet
- bezpośrednio przyłączony interfejs, umieszczony w sieci przeznaczenia

Informację można usunąć z tablicy rutowania podkomendą:

no ip route adres_ sieci adres_ interfejsu

Zawartość tablicy rutowania można sprawdzić poleceniem:

s*how ip route*

Zawartość tej tablicy może być następująca:

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, * - candidate default*
U - per-user static route, o - ODR
Gateway of last resort is 212.182.58.1 to network 0.0.0.0

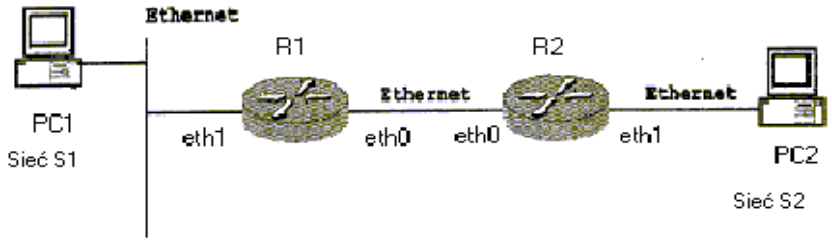
192.168.1.0/29 is subnetted, 1 subnets
C 192.168.1.0 is directly connected, Ethernet5
192.168.2.0/27 is subnetted, 1 subnets
C 192.168.2.0 is directly connected, ATM0.3
S 0.0.0.0/0 [1/0] via 212.182.58.1*

Pierwsza część poleceń zwróconych przez komendę *show ip route*, to legenda skrótów określających między innymi skąd została wyprowadzona trasa. Ostatnia część wyniku to sama tablica routingu. Należy zwrócić uwagę, że w tej tablicy podane są adresy sieci i podsieci, a nie adresy IP pojedynczych urządzeń[2].

Gateway of last resortI (tzw. brama ostatniej szansy) oznacza sieciowy adres rutera, do którego powinny być kierowane pakiety zmierzające na zewnątrz sieci, jeśli nie ma szczegółowych informacji, w jaki sposób można osiągnąć miejsce przeznaczenia[4].

3.7 Konfiguracja rutingu statycznego [4]

Dla schematu połączeń przedstawionego poniżej, należy skonfigurować adresy IP interfejsów urządzeń zgodnie z podanymi wartościami. Następnie należy tak skonfigurować rutery, aby zapewnić możliwość komunikacji pomiędzy obiema sieciami, stosując ruting statyczny.



Router R1:

eth0 :	192.168.0.1	255.255.255.0
eth1 :	212.182.41.1	255.255.255.0

Router R2:

eth0 :	192.168.0.2	255.255.255.0
eth1 :	192.168.2.1	255.255.255.0
PC1 :	212.182.41.6	255.255.255.0
PC2 :	192.168.2.2	255.255.255.0

Rys 3.7.1 Topologia sieci na przykładzie której pokazano sposób konfiguracji rutingu statycznego [4]

Konfiguracja interfejsów rutera R1:

Router> en
Router# conf term
Router(config)# int eth0
Router(config-if)# ip address 192.168.0.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# int eth1
Router(config-if)# ip address 212.182.41.1 255.255.255.0
Router(config-if)# no shutdown

Za pomocą polecenia *sh int eth0* sprawdzamy czy wartości zwrócone w wyniku są zgodne z wprowadzonymi ustawieniami. Jeśli tak przechodzimy do konfiguracji rutera R2.

Konfiguracja interfejsów rutera R2:

Router> en
Router# conf term
Router(config)# int eth0
Router(config-if)# ip address 192.168.0.2 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# int eth1
Router(config-if)# ip address 192.168.2.1 255.255.255.0
Router(config-if)# no shutdown

Ruter R1 ma za zadanie kierować pakiety zaadresowane do sieci 212.182.41.0 na port o adresie 192.168.0.1, który przejmuje odpowiedzialność za przetransportowanie ich do miejsca docelowego. Tablicę rutingu rutera R1 wypełniamy w sposób pokazany poniżej, a następnie sprawdzamy tablicę rutingu:

Router> en
Router# conf term
Router# ip route 192.168.2.0 255.255.255.0 192.168.0.1
Router(config-if)# 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
       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, * - candidate default
       U - per-user static route

