Routing

1. Wprowadzenie

Routing (ang.- trasowanie) jest to algorytm, dzięki któremu możliwa jest wymiana pakietów pomiędzy dwoma sieciami. Jest to o tyle istotne, ponieważ gdyby nie urządzenia routujące – routery to niemożliwe byłoby tworzenie dużych sieci. Przykładem takiej sieci jest Internet.

Router (ang. trasownik) jest to urządzenie dzięki któremu możliwa jest realizacja routingu. Zadaniem routera jest określanie tras pomiędzy innymi routerami w swoim najbliższym sąsiedztwie. Urządzeniem takim może być zwykły komputer, którym kieruje specjalnie skonfigurowany system operacyjny np. Linux (router programowy) lub specjalistyczny sprzęt. W mniejszych sieciach najczęściej spotykane są są routery desktop'owe, cechujące się małymi rozmiarami i pełniące jednocześnie funkcję switchy oraz bezprzewodowych punktów dostępowych. W sieciach rozległych (WAN) oraz na ich styku z dużymi sieciami korporacyjnymi (EDGE) stosowane są już zaawansowane urządzenia w oparciu o dedykowaną, wysokowydajną architekturę sprzętową zdolną przełączać miliardy pakietów na sekundę oraz realizować dodatkowe funkcjonalności związane z filtrowaniem i bezpieczeństwem.

Linksys BEFSR41


Cisco ASR 1001-X


Juniper JRR200

2. Algorytmy routing

- Algorytmy statyczne i dynamiczne
  Algorytm statyczny nie jest właściwie algorytmem. Wszystkie ścieżki routingu wyznacza tu na stałe administrator systemu. Jeżeli topologia sieci zmieni się, router nie będzie przekazywał pakietów. Algorytmy dynamiczne natomiast śledzą cały czas topologię sieci (praca w czasie rzeczywistym) i modyfikują w razie potrzeby tablice 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 ściekę dostępu do adresata, tak algorytm multi path pozwala przesyłać pakiety przez wiele niezależnych ścieżek, co nie tylko zwiększa szybko transmisji pakietów, ale te chroni system routingu przed skutkami awarii.

- Algorytmy płaskie i hierarchiczne
  W przypadku algorytmów płaskich wszystkie routery są równorzędne. Można to porówna do sieci typu „peerto-peer". Nie ma tu (ze względu na strukturę logiczną) ważniejszych i mniej ważnych routerów. Algorytmy hierarchiczne postrzegają sieć jako strukturę zhierarchizowaną, dzieląc je na domeny. Pakietami krążącymi w obrąbie każdej domeny zawiaduje wtedy w 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 inteligent). W tym układzie router pełni tylko rolę „przekaźnika" 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 trasy spoczywa na routerach.

