

**Tytuł pracy:** „Routing statyczny w sieci opartej o router Cisco i routery oparte na SO. Solaris”.

Autor: Łukasz Michalik IVFDS

**STRESZCZENIE :**

Tematem projektu jest konfiguracja przykładowej sieci , w której trzeba skonfigurować router Cisco oraz dwa komputery pełniące rolę routerów opartych na systemie operacyjnym Solaris.

W projekcie zawarte są podstawowe informacje dotyczące właściwości routerów, rodzajów algorytmów trasowania oraz protokołów trasowania. W szczególności opisany jest protokół routingu dynamicznego i statycznego. Opracowany jest krok po kroku schemat konfiguracji przykładowej sieci oraz opisane polecenia SO Solaris.

**SPIS TREŚCI:**

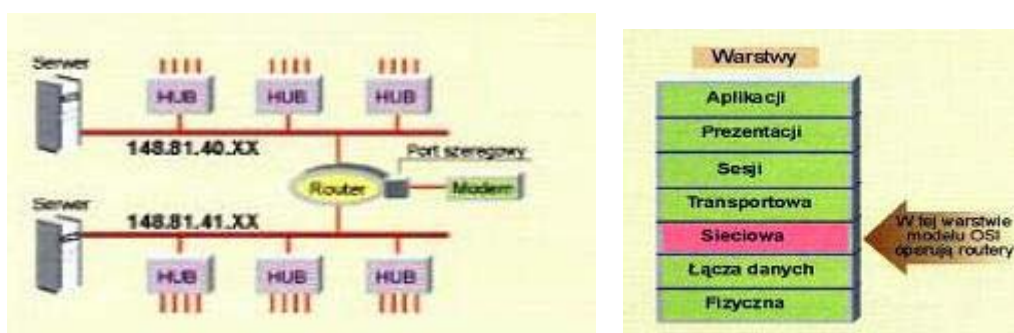
Streszczenie.....	2
1. Teoria routingu.....	4
1.1 Algorytmy trasowania.....	5
1.2 Protokoły trasowania.....	6
1.3 Routing dynamiczny.....	7
1.4 Routing statyczny.....	7
2. Konfiguracja przykładowej sieci.....	8
2.1 Konfiguracja routera Cisco z pliku konfiguracyjnego.....	9
2.2 Konfiguracja routerów w systemie Solaris.....	9
2.2.1 Nadanie nazwy komputerowi.....	9
2.2.2 Konfiguracja routera R1.....	9
2.2.3 Konfiguracja hosta jednej z podsieci.....	10
2.2.4 Konfiguracja routera R2.....	10
2.2.5 Ustawienie masek.....	11
3. Opis wykorzystywanych poleceń SO. Solaris.....	11
Literatura.....	12

## 1. TEORIA ROUTINGU:

Węzły sieci operujące w trzeciej (sieciowej) warstwie modelu OSI noszą nazwę **routerów**. Są to urządzenia wyposażone najczęściej w kilka interfejsów sieciowych LAN, porty obsługujące sieci WAN, pracujący wydajnie procesor i specjalne oprogramowanie zawiadujące ruchem pakietów przepływających przez router. Jak sama nazwa wskazuje (ang. *route to trasa*), routery wyznaczają pakietom marszruty, kierując je do odpowiedniego portu lub karty sieciowej. Chociaż routerem może też być zwykły komputer dysponujący kilkoma kartami sieciowymi i specjalnym oprogramowaniem, to jest to najczęściej dedykowany komputer, dysponujący rozwiązaniami znacznie zwiększającymi wydajność tego rodzaju węzłów sieci. Przez lata routing IP ewoluował od przekazywania pakietów obsługiwanego programowo, poprzez przekazywanie realizowane przez specjalizowane układy scalone (ASIC), dalej przekazywanie przez układy ASIC z szybkością danego interfejsu, aż do wprowadzania obecnie, przekazywania realizowanego przez procesory sieciowe z szybkością interfejsu.

