Politechnika Gdańska

WYDZIAŁ ELEKTRONIKI
TELEKOMUNIKACJI
I INFORMATYKI

Materiały dydaktyczne do laboratorium

„Podstawy konfiguracji protokołów routingu dynamicznego RIP, OSPF oraz BGP wspieranych przez routery firmy *Olicom*”

1. Wstęp

1.1 Cel ćwiczenia

Głównym celem ćwiczenia jest umożliwienie poznania podstaw konfiguracji protokołów routingu dynamicznego realizowanych przez routery firmy *Olicom*. Rozpatrywane są: *Routing Information Protocol, Open Shortest Path First* oraz *Border Gateway Protocol*. Przed przystąpieniem do ćwiczenia, studenci powinni zapoznać się z wymaganą literaturą (patrz pkt. 5), która zostanie wyegzekwowana w postaci tzw. wejściówki. Teoria oraz praktyka nabyta w czasie ćwiczeń, umożliwi studentom prawidłowe rozróżnianie protokołów routingu IGP (ang. Interior Gateway Protocols) oraz EGP (ang. Exterior Gateway Protocols), zdefiniowanie obszaru ich zastosowania. Student będzie potrafił uruchomić oraz zweryfikować prawidłowe ich funkcjonowanie.

1.2 Protokoły routingu dynamicznego

Protokoły routingu dynamicznego są technologią, która umożliwia routerom: odkrywanie i utrzymywanie tras połączeń, rozpoznawanie topologii sieci oraz parametrów połączeń, które wykorzystywane są do obliczenia i wyznaczenia tras. W celu wymiany informacji pomiędzy routerami wykorzystywane są specjalne komunikaty przenoszące informacje o zmianach w sieci (ang. routing update messges). Ich treść w zależności od sytuacji to całkowita zawartość tablicy routingu lub jej fragment.

Dwie podstawowe klasy algorytmów routingu dynamicznego to: wektorowo – odległościowe oraz stanu łącza. W przypadku tych pierwszych decyzje o wyborze trasy podejmowane są w oparciu o odległości do poszczególnych sieci lub koszt związany z przesłaniem pakietu po danej trasie. Natomiast w przypadku tych drugich - stanu łącza (inaczej zwanych najkrótszych ścieżek) wymagany jest większy nakład czasu na przetwarzanie. Umożliwiają one efektywniejszą kontrolę procesu routingu[1].

1.2.1 Protokół RIP

W protokole RIP stosowany jest algorytm *distance - vector*. RIP jest wykorzystywany w sieciach jako wewnętrzny protokół routingu (IGP). Specyfikację protokołu RIP definiują dwa dokumenty RFC 1058 oraz 1723. RFC 1058 opisuje pierwszą implementację protokołu, natomiast jego wersję zaktualizowaną (RIP v2) opisuje drugi dokument.

[1] Obszerniejsza dyskusja reguł doboru tras w pracy dyplomowej – punkt 4.3

Przy wyborze trasy przez algorytm *distance-vector* stosowane jest kryterium najmniejszej liczby skoków (ang. hops) niezbędnych do osiągnięcia miejsca przeznaczenia.
W protokole RIP komunikaty uaktualniające wysyłane są co określony, stały przedział czasu, lub w przypadku pojawienia się zmian w topologii sieci. Router po przyjęciu takiego komunikatu, uaktualnia tablicę routingu. Do każdej znanej routerowi sieci utrzymywana jest tylko jedna trasa – ta z najmniejszą liczbą skoków. Router niezwłocznie po uaktualnieniu swojej tablicy routingu wysyła informacje o zmianie do pozostałych routerów w sieci. Są one wysyłane niezależnie od regularnie wysyłanych uaktualnień.
Protokół RIP, dzięki ograniczeniu liczby skoków, które mogą pojawić się pomiędzy źródłem a miejscem przeznaczenia, zapobiega przesyłaniu pakietów bez końca w pętli. Maksymalna liczba skoków na ścieżce wynosi 15. Jeśli router przyjmie uaktualnienie routingu, a następnie po zwiększeniu miary (czyli liczby hop-ów) o jeden nastąpi przekroczenie granicy 15 skoków, to takie miejsce przeznaczenia w sieci staje się nieosiągalne (nieskończoność).
W celu dostosowania się do szybkich zmian topologii sieci protokół RIP wyposażono w mechanizmy stabilizujące. Na przykład, by zapobiec skutkom błędnej informacji o routingu, zaimplementowano mechanizmy *split-horizon* i *hold-down*. Jak już wspomniano, powstawaniu pętli zapobiega ograniczenie liczby skoków.
W celu dostosowania do potrzeb wydajności routingu, protokół RIP wyposażono w kilka zegarów (ang. timers). Wśród nich są zegary: uaktualnienia routingu (ang. routing-update timer), limitu czasu trasy (ang. route timeout timer) i czyszczenia trasy (ang. route-flush timer). Zegar uaktualnienia routingu wyznacza przedziały czasu pomiędzy kolejnymi okresami uaktualnienia. Jest to stały przedział nie przekraczający 30 [s]. Do każdego wpisu w tablicy routingu przypisany jest limit czasu trasy; w przypadku jego wyczerpania trasa zostaje oznaczona jako nieważna. Mimo tego jest nadal utrzymywana w tablicy routingu aż do momentu, gdy zostanie wyczerpany czas czyszczenia trasy.