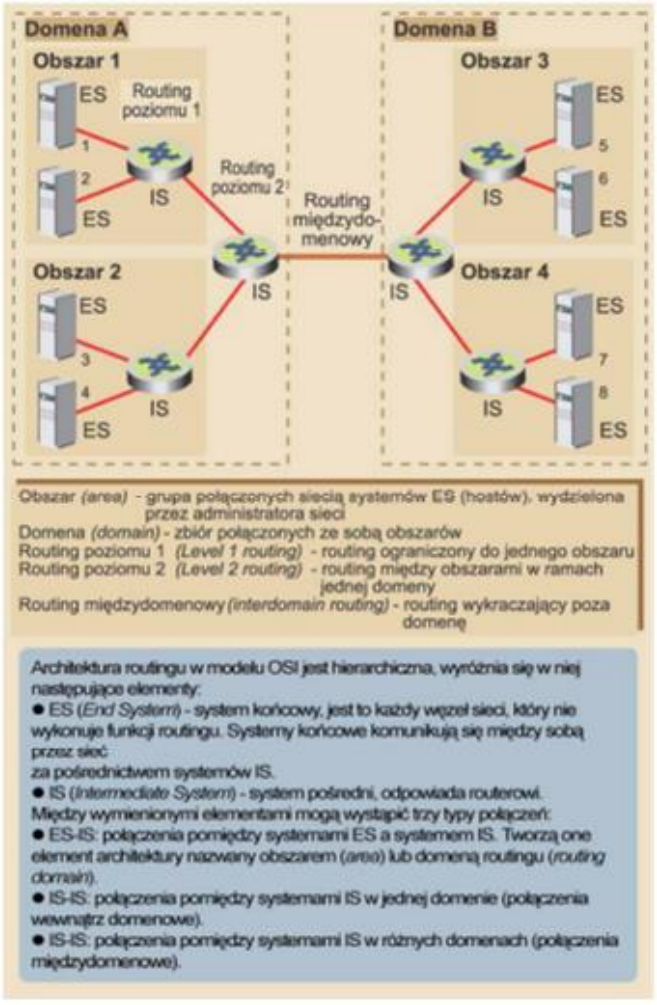
- Algorytmy intradomain i interdomain
  Algorytmy trasowania intradomain operują wyłącznie w obszarze konkretnej domeny, podczas gdy algorytmy interdomain zawiadują pakietami biorąc pod uwag nie tylko zależności zachodzące w ramach konkretnej domeny, ale też powiązania między tą domeną i innymi,

otaczającymi ją domenami. Optymalne trasy wyznaczane przez algorytm intradomain nie muszą być (i najczęściej nie są) najlepsze, jeśli porównamy je z optymalnymi trasami wypracowanymi przez algorytm interdomain („widzący" całą strukturę sieci).

- Algorytmy link state i distance vector
  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 te 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.

3. Działanie routingu OSI

a) Routing OSI rozpoczyna się z chwilą, gdy systemy ES odbierając pakiety ISH zidentyfikują najbliższy system IS.
b) System ES, chcąc wysłać pakiet do innego systemu ES, wysyła pakiet do jednego bezpośrednio z nim połączonych systemów IS.
c) System IS (router) sprawdza adres miejsca przeznaczenia i wysyła pakiet przez najlepszą ścieżkę.
d) Jeśli adres wskazuje docelowy system ES w tej samej podsieci, o czym router wie dzięki zebranej informacji, to wybierze odpowiednią trasę wewnątrz podsieci.
e) Jeśli adres wskazuje docelowy system ES w innej podsieci tego samego obszaru, to router również będzie znał prawidłową trasę.
f) Jeśli adres wskazuje docelowy system ES w innym obszarze, to router poziomu 1 wysyła pakiet do najbliższego routera poziomu 2.
g) Przesyłanie przez routery poziomu 2 trwa tak długo, aż pakiet dotrze do routera w obszarze docelowego sytemu ES.
h) W obszarze docelowego systemu ES router wysyła pakiet do właściwego systemu ES.
i) Systemy IS poznają topologię sieci, używając komunikatów uaktualniania stanu łącz (*linkstate update message*).



4. Wybrane protokoły routingu

Protokół RIP
Protokół RIP (*ang. Routing Information Protocol*) jest protokołem routingu o trybie rozgłoszeniowym, w którym zastosowano algorytm distance-vector, który jako metryki używa licznika skoków między routerami. Maksymalna liczba skoków wynosi 15. Każda dłuższa trasa jest jako nieosiągalna, poprzez ustawienie licznika skoków na 16. Informacje o routingu w protokole RIP przekazywane są z routera do sąsiednich routerów przez rozgłoszenie IP z wykorzystaniem protokołu UDP i portu 250. Jest on szeroko stosowany w sieciach jako protokół wewnętrzny IGP (*Interior Gateway Protocol*), co oznacza, że wykonuje routing pojedynczym autonomicznym systemem albo protokołem zewnętrznym EGP (*Exterior Gateway Protocol*) – wykonuje routing pomiędzy różnymi autonomicznymi systemami. Protokół RIP jest obecnie szeroko wykorzystywany w Internecie i używany w sieciach jako podstawowa metoda wymiany informacji o routingu pomiędzy routerami.