Routery są stosowane zarówno w sieciach LAN, jak i WAN. W sieciach LAN (routery lokalne) są używane wtedy, gdy system informatyczny chcemy podzielić na dwie lub więcej podsieci, czyli poddać operacji segmentowania. Segmentacja sieci powoduje, że poszczególne podsieci są od siebie odseparowane i pakiety (zarówno Point-to-Point, jak i multicast czy broadcast) nie przenikają z jednej podsieci do drugiej. Korzyść jest oczywista: w ten sposób zwiększamy przepustowość każdej z podsieci.

Inną rolę pełnią **routery dostępne**, czyli sprzęgające sieć LAN ze światem zewnętrznym. W tym przypadku nie chodzi już o segmentację sieci LAN na mniejsze domeny rozgłoszeniową, ale o zainstalowanie węzła sieci ekspediującego przez łącze WAN pakiety generowane przez pracujące w sieci LAN stacje do innego routera pracującego po drugiej stronie tego łącza. Oczywiście, może się zdarzyć i tak, że jeden router obsługuje zarówno pakiety lokalne, jak i te kierowane na zewnątrz.



Rys 1.1 schemat sieci z routerem dostępowym [1]

1.2 warstwa sieciowa na której pracuje router [1]

Routery nie interesują się adresami MAC (w przypadku sieci Ethernet jest to 48-bitowa liczba przypisywana każdej karcie sieciowej), a po odebraniu pakietu odczytują i poddają analizie adres budowany w obszarze warstwy sieciowej

W sieciach Internet będzie do adresu IP przypisywany przez administratora każdemu ze stanowisk pracy. Adres taki składa się zawsze z dwóch części: jedna definiuje adres sieci, a druga adres komputera pracującego w tej sieci, i tak np. numer 148.81.40.10 oznacza (zakładając, że administrator zdefiniował dodatkowo maskę podsieci 255.255.255.0), że stacja docelowa jest zainstalowana w sieci 148.81.40, a jej numer to 10. Ponieważ routery służą do sprzęgania różnych sieci komputerowych (czyli takich, którym przypisano inne adresy definiujące numer sieci), to do routera zostaną wysłane tylko te pakiety, które są kierowane do innych sieci. Żaden pakiet wysłany przez stację 148.81.40.X do stacji 148.81.40.X nie trafi do routera, ponieważ stacja docelowa pracuje w tej samej sieci, a nie na zewnątrz.

Routery zakładają tabele routingu i mają zdolność „uczenia się” topologii sieci, wymieniając informacje z innymi routerami zainstalowanymi w sieci. Ponieważ prawie wszystkie operacje związane z odbieraniem i ekspediowaniem pakietów do odpowiedniego portu są realizowane w routerze przez oprogramowanie, to tego rodzaju węzły sieci pracują dużo wolniej niż np. przełączniki.

Protokoły trasowania wyznaczają pakietom marszruty opierając się na różnych algorytmach. Mogą to być algorytmy statyczne lub dynamiczne, single path lub multi path, płaskie lub hierarchiczne, host intelligent lub router intelligent, intradomain lub interdomain i opierające się na technologii link state lub distance vector. [1]

## 1.1 Algorytmy trasowania

Algorytmy statyczne i dynamiczne. Algorytm statyczny nie jest właściwie algorytmem. Wszystkie drogi routingu wyznacza tu bowiem na stałe sam administrator systemu. Jeśli topologia sieci zmieni się, router jest po prostu bezsilny. Algorytmy dynamiczne natomiast śledzą cały czas topologię sieci (praca w czasie rzeczywistym) i modyfikują w razie potrzeby tabele routingu zakładane przez router.

Algorytmy single path i multi path. Niektóre protokoły trasowania wyznaczają pakietom kilka dróg dostępu do stacji przeznaczenia, czyli wspierają multipleksowanie. I tak jak algorytm single path definiuje tylko jedną ścieżkę dostępu do adresata, tak algorytm multi path pozwala przesyłać pakiety przez wiele niezależnych ścieżek, co nie tylko zwiększa szybkość transmisji pakietów, ale też chroni system routingu przed skutkami awarii.