Gateway of last resort is not set
C       192.168.0.0/24 is directly connected, 192.168.0.1
C       212.182.41.0/24 is directly connected, 212.182.41.1
S       192.168.2.0/24 [1/0] via 192.168.0.1
```

Rys 3.7.2 Zawartość tablicy rutingu rutera R1

W analogiczny sposób postępujemy z ruterem R2.Router R2 ma za zadanie kierować pakiety zaadresowane do sieci 192.168.2.0 na port o adresie 192.168.0.2, który dalej przesyła je we właściwym kierunku.

Router> en
Router# conf term
Router# ip route 212.182.41.0 255.255.255.0 192.168.0.2
Router(config-if)# sh ip route

Po wyświetleniu tablicy rutingu powinna ona mieć zawartość pokazaną poniżej:

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       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, * - candidate default
       U - per-user static route

Gateway of last resort is not set
C       192.168.0.0/24 is directly connected, 192.168.0.2
C       192.168.2.0/24 is directly connected, 192.168.2.1
S       212.182.41.0/24 [1/0] via 192.168.0.2
```

Rys 3.7.3 Zawartość tablicy rutingu rutera R2

Komputery w sieci S1 powinny mieć przypisaną bramkę domyślną(*default gateway*) o adresie 212.182.41.1. W sieci S2 bramka domyślna to 192.168.2.1.

3.8 Konfiguracja rutingu dynamicznego w oparciu o protokół RIP [4]

Protokół RIP, to protokół wektora odległości, który jako metryki używa licznika skoków między ruterami. Maksymalna liczba skoków w RIP wynosi 15. Każda dłuższa trasa oznaczana jest jako nieosiągalna, poprzez ustawienie licznika skoków na wartość 16. Informacje w protokole RIP przekazywane są z rutera do sąsiednich ruterów przez rozgłaszanie IP, z wykorzystaniem UDP i portu 520. Rozgłaszanie to odbywa się średnio co 30 s.

Do konfiguracji rutingu dynamicznego służą dwa polecenia:

router protokół – definiuje protokół rutingu
network numer-sieci – adresy sieci, z którymi jest bezpośrednio połączony ruter. Informacje te będą rozsyłane w sieci do sąsiednich ruterów.

Wyłączenie rutingu dynamicznego można wykonać za pomocą komendy

Router(config)# no router rip

Domyślnie uruchamiany jest protokół RIP ver. 1.
Za pomocą polecenia

version nr-wersji

można wskazać, która wersja protokołu ma zostać uruchomiona. Parametr *nr-wersji* przyjmuje wartość 1 lub 2.

Poniżej opisany został sposób konfiguracji sieci o topologii takiej jak na rysunku 3.7.1 w oparciu o protokół RIP.
Po przypisaniu adresów do interfejsów w obu ruterach, można przejść do konfiguracji rutingu. W tym celu należy przejść do trybu uprzywilejowanego i wpisać w linii poleceń terminali podłączonych do ruterów R1 i R2, odpowiednio polecenia:

Router> en
Router# conf term
Router(config)# router rip
Router(config-if)# network 212.182.41.0
Router(config-if)# network 192.168.0.0

Po sprawdzeniu tablicy rutingu poleceniem:

Router> sh ip route

powinna ona zawierać:

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       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, * - candidate default
       U - per-user static route

Gateway of last resort is not set
C       192.168.0.0/24 is directly connected, 192.168.0.1
C       212.182.41.0/24 is directly connected, 212.182.41.1
R       192.168.2.0/24 [120/1] via 192.168.0.2, 00:05:35, Ethernet0
```

Rys 3.8.1 Tablica rutingu rutera R1

Podobnie należy postępować w przypadku rutera R2:

Router> en
Router# conf term
Router(config)# router rip
Router(config-if)# network 192.162.2.0

Router(config-if)# network 192.168.0.0
Router> 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
       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, * - candidate default
       U - per-user static route

Gateway of last resort is not set
C       192.168.0.0/24 is directly connected, 192.168.0.2
C       192.168.2.0/24 is directly connected, 192.168.2.1
R       212.182.41.0/24 [120/1] via 192.168.0.1, 00:04:35, Ethernet0
```