Protokół IGRP
Protokół IGRP (*ang. Interior Gateway Routing Protocol*) został zaprojektowany, aby wyeliminować pewne mankamenty protokołu RIP oraz poprawić obsługę większych sieci o różnych przepustowościach łączy. IGRP, podobnie jak RIP, używa trybu rozgłoszeniowego do przekazywania informacji o routingu sąsiednim routerem. Jednak IGRP ma własny protokół warstwy transportu. Nie wykorzystuje UDP ani TCP do przekazywania informacji na temat trasy sieciowej. Oferuje on trzy główne rozszerzenia względem protokołu RIP. Po pierwsze może obsługiwać sieć do 255 skoków miedzy routerami. Po drugie potrafi rozróżniać odmienne rodzaje nośników połączeń i związane z nimi koszty. Po trzecie oferuje szybszą konwergencję , dzięki użyciu aktualizacji typu flash.

Protokół OSPF
Protokół OSPF (*ang. Open Shortest Path First*) został zaprojektowany, by spełniać potrzeby sieci opartych na IP, uwierzytelnianiu źródła trasy, szybkością konwergencji, oznaczaniem tras przez zewnętrzne protokoły routingu oraz podawanie tras w trybie rozgłoszeniowym. W przeciwieństwie do protokołów RIP i IGRP, które ogłaszają swoje trasy tylko sąsiednim routerem, routery OSPF wysyłają ogłoszenia stanu łącza do wszystkich routerów w obrębie tego samego obszaru hierarchicznego poprzez transmisję IP w trybie rozgłoszeniowym. Ogłoszenie stanu łącza zawiera informacje dotyczące podłączonych interfejsów, używanych metryk oraz inne niezbędne do przetwarzania baz danych ścieżek sieciowych i topologii. Routery OSPF gromadzą informacje na temat łącza danych i uruchamiaj algorytm SPF (znany także jako algorytm Dijkstry), aby obliczy najkrótszą ścieżkę do każdego węzła.

Routing statyczny
Routing statyczny używany jest wówczas, gdy mapa połączeń sieciowych jest programowana w routerze „ręcznie” przez administratora. W razie, gdy jakaś ścieka zostanie przerwana, administrator musi przeprogramować router, aby odpowiednie pakiety mogły dotrze do celu. W systemach sieciowych o kluczowym znaczeniu taki sposób trasowania jest niemożliwy do zaakceptowania. Stosuje się więc dynamiczne routery, które automatycznie diagnozują stan połączeń i wyznaczają połączenia alternatywne.

5. Instrukcje do użytego oprogramowania

a. traceroute

Aplikacja traceroute jest programem pozwalającym na zbadanie trasy pakietu od stacji źródłowej do docelowej wraz z oszacowaniem czasów opóźnień na poszczególnych węzłach (czas minimalny, maksymalny i średni).
Przykłady użycia:
Korzystanie z aplikacji sprowadza się do wprowadzenia adresu analizowanego węzła:

- w przypadku systemu Windows - `tracert www.google.pl` lub `adresIP`
- w przypadku Linuxa natomiast - `traceroute www.google.pl` lub `adresIP`

b. ping

Ping – program używany w sieciach komputerowych TCP/IP (takich jak Internet), służący do diagnozowania połączeń sieciowych. Pozwala na sprawdzenie czy istnieje połączenie pomiędzy hostami testującym i testowanym. Umożliwia on zmierzenie liczby zgubionych pakietów oraz opóźnień w ich transmisji, zwanych lagami.
Przykład użycia:

```
ping www.google.pl
```

Literatura:

[1] http://cisco.netacad.net
[2] James F. Kurose, Keith W. Ross: Sieci komputerowe. Od ogółu do szczegółu z Internetem w tle. Wyd. Helion, Gliwice 2006
[3] Gała Z.: Sieci komputerowe księga eksperta. Wyd. Helion, Gliwice 2004
[4] Sportack M.: Sieci komputerowe - Księga eksperta. Wyd. Helion, Gliwice 1999
[5] Michałowska A., Michałowski S.: Sieci komputerowe od A do Z. Wyd. Mikom, Warszawa 2000

Scenariusz nr 1

1. **Oprogramowanie:**

Systemowe:
Windows: *ping, tracert* – uruchamiane w systemie Windows z linii poleceń
(Menu Start → Uruchom → ***cmd.exe****)*
Linux: *ping, traceroute* - Programy → Ulubione → Terminal

Serwisy geolokalizacyjne zwracające informacje o fizycznym miejscu (kraj, miasto, przybliżone współrzędne geograficzne) w którym znajduje się serwer w oparciu o adres IP lub nazwę domeny (do wykorzystania w punkcie 2.b): www.iplocationfinder.com, **www.iplocation.net**, www.infosniper.net, www.ip-tracker.org

2. **Przygotowanie do wykonania ćwiczenia**

a) Wybrać „branżę" dla której realizowane będzie laboratorium: …… (← uzupełnić) (motoryzacja, nauka, media, sport, itp.)
b) Uzupełnić tabelę adresami domen z wybranych branży, tak aby każdy z serwerów był fizycznie zlokalizowany na innym kontynencie.
!!! Zwrócić uwagę na to, że rozszerzenie domenowe (np. .pl) nie musi odpowiadać fizycznej lokalizacji serwera (którą sprawdzamy w oparciu o serwisy geolokalizacyjne) !!!
c) Zanotować dane na temat miejsca, z którego przeprowadzane jest ćwiczenie:
- adres IP - …….
- fizyczna lokalizacja - ……..
(sprawdzić, czy fizyczna lokalizacja dla bazowego (startowego) adresu IP zgadza się z informacją zwracaną przez serwisy geolokalizacyjne, oraz jaka jest ich dokładność)

Lp.	adres IP	Domena	kontynent	kraj	miasto
1			Europa		
2			Azja		
3			Afryka		
4			Australia		
5			Ameryka Płn.		
6			Ameryka Pd.		

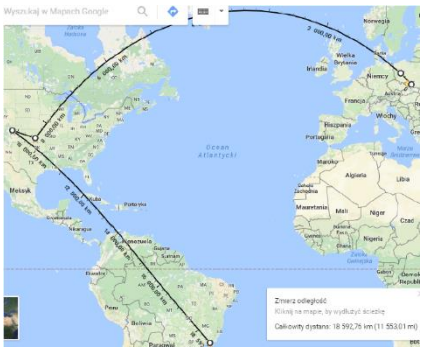
3. **Wykonanie ćwiczenia:**

Dla każdego z serwerów z tabeli wykonać kroki A, B i C.

A) Wyznaczyć średni czas trasy pakietu do miejsca docelowego (za pomocą polecenia ***ping***),
   a. Windows: *ping <adres_IP>*
   b. Linux: *ping -c X <adres_IP>* (X to ilość powtórzeń zapytania)
B) Wyznaczyć trasę pakietów do miejsca docelowego (za pomocą polecenia ***tracert)*** Zapisać wyznaczone trasy pakietów (na zrzutach ekranu, w plikach tekstowym lub arkuszu kalkulacyjnym).
   a. Windows: *tracert <adres_IP>*
   b. Linux: *traceroute <adres_IP>*
C) Wyszukać i opracować informacje na temat użytkowników odwiedzających daną stronę (serwisy http://www.alexa.com , http://follow.net).
   Wyszukać informacje dla maksymalnego okresu czasowego dotyczące:
   a. *Global Rank i ranking strony dla danego kraju,*
   b. *Pageviews / User (średnia liczba stron przeglądanych dziennie dla jednego użytkownika)*
   c. *Time on site (średni czas spędzony dzienne na stronie przez użytkownika),*
   d. *Lista trzech krajów których mieszkańcy najczęściej odwiedzają daną stronę*
   e. *Pozycja w rankingu krajowym analizowanej strony*
   f. *Podać trzy strony, które użytkownicy odwiedzają przed wejściem na daną stronę*