Algorytmy płaskie i hierarchiczne. W tym pierwszym przypadku wszystkie routery są równorzędne. Można to porównać do sieci typu „peer-to-peer”. Nie ma tu (ze względu na strukturę logiczną) ważniejszych i mniej ważnych routerów czy też nadrzędnych lub podrzędnych. Algorytmy hierarchiczne postrzegają sieć jako strukturę zhierarchizowaną, dzieląc ją na domeny. Pakietami krążącymi w obrębie każdej domeny zawiaduje wtedy właściwy router, przekazując je routerowi nadrzędnemu lub podrzędnemu.

Algorytmy host intelligent i router intelligent. Niektóre algorytmy zakładają, że całą drogę pakietu do stacji przeznaczenia wyznaczy od razu stacja nadająca. Mamy wtedy do czynienia z trasowaniem źródłowym (source routing, czyli host intelligent). W tym układzie router pełni tylko rolę „przekaznika” odbierającego pakiet i ekspediującego go do następnego miejsca. W algorytmach router intelligent stacja wysyłająca nie ma pojęcia, jaką drogę przemierzy pakiet, zanim dotrze do adresata. Obowiązek wyznaczenia pakietowi marszruty spoczywa na routerach.

Algorytmy intradomain i interdomain. Algorytmy trasowania intradomain operują wyłącznie w obszarze konkretnej domeny, podczas gdy algorytmy interdomain zawiadują pakietami biorąc pod uwagę nie tylko zależności zachodzące w ramach konkretnej domeny, ale też powiązania między tą domeną i innymi, otaczającymi ją domenami. Optymalne marszruty wyznaczone przez algorytm intradomain nie muszą być (i najczęściej nie są) najlepsze, jeśli porównamy je z optymalnymi marszrutami wypracowanymi przez algorytm interdomain („widzący” całą strukturę sieci).

Algorytm link state i distance vektor. Algorytm link state (znany jako shortest path first) rozsyła informacje routingu do wszystkich węzłów obsługujących połączenia międzysieciowe. Każdy router wysyła jednak tylko tę część tabeli routingu, która opisuje stan jego własnych łączy. Algorytm distance vector (znany też pod nazwą Bellman-Ford) wysyła w sieć całą tabelę routingu, ale tylko do sąsiadujących z nim routerów. Mówiąc inaczej, algorytm link state rozsyła wszędzie, ale za to niewielkie, wybrane porcje informacji, podczas gdy distance vector rozsyła komplet informacji, ale tylko do najbliższych węzłów sieci. Każdy z algorytmów ma swoje wady i zalety. Link state jest skomplikowany i trudny do konfigurowania oraz wymaga obecności silniejszego procesora CPU. Odnotowuje za to szybciej wszelkie zmiany zachodzące w topologii sieci. Distance vector nie pracuje może tak stabilnie, ale jest za to łatwiejszy do implementowania i sprawuje się dobrze w dużych sieciach składających się z kilkudziesięciu czy nawet kilkuset routerów.

Po odebraniu pakietu i odczytaniu adresu IP stacji docelowej (sieć TCP/IP) router musi zawsze wyekspediować go na zewnątrz. Jeśli stacja docelowa jest zlokalizowana w innej sieci czy podsieci LAN dołączonej do routera, to sprawa jest prosta - router dołącza do takiego pakietu adres MAC tej stacji (pobierając go z tabeli ARP) i wysyła do określonej karty sieciowej. Jeśli jednak stacja docelowa znajduje się w zupełnie innej sieci LAN, to router musi go opakować w specjalną „kopertę” (czyli posłużyć się odpowiednim protokołem routingu) i przesłać do innego routera. Nie należy przy tym mylić dwóch pojęć: protokołu używanego do trasowania pakietów (routing protocol) i protokołów obsługiwanych przez router (routed protocol). Router może np. obsługiwać tylko sieć Internet i wtedy potrafi wyznaczać marszruty pakietom generowanym przez protokół IP. Istnieją też routery wieloprotokołowe, które potrafią obsługiwać pakiety generowane przez kilka różnych protokołów, np. przez dwa protokoły: IP i IPX. [1]