1.2.2 Protokół OSPF

Protokół OSPF został opracowany przez IETF (ang. Internet Engineering Task Force) i zdefiniowany w dokumencie RFC 1247. OSPF jest protokołem otwartym, co oznacza, że jego specyfikacja jest ogólnie dostępna. Jest to protokół klasy *link-state*, wykorzystujący algorytm SPF (ang. Shortest Path First) Dijkstry. OSPF został zaprojektowany w celu zwiększenia efektywności przetwarzania w sieciach pracujących z protokołem IP. Wybór trasy odbywa się na podstawie wielu czynników takich jak szybkość i opóźnienie wprowadzane przez łącze,

potrzeba ominięcia określonych obszarów lub różnorodne priorytety. Decyzja o wyborze trasy podejmowana jest na podstawie algorytmu SPF, który uwzględnia:

- liczbę routerów, które musi przejść pakiet, by dotrzeć do miejsca przeznaczenia, zwaną liczbą skoków (ang. hops)
- szybkość transmisji połączeń pomiędzy poszczególnymi systemami autonomicznymi
- opóźnienia spowodowane przeciążeniem sieci. Router może skierować pakiety trasą omijającą przeciążone fragmenty sieci
- koszt trasy, którego miara jest określona przez administratora sieci, najczęściej oparta na rodzaju użytego medium transmisyjnego

Protokół OSPF wysyła zgłoszenia LSA (ang. Link-State Advertisement) do wszystkich routerów znajdujących się w danym obszarze hierarchicznym. W LSA zawarte są między innymi informacje o przyłączonych interfejsach i użytych miarach. Po zgromadzeniu informacji o łączach (link-state) routery, stosując algorytm SPF, wyznaczają najkrótszą ścieżkę do każdego węzła.

W odróżnieniu od protokołu RIP protokół OSPF może działać w układzie hierarchicznym. Największą jednostką w hierarchii jest system autonomiczny (ang. Autonomous System), który jest zbiorem sieci wspólnie administrowanych, które mają wspólną strategię routingu. OSPF jest protokołem IGP, może jednak przyjmować i wysyłać trasy do innych systemów (AS).

System AS można podzielić na obszary (ang. Areas), które są grupami sąsiednich sieci i przyłączonych hostów. Poszczególne obszary sprzęgają routery graniczne obszaru (ang. Area Border Routers). Router graniczny utrzymuje oddzielną dla każdego obszaru bazę danych, zawierającą topologię sieci.

Baza danych jest obrazem sieci wyrażonym w powiązaniach między routerami. Zawiera zbiór zgłoszeń LSA pochodzących od wszystkich routerów w danym obszarze. Ponieważ routery w jednym obszarze otrzymują tę samą informację, to ich bazy dotyczące topologii są identyczne. Toplogia obszaru jest niewidoczna dla urządzeń znajdujących się poza nim. Podział systemów AS na obszary przyczynia się do zmniejszenia ruchu związanego z routingiem.

Wydzielenie obszarów stworzyło dwa typy routingu OSPF:

- wewnętrzny – źródło i miejsce przeznaczenia znajdują się w tym samym obszarze
- zewnętrzny - źródło i miejsce przeznaczenia znajdują się w dwóch różnych obszarach

Za dystrybucję informacji pomiędzy obszarami jest odpowiedzialna sieć szkieletowa OSPF (ang. OSPF backbone). Składa się ona ze wszystkich routerów granicznych, linii, które nie łączą routerów wewnątrz obszaru, oraz przyłączonych do nich routerów. Szkielet jest również

obszarem OSPF, stąd wynika, że routery szkieletu używają takich samych procedur i algorytmów do utrzymania informacji routingu w szkielecie, jak każdy inny router w obszarach sprzężonych ze szkieletem. Topologia szkieletu jest niewidoczna dla routerów wewnątrz obszarów, ponieważ nie należy do topologii obszarów.