Uwaga: Otrzymywanie statystyk na stronie alexa: www.alexa.com → Features → Website Traffic Statistics

D) Dla minimum **trzech** wybranych serwerów opracować na mapie świata trasę z punktu początkowego do punktu docelowego (routery znajdujące się w tej samej lokalizacji należy zagregować na mapie do jednego punktu)



E) Dla wszystkich sześciu serwerów, na podstawie wyznaczonych (w punkcie B) tras określić
- ostatni wspólny router na trasie dla wszystkich ścieżek,
- 6 unikalnych ruterów (po jednym dla każdej ścieżki)

Lokalizacje powyższych routerów należy opisać (kraj, miasto) oraz umieścić na mapie.

F) Na koniec laboratorium powtórnie sprawdzić i zapisać trasę do wszystkich serwerów (punkt B), porównać z trasą z początku zajęć i sprawdzić czy nie uległy zmianie. Zanotować spostrzeżenia i miejsca zmian. Zanotować czas, po którym ponownie sprawdzano trasy do serwerów (im więcej czasu upłynie pomiędzy pierwszym i drugim sprawdzeniem tras, tym lepiej – tym większa szansa na zmiany w konfiguracji mechanizmów routingu)

4. Analiza nagłówków email

Do testów wykorzystać 3 wiadomości email przesyłane pomiędzy kontami pocztowymi różnych serwerów poczty:

a) Archiwalną (najlepiej taką, której nadawca znajdował się w momencie wysyłania wiadomości na innym kontynencie/za granicą)
b) Wysłaną podczas zajęć między członkami grupy
c) Wysłaną po zakończeniu zajęć pomiędzy członkami grupy przy wykorzystaniu sieci „domowej” (przy realizacji ćwiczenia w laboratorium). W przypadku zdalnej realizacji laboratorium, należy w zastępstwie wykorzystać drugą (inną) wiadomość opisaną w podpunkcie a) (archiwalną)

Należy przeanalizować szczegółowe nagłówki e-mail zarówno po stronie odbiorcy i podać następujące informację:

a) Czas wysłania i odebrania wiadomości
b) Adres IP nadawcy wiadomości
c) Lista serwerów pośredniczących w przesyłaniu wiadomości (domena + adres IP)
d) Trasa transferu wiadomości pomiędzy serwerami na mapie (jak w punkcie 3.D)
e) Czy nadawca został zweryfikowany przez SPF?
f) Czy nadawca został zweryfikowany przez DKIM
g) Wersja MIME
h) Format wiadomości (HTML, czysty tekst itp.)

Każda odpowiedź powinna być uzupełniona odpowiednim fragmentem nagłówka wiadomości email.

Notatka: Do analizy nagłówków można wykorzystać narzędzie G Suite:
https://toolbox.googleapps.com/apps/messageheader/
(należy samodzielnie opracować niezbędne informacje a nie przeklejać „output” z narzędzia GSuite)

5. Zawartość sprawozdania:

- analiza uzyskanych danych dla wszystkich serwerów z tabeli
- skan lub zdjęcie tabeli uzupełnionej w trakcie zajęć (dla zajęć realizowanych w laboratorium)
- informacje o wystąpieniu zmian w trasach routingu do serwerów docelowych
- informacje o routerach unikalnych i routerze wspólnym
- mapy tras dla minumum trzech wybranych serwerów
- analizę, porównanie i wnioski części związanej z analizą nagłówków email