Rys 3.8.2 Tablica rutingu rutera R2

W tablicach rutingu obu ruterów znajdują się m.in. następujące wpisy:

R 192.168.2.0/24 [120/1] via 192.168.0.2, 00:05:35, Ethernet0
R 212.182.41.0/24 [120/1] via 192.168.0.1, 00:04:35, Ethernet0

Wpisy te oznaczają, że tablica rutowania została uaktualniona na podstawie informacji rozsyłanych przez protokół RIP (oznacza to litera R na początku).
Do tablicy rutingu dodana została sieć i adres portu rutera, przez który można się do niej dostać. Wpis ten zawiera także czas (w sekundach), przez który trasa była w tablicy lub który upłynął od ostatniej aktualizacji. Dla wszystkich tras, poza bezpośrednio połączonymi, wypisywana jest w nawiasie kwadratowym odległość administracyjna i metryka protokołu.

Bardziej szczegółowe informacje o rozsyłanych i otrzymywanych uaktualnieniach, wartości metryk i ilości skoków potrzebnych na osiągnięcie sieci docelowej udostępnia polecenie

Router# debug ip rip

Informacje te są średnio co 30 s wypisywane na ekranie terminala podłączonego do rutera.
Wyłączenie trybu *debug ip route* jest możliwe za pomocą polecenia

Router# no debug ip rip

3.9 Konfiguracja rutingu dynamicznego w oparciu o protokół IGRP[4]

IGRP został opracowany w połowie lat 80-tych przez firmę CISCO. IGRP jest protokołem z wektorem odległości, w którym stosuje się metrykę bardziej zaawansowaną niż w RIP: 24-bitową wartość, obliczaną na podstawie pomiaru sumy opóźnień na trasie, przepustowości poszczególnych łączy, ich pewności i obciążenia. Dla homogenicznych łączy metryka ta redu-

kuje się do liczby przejść. Rutery wykonujące protokół IGRP rozgłaszają znane sobie trasy co 90 sekund. Jeśli ruter nie otrzyma od danego sąsiada pakietu IGRP przez trzy kolejne okresy (270 sekund), zaznacza obsługiwane przez niego trasy jako nieużyteczne. Po kolejnych siedmiu okresach ciszy (630 sekund) ruter usuwa te trasy ze swej tablicy. Ruter może wysłać pakiet IGRP z odświeżoną (poprawioną) zawartością wcześniej niż upłynie wyżej wymieniony interwał w przypadku zmiany trasy lub metryki[4][3].
Protokół IGRP uruchamia się za pomocą polecenia:

Router(config)# router igrp id-procesu

gdzie:

id-procesu oznacza liczbę całkowitą z zakresu 1- 65535. Ponieważ w tym samym ruterze może działać wiele procesów IGRP, identyfikator jest niezbędny do rozróżnienia ich.

Polecenie

Router(config)# network numer-sieci

definiuje sieci bezpośrednio połączone z ruterem.

Poniżej został opisany sposób konfiguracji urządzeń w sieci pokazanej na rysunku 3.7.1 z wykorzystaniem protokołu IGRP .
Po przypisaniu adresów do interfejsów w obu ruterach, przechodzimy do konfiguracji rutingu z wykorzystaniem IGRP. W tym celu należy przejść do trybu uprzywilejowanego i wpisać następujące polecenia dla ruterów R1 i R2:

Router> en
Router# conf term
Router(config)# routerigrp 110
Router(config-if)# network 212.182.41.0
Router(config-if)# network 192.168.0.0

Sprawdzamy tablicę rutingu:

Router> sh ip route

Jej zawartość powinna być taka sama, jak tablicy pokazanej poniżej:

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       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, * - candidate default
       U - per-user static route

