Rzeszów, 08.01.2003r.

Laboratorium
„Sieci Komputerowe”

B G P

Autor: **Kurc Bartłomiej** IV FDS L07

Spis treści

STRESZCZENIE

Niniejsze opracowanie ma na celu rozszyfrować i wyjaśnić znaczenie skrótu BGP. Ponieważ czysto szczegółowe rozwinięcie w/w tematu rzuciło by tylko cień światła na interesujące nas zagadnienie, dlatego też na początku należy ogólnie zapoznać się z dziedziną, w której jednym z wątków okaże się być właśnie BGP – jego opis, właściwości i charakterystyka. W tym celu szerzej poznajmy rodzinę protokołów TCP/IP.

Opracowanie to może stanowić wstęp do badań najpopularniejszych obecnie protokołów rutingu, wykorzystywanych zarówno w małych (z niewielką liczbą ruterów) sieciach LAN, jak i w dużych systemach autonomicznych sieci Internet. Wybór protokołu rutingu i jego właściwe skonfigurowanie jest ciekawym zadaniem projektowym. Przemyślana konfiguracja sieci owocuje wysoką wydajnością, a przede wszystkim jej niezawodnością działania (ciągłą dostępnością najlepszych ścieżek dla trasowanych pakietów). Znajomość tajników działania protokołów trasowania jest również kluczem do zabezpieczenia sieci przed nadmiernym ruchem o charakterze organizacyjnym i ruchem związanym z wszelkimi próbami niepowołanego dostępu z zewnątrz. Omawiane w pracy rozwiązanie ma duże walory poznawcze. Umożliwia zapoznanie się z oprogramowaniem odpowiadającym na poziomie funkcjonalnym oprogramowaniu ruterów Cisco, firmy nazywanej „szarą eminencją Internetu”, której wysokiej klasy produkty dominują ostatnio rynek sprzętu przełączającego i rutującego.

1. „W drodze do celu – czyli krótkie wprowadzenie teoretyczne.

1.1. Rodzina protokołów TCP / IP

Podrozdział ten poświęcony zostanie właśnie protokołom TCP/IP – ich charakterystyce, zastosowaniu i miejscu w hierarchii współczesnej informatyki w kontekście sieci komputerowych i usług internetowych.

1.1.1. Architektura protokołów

Architektura protokołów opisuje zestaw protokołów, który został opracowany w celu umożliwienia komunikacji między różnymi typami systemów komputerowych, jak również między różnymi sieciami. Już w 1973 roku agencje DARPA oraz Stanford University rozpoczęły pracę nad protokołem TCP. Efektem tego (trwającego 5lat) okresu badań było opracowanie dwóch wzajemnie uzupełniających się protokołów: protokołu połączeniowego TCP i protokołu bezpołączeniowego IP (stąd też właśnie bierze się nazwa TCP/IP). Protokoły TCP/IP są wykorzystywane w systemach UNIX-owych, sieciach lokalnych i sieciach rozległych. Służą one do łączenia oddzielnych fizycznie sieci w jedną całość - sieć logiczną.

Do najistotniejszych zalet protokołów TCP/IP można tu zaliczyć:

- otwartość i niezależność od specyfikacji sprzętowo-programowej systemów komputerowych.
- możliwość integracji wielu różnych rodzajów sieci komputerowych.
- wspólny schemat adresacji pozwalający na jednoznaczne zaadresowanie każdego użytkownika.
- istnienie standardowych protokołów warstw wyższych .

Protokoły TCP/IP to dzisiaj cały zestaw protokołów przeznaczonych do:

- transferu danych: IP, TCP, UDP (User Datagram Protocol).
- kontroli poprawności połączeń: ICMP (Internet Control Message Protocol).
- zarządzania siecią: SNMP (Simple Network Management Protocol).
- zdalnego włączania się do sieci: TELNET.
- usług aplikacyjnych typu przesyłania plików: FTP (File Transfer Protocol).

Architektura protokołów TCP/IP różni się nieznacznie od modelu ISO/OSI. Spotykamy się tutaj do z czterowarstwowym hierarchicznym modelem protokołów TCP/IP. Dane generowane przez programy aplikacyjne są przekazywane w dół stosu jeśli mają być przesyłane poprzez sieć i w górę stosu przy odbiorze. Zaś każda warstwa stosu dodaje do danych przekazywanych z warstwy wyższej informacje sterujące w postaci nagłówków. Nagłówek bowiem dodany w warstwie wyższej jest traktowany jako dane w warstwie niższej.