## 1.2 Protokoły trasowania

Jeśli chodzi o protokoły używane do trasowania pakietów i komunikowania się z innymi routerami (oraz do modyfikowania i zarządzania tabelami routingu), to można wymienić sześć podstawowych protokołów:

- **RIP** (Routing Information Protocol),
- **IGRP** (Interior Gateway Routing Protocol),
- **Enhanced IGRP**,
- **OSFP** (Open Shortest Path First),
- **IS-IS** (Integrated intermediate System-to-System)
- **Routing statyczny**[1]

### 1.3 Routing dynamiczny:

Routing dynamiczny działa w odmienny sposób. Po wprowadzeniu przez administratora sieci poleceń konfiguracyjnych inicjujących dynamiczny routing, informacje o trasach są automatycznie uaktualniane przez proces routingu za każdym razem, gdy z sieci otrzymywane są nowe informacje. Informacje o zmianach są wymieniane między routerami, jako element procesu uaktualniania. Wyróżniamy dwa podstawowe protokoły routingu dynamicznego : stanu łącza oraz wektora odległości.

Wektor odległości wyznaczany jest przez określenie metryki. Najczęściej stosowane metryki :

- Liczba skoków - jest to liczba routerów, przez które musi przejść pakiet w drodze do celu. Im mniejsza jest liczba skoków, tym lepsza jest metryka. Suma skoków nazywana jest długością ścieżki.
- Pasma - jest to pojemność łącza. Na przykład łącze T1 z pojemnością 1 544 Mb/s jest lepsze niż łącze dzierżawione 64 kb/s.
- Opóźnienie - czas potrzebny do przesłania pakietu z punktu źródłowego do miejsca przeznaczenia.
- Obciążenie - suma aktywności w zasobach sieciowych, takich jak router lub łącze.
- Niezawodność - stopa błędów każdego łącza w sieci.
- Takty zegara - opóźnienie łącza danych wyrażone w taktach zegara IBM PC (w przybliżeniu 55 ms).
- Koszt - dowolna wartość, wyznaczona w oparciu o pasmo, wydatki pieniężne lub inne miary, przyporządkowywana przez administratora sieci. [3]

### 1.4 Routing statyczny:

Routing statyczny jest zarządzany w sposób ręczny, to znaczy konfigurowany przez administratora sieci. Jeśli topologia sieci ulegnie zmianie administrator sieci musi w sposób ręczny dokonać uaktualnienia poszczególnych pozycji tablic routingu.