Gateway of last resort is not set
C       192.168.0.0/24 is directly connected, 192.168.0.1
C       212.182.41.0/24 is directly connected, 212.182.41.1
I       192.168.2.0/24 [100/273] via 192.168.0.2, 00:07:28, Ethernet0
```

Rys 3.9.1 Tablica rutingu rutera R1

Podobnie dla rutera R2:

Router> en
Router# conf term
Router(config)# routeri9grp 120
Router(config-if)# network 192.162.2.0
Router(config-if)# network 192.168.0.0

Sprawdzamy tablicę rutingu:

Router> sh ip route

Jej zawartość powinna być taka sama jak tablicy na rysunku poniżej:

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       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, * - candidate default
       U - per-user static route

Gateway of last resort is not set
C       192.168.0.0/24 is directly connected, 192.168.0.1
C       212.182.41.0/24 is directly connected, 212.182.41.1
I       192.168.2.0/24 [100/273] via 192.168.0.2, 00:07:28, Ethernet0
```

Rys 3.9.2 Tablica rutingu rutera R2

Odpowiednie wpisy w obydwu tablicach rutingu poprzedzone literą “I” oznaczają, że te informacje zostały dodane za pomocą protokołu IGRP.
Za pomocą komendy

Router# sh ip protocols

można sprawdzić informacje o rutingu, a w przypadku IGRP wyświetlany jest także algorytm służący do wyznaczania metryki rutingu:

```
Routing Protocol is "igrp 110"
  Sending updates every 90 seconds, next due in 56 seconds
  Invalid after 270 seconds, hold down 280, flushed after 630
  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
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing: igrp 100
  Routing for Networks:
    192.168.2.0
    192.168.0.0
  Routing Information Sources:
    192.168.0.2           100      00:00:07
  Distance: (default is 100)
```

Rys 3.9.3 Informacje zwracane przez polecenie sh ip protocols

Rutery mogą korzystać tylko z jednego lub wielu różnych protokołów rutingu.

3.10 Konfiguracja trasy domyślnej [4]

Ruter może nie znać tras do wszystkich sieci. Aby zapewnić pełne możliwości rutingu wyznacza się niektóre rutery jako rutery domyślne, z których mogą korzystać pozostałe rutery w sieci. Jeśli adres docelowy nie istnieje w tablicy rutingu, wówczas pakiet jest kierowany do sieci domyślnej. Sieć ta musi istnieć w tablicy rutingu.
Do ustawienia trasy domyślnej służy polecenie *ip default –network.* Składnia tego polecenia jest następująca:

ip default-network numer-sieci

gdzie:

numer-sieci – określa adres sieci lub adres podsieci zdefiniowanej jako domyślna

3.11 Podstawowe informacje o konfiguracji list dostępowych [4]

Aby zapewnić właściwą ochronę sieci LAN przed próbami naruszenia ich poufności oraz odpowiedniego podziału na część chronioną oraz publiczną, stosuje się mechanizm filtracji pakietów transmitowanych przez rutery znajdujące się na styku struktur podlegających ochronie. Funkcje filtracji pakietów definiowane są za pomocą listy dostępu. Za ich pomocą ruter rozstrzyga czy pakiety docierające do sieci publicznej poprzez wskazany interfejs mogą być przekazane do innych urządzeń dołączonych do sieci.

Pojęcie list dostępu związane jest z interfejsem sieciowym, w związku z tym trzeba zadbać, aby każdy z interfejsów, dla którego należy zastosować kontrolę dostępu, miał skonfigurowany odpowiedni ich zestaw. W związku z tym, że kontrola transmisji opiera się na innych parametrach podczas analizy ruchu przychodzącego i wychodzącego, dlatego stosuje się osobne zestawy list dostępu dla obydwu kierunków transmisji.[4][2]

Filtrowanie pakietów udostępniane przez IOS umożliwia ograniczenie przepływu pakietów na podstawie następujących kryteriów:

- Źródłowe adresy IP
- Adres źródłowy i docelowy IP
- Rodzaje protokołów IP, w tym TCP, UDP, ICMP
- Źródłowe i docelowe usługi protokołu TCP (np. Telnet)
- Źródłowe i docelowe usługi protokołu UDP
- Usługi protokołu ICMP

Kryteria filtrowania definiowane w formie listy zawierają zezwolenia i zakazy. Każdy wiersz listy dostępowej porównywany jest z adresami IP i innymi informacjami zawartymi w pakiecie danych, aż do odnalezienia pasującego wiersza. Wówczas lista dalej nie jest przeszukiwana. Z tego powodu kolejność instrukcji na liście ma
zasadnicze znaczenie. Listy dostępowe dzielą się na dwie kategorie:

- **Listy proste** związane są z filtracją transmisji danych z/do określonego adresu sieciowego stosowanego w warstwie łącza danych lub sieci. Zazwyczaj istnieje również możliwość konstruowania list, które dotyczą logicznej grupy adresów, jaką stanowi np. sieć lub podsieć wynikająca z klasy adresacji.
  Składnia komendy definiującej proste listy dostępu jest następująca:

  access-list access-list-number {permit | deny} source [source mask]
  gdzie:
  access-list - komenda definiująca element dostępu
  access-list-number - numer listy z przedziału [1-99]
  permit - zezwolenie na transmisje przy spełnieniu danego warunku
  deny - zabronienie transmisji przy spełnieniu danego warunku
  source - adres, z którym jest porównywany adres źródłowy pakietu
  source-mask - opcjonalna maska określająca ważność bitów w trakcie porównania obserwowanego z adresem source wartość 1 oznacza, iż dany bit ma być zignorowany w trakcie porównania

- **Listy złożone** umożliwiają bardziej szczegółową specyfikację warunków filtracji pakietów opartą na analizie zawartości nagłówków pakietów warstwy łącza danych, sieci i transportu. Dzięki temu pozwalają one na szczegółowe określenie nie tylko adresu nadawcy oraz odbiorcy pakietów, ale także na wskazanie, która konkretnie usługa ma podlegać filtracji.
  Składnia komendy definiującej rozszerzone listy dostępu jest następująca:

  access-list access-list-number protocol {permit | deny} source
  [source mask] destination-address [destination mask]
  [operator operand]

gdzie:

access-list - komenda definiująca element listy dostępu
access-list-number - numer listy z przedziału [100-199]
permit - zezwolenie na transmisję przy spełnieniu danego warunku
deny - zabronienie transmisji przy spełnieniu danego warunku
protocol - protokół icmp, igmp, ip, nos, tcp, udp
source - adres, z którym jest porównywany adres źródłowy pakietu
source-mask - opcjonalna maska określająca ważność bitów w trakcie porównania obserwowanego z adresem source wartość 1 oznacza, iż dany bit ma być zignorowany w trakcie porównania
destination - jak wyżej dla dresu przeznaczenia
destination-mask - jak wyżej dla adresu przeznaczenia
operator - operator: lt, gt, eq, neq porównujący numer portu w pakiecie z wartością w polu operand
operand - liczba dziesiętna, z którą porównuje się numer portu

4. INSTRUKCJA DO LABORATORIUM

1. Zapoznać się z danymi technicznymi i możliwościami rutera dostępnego w laboratorium.
2. Zapoznać się z przeznaczeniem poszczególnych interfejsów urządzenia oraz funkcją elementów sygnalizacyjnych LED.
3. Zapoznać się ze sposobem konfiguracji rutera w trybie terminalowym.
4. Skonfigurować ruter za pomocą pliku pobranego z serwera TFTP.
5. Zapisać bieżącą konfigurację w pliku na serwerze TFTP.
6. Sprawdzić bieżącą i startową konfigurację rutera.
7. Sprawdzić aktualny stan interfejsów rutera.
8. Skonfigurować wybranym interfejsom adresy IP.
9. Zrealizować przykładową strukturę sieciową w oparciu o rutery i komputery PC, a następnie:
    a) uruchomić ruting statyczny. Sprawdzić tablicę rutingu oraz możliwość wzajemnej komunikacji pomiędzy podsieciami (np. za pomocą polecenia *ping)*
    b) Dokonać analizy trasy pakietów do wskazanego komputera (polecenia *traceroute, tracert*)
    c) Skonfigurować rutery do pracy z protokołami RIP i IGRP
    d) Ustawić trasę domyślną

5. LITERATURA

[1] Vito Amato, Wayne Lewis „Akademia Sieci Cisco – pierwszy rok nauki1“. Mikom Warszawa 2001

[2] A.Leinwand, B.Pinsky, M.Culpepper „ Konfiguracja routerów Cisco”. Mikom Warszawa 2000

[3] www.cisco.com

[4] Materiały do laboratorium „sieci komputerowe” – sem. 6