Warstwy protokołów TCP/IP mogą używać różnych nazw do określania przekazywanych danych. Aplikacje, które stosują w warstwie transportowej protokół TCP nazywają swoje dane strumieniem. Zaś TCP określa swoje dane nazwą segmentu. Aplikacje wykorzystujące w warstwie transportowej protokół UDP definiują swoje dane jako wiadomości, a dane protokołu UDP to pakiety. W warstwie Internet protokół IP traktuje swoje dane jako bloki zwane datagramami. W najniższej warstwie bloki danych to ramki lub pakiety w zależności od używanego protokołu.

Protokoły TCP/IP wyróżniają dwa typy urządzeń sieciowych: routery (lub gatewaye) oraz hosty (czyli komputery). Routery służą do przesyłania pakietów między sieciami (TCP/IP), a na hostach instalowane jest oprogramowanie aplikacyjne użytkowników.

Aplikacja, która korzysta z protokołów TCP/IP jest musi być identyfikowana za pomocą numeru portu, a protokoły transportowe są określone za pomocą numerów protokołów. W prosty sposób pozwala to łączyć dane generowane przez różne aplikacje z kilkoma protokołami transportowymi i z kolei te protokoły z protokołem IP. Takie rozwiązanie daje możliwość multipleksacji danych, czyli np. umożliwia równoczesną komunikację wielu aplikacji z TCP. W Internecie niektóre numery portów są zarezerwowane i wstępnie przypisane do usług takich jak protokoły sieciowe: FTP lub TELNET. (mogą przyjmować numery z zakresu 0 do 255). Protokoły TCP/IP używają również abstrakcyjnego pojęcia gniazda, czyli kombinacji adresu IP i numeru portu. W związku z tym gniazdo jednoznacznie określa proces w Internecie jak również jest zakończeniem logicznego łącza komunikacyjnego między dwiema aplikacjami. Jeśli aplikacje realizowane są na dwóch różnych komputerach, to para odpowiadających im gniazd definiuje połączenie w protokole połączeniowym TCP [7].

1.1.2. Protokół IP.

Jest to protokół bezpołączeniowy, co oznacza, że sprawdza on poprawności dostarczenia datagramów do miejsc przeznaczenia. Do podstawowych funkcji protokołu IP możemy zaliczyć:

- określenie struktury datagramu.
- określenie schematu adresacji.
- kierowanie ruchem datagramów w sieci.
- dokonywanie fragmentacji datagramu i odtwarzanie z fragmentów oryginalnego datagramu.

Protokół IP jest protokołem przeznaczonym do działania w sieci z komutacją pakietów. Właśnie pakiet ten jest przez IP określany w/w już nazwą datagram. Każdy datagram jest podstawową, samodzielną jednostką przesyłaną w sieci na poziomie warstwy Internet, który może być adresowany do pojedynczych węzłów lub do wielu węzłów. W przesyłaniu datagramów poprzez sieci uczestniczą routery (węzły sieci), które określają dla każdego datagramu trasę od węzła źródłowego do węzła docelowego. Jednak w różnych sieciach mogą być ustalone różne maksymalne długości datagramów, więc w zależności od potrzeb, datagram może być podzielony na kilka mniejszych części, tzn. na kilka datagramów za pomocą operacji fragmentacji datagramów. Format każdego fragmentu jest taki sam jak format każdego innego niepodzielnego datagramu. Konieczność fragmentacji datagramu może być również powodowana przez przesyłanie datagramów przez sieci rozległe dopuszczające inne protokoły i inne długości pakietów, np. dla sieci X.25, gdzie pakiety mają maksymalną długośc 128 bajtów. Kompletowanie pierwotnego datagramu z fragmentów dokonuje się w komputerze docelowym [7].