Routery brzegowe systemów autonomicznych pracujące z protokołem OSPF dowiadują się o zewnętrznych trasach przez zewnętrzne protokoły bramowe, takie jak np. protokół EGP (ang. Exterior Gateway Protocol) lub protokół BGP (ang. Border Gateway Protocol).

Wśród dodatkowych właściwości protokołu OSPF można wymienić: jednakowy koszt (ang. equal cost), routing wielościeżkowy (ang. multipath routing) i routing oparty na żądaniach TOS (ang. type-of-service) wyższej warstwy. Routing oparty na żądaniach TOS wspomaga te protokoły warstwy wyższej, które mogą określić szczególne typy usług. Na przykład aplikacja może określić pewne dane jako pilne. Jeśli protokół OSPF dysponuje szybkimi łączami, to może ich użyć do przekazywania pilnych danych.

Protokół OSPF może posługiwać się jedną lub wieloma miarami. W przypadku użycia jednej miary jest ona przyjmowana arbitralnie i nie zachodzi potrzeba obsługi TOS. W przypadku użycia większej liczby miar, TOS jest wspomagany oddzielnie każdą z nich i związanymi z nimi tablicami routingu. Ponieważ TOS protokołu IP zawiera trzy bity - opóźnienie (ang. delay), przepustowość (ang. throughput) i niezawodność (ang. reliability) - to do dyspozycji jest osiem kombinacji. Jeśli przykładowo trzy bity TOS określają małe opóźnienie, niską przepustowość i wysoką niezawodność, to protokół OSPF wylicza trasy do wszystkich miejsc przeznaczenia opierając się na tym wyznaczniku TOS.

Do zgłoszenia każdego miejsca przeznaczenia są dołączane maski podsieci IP, dające możliwość użycia opcji zmiennej długości maski podsieci (ang. variable-length subnet mask). Dysponując tą opcją, sieć IP można podzielić na wiele podsieci o różnych rozmiarach, dzięki czemu administrator może bardzo elastycznie konfigurować sieć.

1.2.3 Protokół BGP

Protokół BGP należy do klasy protokołów zewnętrznych (EGP), został zdefiniowany w RFC 1771. BGP realizuje routing pomiędzy wieloma systemami autonomicznymi (domenami) i wymienia informacje o routingu i dostępności z innymi systemami posługującymi się protokołem BGP. Protokół BGP został tak zaprojektowany, aby zastąpić swego poprzednika, obecnie już zdezaktualizowany protokół EGP. BGP efektywnie rozwiązuje problemy związane z routingiem międzydomenowym oraz skalowaniem sieci Internet.

Przy wyborze optymalnej trasy protokół BGP posługuje się algorytmem *distance-vector*. W trakcie inicjacji połączenia równorzędne routery BGP (sąsiedzi) (ang. BGP peers) wymieniają kompletne kopie swoich tablic routingu. Przy kolejnych modyfiakcjach tras, aktualizowane są jedynie zmiany.

Protokół BGP wykonuje trzy typy routingu:

- wewnątrz systemów autonomicznych - między dwoma lub większą liczbą routerów BGP zlokalizowanych w jednym systemie autonomicznym, na przykład w przedsiębiorstwie, uczelni lub u jednego dostawcy usług internetowych
- na zewnątrz systemów autonomicznych - między dwoma lub większą liczbą routerów w różnych systemach autonomicznych
- przez systemy autonomiczne - między dwoma lub większą liczbą routerów BGP, które wymieniają ruch przez system autonomiczny, nie obsługujący protokołu BGP

Urządzenia pracujące z protokołem BGP wymieniają informacje o routingu podczas inicjacji i uaktualniania. Gdy router jest włączany do sieci po raz pierwszy, routery BGP wymieniają swoje wewnętrzne tablice routingu. Podobnie, gdy zachodzą zmiany w tych tablicach, routery wysyłają te fragmenty tablicy, które zostały zmienione. Routing BGP uaktualnia tylko zgłoszenia ścieżek optymalnych do sieci, natomiast nie wysyła regularnie harmonogramowanych uaktualnień.

Protokół BGP używa tylko jednej miary routingu do wyznaczenia optymalnej ścieżki do danej sieci. Miara ta składa się z arbitralnie przyjętej liczby jednostkowej, która określa stopień preferencji konkretnego łącza. Zazwyczaj miarę tę przypisuje do każdego z łączy administrator sieci, kierując się różnorodnymi kryteriami. Może to być liczba systemów autonomicznych, przez które przechodzą, ścieżka, stabilność, szybkość, opóźnienie lub koszt.