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

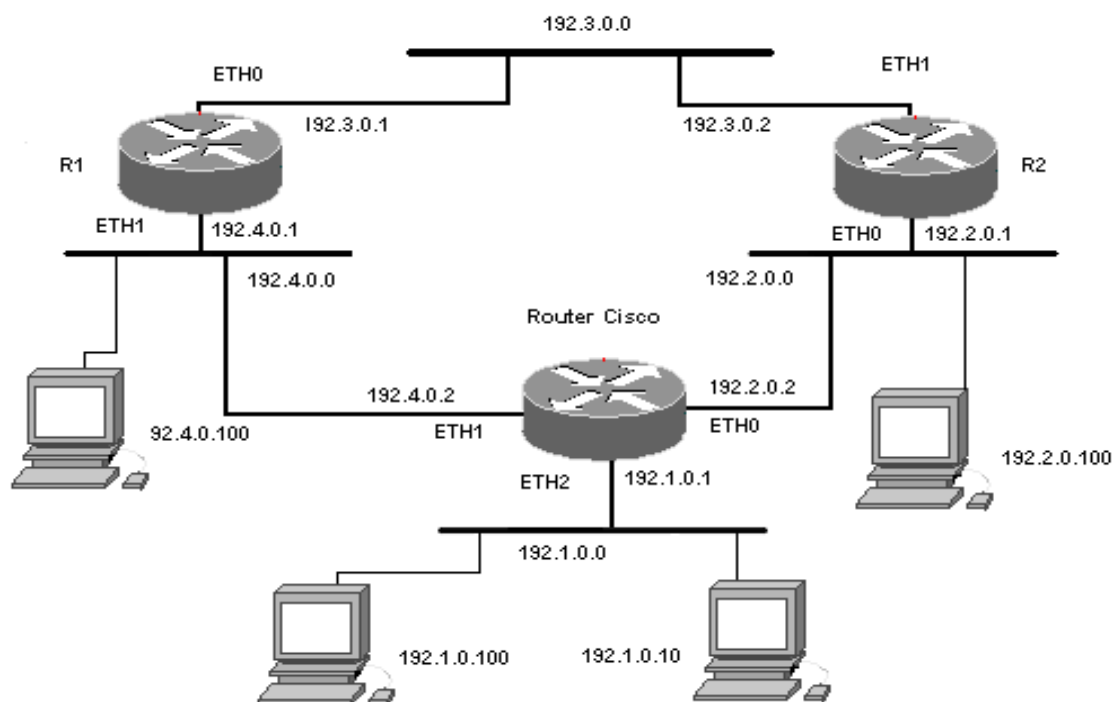
Routing statyczny ma wiele zalet. Router przesyła pakiety przez z góry ustalone interfejsy bez konieczności każdorazowego obliczania tras, co zmniejsza zajętość cykli procesora i pamięci. Informacja statyczna nie jest narażona na deformację spowodowaną zanikiem działania dynamicznego routingu na routerach sąsiednich. Dodatkowo zmniejsza się zajętość pasma

transmisji, gdyż nie są rozsyłane pakiety rozgłoszeniowe protokołów routingu dynamicznego. Dla małych sieci jest to doskonałe rozwiązanie, ponieważ nie musimy posiadać zaawansowanych technologicznie i rozbudowanych sprzętowo routerów. Routing statyczny zapewnia również konfigurację tras domyślnych, nazywanych *bramkami ostatniej szansy* (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. [2]

## 2. Konfiguracja przykładowej sieci :

- konfiguracja routera Cisco z pliku konfiguracyjnego
- konfiguracja routerów R1 i R2 przy pomocy programu **ifconfig** wyświetla i konfiguruje informacje o interfejsie



Rys 2.1 : Schemat konfigurowanej sieci



## 2.1 Konfiguracja routera Cisco z pliku konfiguracyjnego :

```
hostname Cisco
boot system TFTP IOS_Plik_nr_3 192.2.0.1
interface Ethernet0/0
ip address 192.2.0.2 255.255.255.0
interface Ethernet0/1
ip address 192.4.0.2 255.255.255.0
interface Ethernet0/2
ip address 192.1.0.1 255.255.255.0
ip route 192.3.0.0 255.255.255.0 192.2.0.1
end
copy running-config startup-config
```

## 2.2 Konfiguracja routerów w systemie Solaris.

### 2.2.1 Nazwę komputera nadajemy w pliku:

```
/etc/nodename
```

Dla każdego interfejsu tworzymy plik:

```
/etc/hostname.interface
```

w nim umieszczamy nazwę komputera

### 2.2.2 Konfigurujemy router R1.

Aby router działał poprawnie należy obu interfejsom (ETH0 i ETH1) nadać adresy IP. Dla interfejsu ETH0 dla routera R1 robimy to w sposób następujący:

```
ifconfig ETH0 192.3.0.1 broadcast 192.3.0.255 netmask
255.255.255.0
```

Teraz poleceniem **route** możemy sprawdzić, że do tablicy routingu został dodany wiersz opisujący ten interfejs.