1.1.3. Adresy IP.

Obecnie protokoły TCP/IP wykorzystywane w sieciach, gdzie stosowane są 32-bitowe adresy jednoznacznie określają sieć oraz komputer dołączony do tej sieci. Taki adres IP składa się z dwóch części: sieciowej i identyfikującej komputer wewnątrz sieci. Adresy IP można sklasyfikować wg ich formatów, a wzajemna relacja między liczbą bitów określających sieć i liczbą bitów określających komputer zależy od klasy adresów, których jest 5 (A, B, C, D, E). Adresy IP są zapisywane jako 4 liczby w systemie dziesiętnym oddzielone kropkami, np. 123.65.101.0. Cyfry te odpowiadają liczbom dwójkowym zawartym w kolejnych czterech bajtach adresu IP, czyli należą do przedziału [0,255]. Dzięki adresom IP możliwe jest stworzenie sieci logicznych w jedną całość - dużą sieć fizyczną posiadającą jeden adres IP. By tego dokonać należy skorzystać z bitów części identyfikującej komputer w adresie IP oraz 32-bitowej maski podsieci. Budowa maski jest następująca: bit o wartość 1 odpowiada bitowi w adresie IP i jest bitem części sieciowej, natomiast w przypadku gdy ten sam bit jest ustawiony na wartość 0, to bit adresu należy do części określającej komputer. Tu właśnie pozanjemy pojęcia netid (network ID – określenie sieci) i hostid (host ID – określenie węzła sieciowego). Obecnie podstawową niedogodnością sieci Internet jest nieustanna redukcja puli adresów IP - praktycznie nie ma już większych możliwości adresowania w klasach A i B. Rozwiązaniem może być propozycja nowego protokołu IP v6, powstającego według idei z roku 1994 IPNextGeneration. Pozbywa się ona dotychczasowego ograniczenia rozciągając dotychczasowe 32-bitowe adresy do 128 bitów. Oczywiście zakłada się, że nowe adresy obejmą aktualnie używane (32-bitowe)[7].

1.1.4. Protokół ICMP. (Internet Control Message Protocol).

Protokół ten jest ściśle związany z protokołem IP i jego częścią warstwy internet, lecz ponieważ IP jako protokół bezpołączeniowy nie posiada on mechanizmów informowania o błędach dlatego wprowadzony został właśnie protokół ICMP, który umożliwia już przesyłanie między komputerami lub routerami także informacji o błędach występujących w funkcjonowaniu sieci IP np.:

- brak możliwości dostarczenia datagramu do miejsca przeznaczenia.
- zmiana wcześniej wyznaczonej trasy przez jeden z pośredniczących routerów.
- brak wolnej pamięci buforowej dla zapamiętania datagramu.

Informacje o tych zaburzeniach w działaniu sieci noszą nazwę komunikatów. Komunikaty protokołu ICMP są przesyłane wewnątrz datagramów IP. Każdy z nich ma własny format. Jednak wszystkie rozpoczynają się takimi samymi polami: typ, kod oraz suma kontrolna. Dalsze pola zależą od typu komunikatu ICMP. Pole *typ* określa rodzaj komunikatu, a pole *kod* opisuje kod błędu. W polu *suma kontrolna* zawarte jest 16-bitowe jedynkowe uzupełnienie sumy komunikatu ICMP. Pole *wskaźnik* określa bajt, w którym wystąpił błąd, natomiast pole *informacja* zawiera nagłówek oraz pierwsze 64 bity datagramu IP, w którym wykryto błąd. Protokół ICMP posługuje się 12 komunikatami, które są wymieniane między routerami i / lub komputerami [7].

1.1.5. Protokół TCP.

Jest to protokół zorientowany połączeniowo, czyli umożliwia zestawienie połączenia w którym efektywnie i niezawodnie przesyłane są dane. Połączenie to charakteryzuje się możliwością sterowania przepływem, potwierdzania odbioru, zachowania kolejności danych, kontroli błędów i przeprowadzania retransmisji. Blok danych wymieniany między współpracującymi komputerami nosi nazwę segmentu (nagłówek + dane).

Ponieważ TCP jest protokołem zorientowanym połączeniowo, więc e celu przesłania danych między dwoma modułami TCP, zainstalowanymi w różnych komputerach, konieczne jest ustanowienie, utrzymanie i rozłączenie połączenia wirtualnego. Po ustanowieniu połączenie wirtualnego między dwoma modułami TCP mogą zostać przesyłane segmenty z danymi. Segmenty te mogą być przesyłane tym połączeniem w obu kierunkach, ponieważ TCP umożliwia transfer danych między dwoma modułami w trybie dupleksowym. Dla zapewnienia niezawodnej transmisji TCP wykorzystuje sekwencyjną numerację bajtów oraz mechanizm pozytywnych potwierdzeń z retransmisją. Numer sekwencyjny przypisany do każdego przesyłanego bajtu danych pozwala na jego jednoznaczną identyfikację, a także jest używany w mechanizmie przesyłania potwierdzeń. Odbywa się to przez wskazanie ile bajtów odbiorczy moduł TCP jest w stanie zaakceptować. Liczba akceptowanych bajtów określona jest w polu *okno* w nagłówku segmentu przesyłanego do nadawczego modułu TCP. Liczba ta może być zmieniana w trakcie trwania połączenia wirtualnego.