Dokument RFC 1771 definiuje cztery typy komunikatów:

- komunikat otwierający (ang. open message) - otwiera sesję komunikacyjną protokołu BGP pomiędzy równorzędnymi routerami i jest pierwszym komunikatem, wysyłanym przez obie strony po ustaleniu połączenia na poziomie protokołu transportowego. Komunikat otwierający jest potwierdzany komunikatem podtrzymującym wysyłanym przez równorzędny router. Natychmiast po potwierdzeniu komunikatu otwierającego mogą być wymieniane komunikaty uaktualniające, zgłoszeniowe i podtrzymujące
- komunikat uaktualniający (ang. update message) - zapewnia uaktualnianie routingu w innych systemach BGP, pozwala routerom odtworzyć u siebie obraz topologii sieci. W celu zapewnienia niezawodnego dostarczania uaktualnień do ich przesyłania używa

się protokołu TCP. Komunikaty otwierające mogą wycofywać z tablicy routingu jedną lub więcej niewykonalnych tras i podczas ich wycofywania zgłaszać nowe

- komunikat zgłoszeniowy (ang. notification message) - jest wysyłany w przypadku wykrycia błędu. Zgłoszenia są używane do zamykania i otwierania sesji i informowania wszystkich przyłączonych routerów o przyczynie zamknięcia sesji
- kmunikat podtrzymujący (ang. keep-alive message) powiadamia równorzędne routery BGP o tym, że router jest aktywny. Częstotliwość wysyłania komunikatu jest dobrana tak, aby zapobiec wygaszeniu sesji

1.3 Routery Olicom

Routery firmy Olicom realizują routing IP. Jak już zostało wspomniane (pkt. 1.1) implementacja dynamicznego routingu wspiera dwa protokoły wewnętrzne, RIP i OSPF, oraz jeden protokół routingu zewnętrznego - BGP. Ich funkcjonalność zgodna jest z wymaganiami zawartymi w dokumentach RFC (ang. Request For Comments) 1058 (RIP), 1247 (OSPF 2), 1771 (BGP-4) wraz z pewnymi dodatkowymi cechami będącymi rozwiązaniami firmy Olicom. Są to odpowiednio dla RIP:

- inteligentne rozgłaszanie (ang. smart advertising) – redukuje ilość rozsyłanych pakietów z uaktualnieniami poprzez łącza WAN,
- przenoszenie na barana (ang. piggy-back) – jako rozszerzenie do inteligentnego rozgłaszania, uaktualnienia wysyłane są jedynie wraz z danymi do strony odbiorczej,
- wsparcie dla numerowanych i nienumerowanych połączeń Point-to-Point,
- wsparcie dla adresów dodatkowych (ang. secondary addresses),
- wymiana informacji routingowej w oparciu o polityki importu oraz eksportu (ang. import/export policies),
- wsparcie dla wymiany informacji routingowej z innymi protokołami

dla OSPF:

- podsieci o zmiennej długości – możliwość podziału adresu IP klasy A, B lub C na wiele podsieci o zmiennej długości,
- wsparcie dla adresów dodatkowych (ang. secondary addresses) – możliwość przypisania do jednego interfejsu kilku adresów,
- wymiana informacji routingowej w oparciu o polityki importu oraz eksportu (ang. import/export policies) (patrz pkt. 2.4.10)

1.3.1 Routery

Wszystkie stanowiska w laboratorium wyposażone są w :

- moduł routera serii CrossFire 8011 / 8012,
- komputer PC wraz z kartą sieciową Ethernet,
- odpowiednie okablowanie umożliwiające połączenie karty sieciowej komputera z modułem routera oraz podłączenie do konsoli routera poprzez port RS

Moduł routera charakteryzuje się poniższymi cechami:

- procesor – 33 MHz Intel i960 RISC dla 8011 oraz 66 MHz Intel i960 RISC dla 8012,
- pamięć systemowa – 16 MB (8011 oraz 8012),
- pamięć flash – 4 MB (8011 oraz 8012),
- AP&D – Address Processor and Directory – umożliwia routerowi bardzo szybkie podejmowanie decyzji routingowej,
- interfejsy – każdy moduł zawiera od jednego do dwóch Intelligent Media Adapter, a każde IMA posiada kilka interfejsów LAN lub WAN; poniżej wymienione są IMA wspierane przez 8011:
    - 16 MHz, Intel i960 RISC based TMA I Dual Token Ring Interface STP (Type 1) or UTP (Type 3),
    - 33 MHz, Intel i960 RISC based TMA II Dual Token Ring Interface STP (Type 1) or UTP (Type 3),
    - 16 MHz, Intel i960 RISC based Dual Token Ring Interface – Fiber Optic Token Ring (IEEE 802.5J),
    - 16 MHz, Intel i960 RISC based Dual Ethernet Interface 10Base-T,
    - 20 MHz, Dual WAN with up to 2 Mb/s per Interface – V.35, RS232, X.21/RS422 or T1,
    - 33 MHz, Intel i960 RISC based Qwad WAN – V.35, RS232, X.21/RS422 or T1,

    dla 8012:

    - 33 MHz, Intel i960 RISC based TMA III Dual Token Ring Interface STP (Type 1) or UTP (Type 3),
    - 33 MHz, Intel i960 RISC based TMA III Dual Token Ring Interface – Fiber Optic Token Ring (IEEE 802.5J),
    - 16 MHz, Intel i960 RISC based Dual Ethernet Interface 10Base-T,

    - 33 MHz, Intel i960 RISC based Qwad WAN – V.35, RS232, X.21/RS422 or T1
- konsola – umożliwia zarządzanie modułem (patrz pkt. 1.3.2.1),
- modem – umożliwia zdalne połączenie z konsolą,
- feature pack – karta PCMCIA w połączeniu z pamięcią flash na płycie modułu umożliwia wykonywanie kopii bezpieczeństwa oprogramowanie podczas upgrade'u,
- dedykowany procesor diagnostyczny (ang. Dedicated Diagnostic Processor) – diagnozuje poprawne działanie funkcji niskiego poziomu (np. port konsoli, modemu)

1.3.2 Zarządzanie

Zarządzanie routerami możliwe jest poprzez wykorzystanie jednej z trzech możliwości:

- kosoli,
- sesji telnet,
- sesji Olicom Clear Sight wykorzystującego protokół SNMP (ang. Simple Network Management Protocol)

1.3.2.1 Konsola

Metoda ta charakteryzuje się tym, że połączenie odbywa się poza pasmem sieci i jest realizowane przez łącze szeregowe, jeśli osoba administrująca znajduje się w pobliżu urządzenia, lub przez modem. Dzięki takiemu podejściu przepustowość sieci nie jest ograniczana. Konfiguracja poprzez konsolę jest trudna ze względu na wymóg pamiętania wielu skomplikowanych poleceń, co wiąże się z koniecznością odpowiedniego przeszkolenia. Z drugiej strony urządzenie zewnętrzne służące do konfiguracji może nie być bardzo skomplikowane, co pomaga obniżyć pewne koszty. Konfiguracja poprzez konsolę zwiększa również poziom bezpieczeństwa, gdyż potencjalny atak musiałby się odbyć przez bezpośredni kontakt z urządzeniem.

1.3.2.2 Sesja protokołu Telnet

Dzięki sesji z wykorzystaniem usługi telnet, administrator uzyskuje funkcjonalność (żmudne polecenia) w ten sam sposób jak poprzez konsolę. Jedyną różnicą jest to, iż sesja taka może się odbyć zdalnie przez sieć, jednak wymagana jest znajomość adresu IP portu routera.

1.3.2.3 Sesja Olicom Clear Sight

Oprogramowanie Clear Sight dostarcza graficzny interfejs, dzięki któremu administrator w sposób łatwy i intuicyjny jest w stanie bardzo szybko skonfigurować router z każdego miejsca w sieci (znając adres IP routera). Ruch generowany przez Clear Sight w niewielkim stopniu obciąża sieć, ponieważ system oparty jest na protokole SNMP. Również w tym przypadku zabezpieczenie jest niewielkie, gdyż osoba zarządzająca może wykorzystać tylko kilkuznakowe hasła, które mogą zostać złamane w bardzo krótkim czasie. Clear Sight posiada wiele bardzo przydatnych funkcji, które są potrzebne do sprawnego zarządzania sieciami. W większości funkcje te nie są dostępne przy wykorzystaniu metod dostępu omówionych w poprzednich dwóch podpunktach. Przykładowe narzędzia Clear Sight:

- zarządzanie zdarzeniami (ang. event management)
- zarządzanie statystykami (ang. statistics management)
- przechwytywanie sesji (ang. session capture)
- analiza protokołów

2. Literatura dla zainteresowanych

1. Woźniak J., Nowicki K.: *Sieci LAN, MAN i WAN – protokoły komunikacyjne*, WFPT, Kraków, 1998
2. Routing Information Protocol, RFC 1058
3. Routing Information Protocol 2, RFC 2453
4. Open Shortest Path First 2, RFC 2328
5. Border Gateway Protocol 4, RFC 1771