Przykładowy wygląd tablicy:

Destination	Gateway	Netmask	Interface
192.3.0.0	0.0.0.0	255.255.255.0	ETH0
127.0.0.0	0.0.0.0	255.0.0.0	lo

Dodatkowy wiersz z adresem 127.0.0.0 jest dodawany automatycznie dla każdego komputera. Jest to tzw. adres zwrotny (*loopback*).

W następnym kroku należy skonfigurować interfejs ETH1 dla routera R1:

```
ifconfig ETH1 192.4.0.1 broadcast 192.4.0.255 netmask
255.255.255.0
```

demony, które należy włączyć:

- inetd,
- rwhod,
- routed,
- named,
- timed

do poprawnego działania sieci włączamy je przez standardowe skrypty startowe:

### 2.2.3 dodatkowa konfiguracja

Aby sieć działała poprawnie należy w pozostałych komputerach tej podsieci (np. w komputerze 192.4.0.100) ustawić adres tego routera (czyli 192.4.0.1) jako bramę. W systemie Windows dokonujemy tego w zakładce otoczenie sieciowe.

### 2.2.4 konfiguracja routera R2 :

Aby router działał poprawnie należy obu interfejsom (ETH0 i ETH1) nadać adresy IP. Dla interfejsu ETH0 robimy to w sposób następujący:

```
ifconfig ETH0 192.2.0.1 broadcast 192.2.0.255 netmask
255.255.255.0
```

Teraz poleceniem **route** możemy sprawdzić, że do tablicy routingu został dodany wiersz opisujący ten interfejs.

Przykładowy wygląd tablicy:

Destination	Gateway	Netmask	Interface
-------------	---------	---------	-----------

```
192.2.0.0          0.0.0.0          255.255.255.0    ETH0
127.0.0.0          0.0.0.0          255.0.0.0        lo
```

Dodatkowy wiersz z adresem 127.0.0.0 jest dodawany automatycznie dla każdego komputera. Jest to tzw. adres zwrotny (*loopback*).

W następnym kroku należy skonfigurować interfejs ETH1:

```
ifconfig ETH1 192.3.0.1 broadcast 192.3.0.255 netmask
255.255.255.0
```

#### Dodatkowa konfiguracja

Aby sieć działała poprawnie należy w pozostałych komputerach tej podsieci (np. w komputerze 192.2.0.100) ustawić adres tego routera (czyli 192.2.0.1) jako bramę. W systemie Windows dokonujemy tego w zakładce otoczenie sieciowe.

#### 2.2.5 Ustawienie masek następuje w pliku:

```
/etc/inet/netmask
```

Przykładowy wygląd pliku:

```
local net.nr      netmask
129.9.0.0         255.255.255.0
```

### 3. Opis wykorzystywanych poleceń SO. Solaris:

**netstat**- wyświetla tablice routingu

**route** – pokazuje/manipuluje tablicą routingu IP

Główne zastosowania to ustawienie routingu statycznego do szczególnych komputerów lub sieci poprzez interfejs po skonfigurowaniu go programem **ifconfig**.

**route** z parametrem **add.del** – modyfikuje tablicę

**show config** – polecenie pokazujące informacje o konfiguracji systemu.

**show version** – polecenie pokazujące konfigurację hardware'u systemu

Aby otrzymać więcej informacji dotyczących interfejsów wykorzystujemy polecenie **show interface ethernet** wyświetlające statystyki dotyczące wszystkich interfejsów ethernetowych: nazwę interfejsu numer jednostki (Ethernet0). [4]

## LITERATURA

- [1] <http://ip.univ.szczecin.pl>
- [2] <http://PCkurier.pl>
- [3] [http://polo.po.opole.pl/~mh/warstwa\\_sieci.html](http://polo.po.opole.pl/~mh/warstwa_sieci.html)
- [4] Dokumentacja SO. Solaris;