TCP realizuje również koncepcję funkcji wymuszającej. Operacja ta jest realizowana wtedy, gdy aplikacja chce mieć pewność, że wszystkie dane przekazane przez nią do modułu TCP zostały wysłane. W odpowiedzi na żądanie aplikacji, moduł TCP wysyła wszystkie dane znajdujące się w buforach w postaci jednego lub kilku segmentów do odbiorczego modułu TCP. Po przesłaniu danych następuje rozłączenie połączenia wirtualnego. Należy tu przypomnieć, że moduł TCP w celu przesyłania segmentu przez sieć przekazuje go do warstwy internet. Tam jest on umieszczany w wewnątrz datagramu, czyli inaczej segment jest uzupełniany o nagłówek datagramu IP. Z kolei protokół IP przekazuje ten datagram do warstwy dostępu do sieci, gdzie po obudowaniu o kolejny nagłówek tworzona jest ramka przesyłana przez sieć [7].

1.1.6. Protokół UDP.

Protokół UDP (User Datagram Protocol) - jest to protokół bezpołączeniowy, nie posiadający mechanizmów sprawdzających poprawność dostarczenia danych. Protokół UDP został opracowany w celu stworzenia aplikacjom możliwości bezpośredniego korzystania z usług IP. Pozwala on aplikacjom na dołączanie do datagramów IP adresów portów komunikujących się aplikacji.

Protokół UDP jest wykorzystywany w sytuacjach, gdy przesyłamy niewielką liczbę danych. Również protokół ten mogą używać aplikacje działające według modelu zapytanie-odpowiedź. Ogólnie możemy powiedzieć, że UDP może być z powodzeniem używany tam gdzie nie są wymagane usługi protokołu UDP [7].

2. „U CELU" – Czyli czym dokładnie jest BGP

2.1. BGP- jako reprezentant rodziny protokołów reguł doboru tras i transmisji szeregowej.

W sieciach TCP/IP routery (gatewaye) spełniają ważną rolę w zakresie kierowania ruchem datagramów. Ruch ten może odbywać się zarówno wewnątrz sieci jak i dotyczyć wymiany informacji między różnymi sieciami. Ponieważ protokół IP nie określa sposobu kierowania ruchem wewnątrz sieci i między sieciami, a zatem opracowano dla tych celów różne protokoły reguł doboru tras. Protokoły te mają za zadanie przede wszystkim przygotować informacje niezbędne do budowy tablic kierunków w routerach (gatewayach).

Dynamiczne protokoły rutowania można sklasyfikować na kilka sposobów. Pierwszy i chyba najważniejszy związany jest z tym, jaką część sieci protokół obejmuje swym zasięgiem. Wyróżnić tutaj możemy :

- Protokoły *zewnętrzne* (*Exterior Gateway Protocols*);
- Protokoły *wewnętrzne* (*Interior Gateway Protocols*).

Protokół klasyfikowany jako zewnętrzny odpowiada za wymianę informacji o rutingu pomiędzy dwiema niezależnymi domenami administracyjnymi, zwanymi często systemami autonomicznymi.

Najpopularniejszym obecnie protokołem rutingu, wykorzystywanym pomiędzy systemami autonomicznymi jest **BGP** (*Border Gateway Protocol*). Charakterystyczną cechą protokołów zewnętrznych jest ich dobra skalowalność i przystosowanie do obsługi dużych sieci. Składają się zwykle z wielu podprotokołów, a ich implementacja jest dość skomplikowana [2].

BGP jest protokołem wykonującym (we współczesnych sieciach) zadania związane z wyborem ścieżek dla ruchu międzydomenowego, oraz rozwiązuje problemy skalowalności Internetu. Ponadto protokół **BGP** wykonuje routing międzydomenowy w sieciach pracujących z protokołem TCP/IP. Należy do klasy protokołów zewnętrznych. Wykonuje 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* (*Exterior Gateway Protocol*) – (patrz szczegóły 2.2.1.)

Routery zewnętrzne pracujące z protokołem BGP podobnie jak routery z protokołem EGP, wymieniają informację o dostępności systemów autonomicznych. Ponadto przesyłane są atrybuty trasy takie jak koszty czy też zabezpieczenia przed niepowołanym dostępem. Atrybuty te również mogą zawierać informacje służące do wyboru tras na podstawie wymagań administracyjnych (nietechnicznych), np. związanych z bezpieczeństwem datagramów. Na podstawie otrzymanych informacji protokół BGP wybiera najkrótszą trasę. Informacje wymieniane są jedynie przyrostowo, a nie przez przesyłanie całej bazy danych dotyczącej zewnętrznej reguły doboru tras, zatem protokół ten nie powoduje dużego przyrostu ruchu w sieci [4].

Protokół BGP otwiera perspektywę przekazywania pakietów z danymi użytkowymi pomiędzy odległymi lokalizacjami między innymi pomiędzy dużymi systemami zarządzanymi przez operatorów sieci, zwanymi systemami autonomicznymi (są to systemy typu „transit", „multihomed" i „stub"). Każdy system autonomiczny jest rejestrowany przez organizację InterNIC, gdzie przydzielany jest mu odpowiedni numer. Numery te są wykorzystywane podczas konfigurowania ruterów dla BGP.

W systemie autonomicznym jeden lub więcej ruterów, które zostają skonfigurowane do obsługi BGP, stają się *speakerami* BGP (reprezentantami pozostałych ruterów i sieci tworzących system autonomiczny). *Speakery* wiedzą wszystko o konfiguracji sieci w ramach AS. Odbierają także komunikaty aktualizujące ruting z danymi o sieciach z innych systemów autonomicznych. Przekazują swoim partnerom aktualizacje rutingu zarówno sieci wewnętrznych jak i sieci z innych AS.

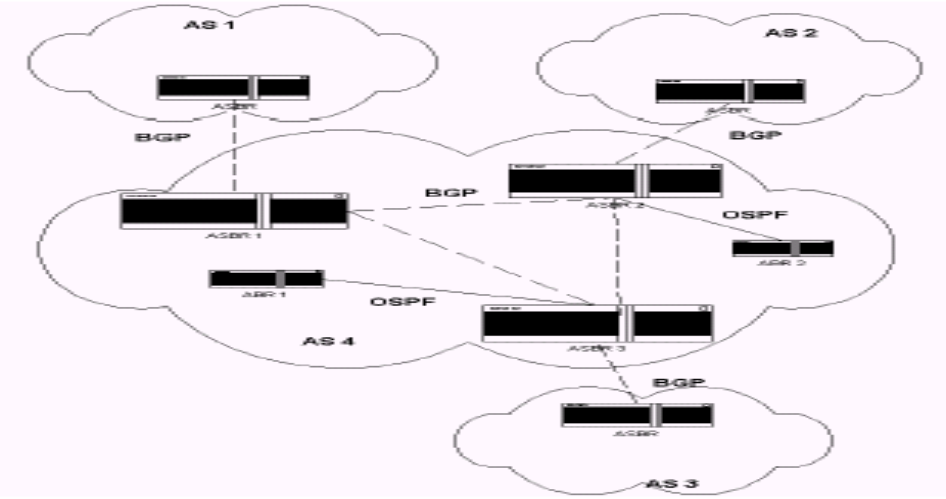
Dowolne rutery skonfigurowane do obsługi BGP wymieniające aktualizacje rutingu nazywane są *BGP peers* (partnerzy BGP). Ruter BGP pozyskuje dane o swoich sąsiadach za pomocą protokołu TCP korzystając z powszechnie znanego portu o numerze 179. Adresy IP oraz numery systemów autonomicznych ze wszystkich partnerskich ruterów BGP, które konfigurowany ruter będzie dostrzegał, muszą być wyspecyfikowane za pomocą polecenia konfiguracyjnego „*neighbor“*. Po nawiązaniu połączenia TCP pomiędzy partnerami BGP do wzajemnego komunikowania wykorzystywane są 4 rodzaje komunikatów: *open, update, keepalive* i *notification.* Najbardziej użytecznym jest *update*, który służy do przekazywania informacji o rutingu. Komunikaty *open* i *keepalive* wykorzystywane są do nawiązania i utrzymywania sesji BGP. Komunikat *notification* służy do powiadamiania o błędnych warunkach pomiędzy partnerskimi BGP.

Partnerzy BGP mogą być zarówno wewnętrzni jak i zewnętrzni. Wewnętrzni partnerzy budują (nawiązują) sesję w ramach jednego systemu autonomicznego, a partnerzy zewnętrzni to rutery należące do różnych systemów autonomicznych.

Protokół BGP posiada możliwość realizacji następujących funkcji:

- agregacji tras;
- egzekwowania reguł różnej polityki rutingu dla różnych systemów autonomicznych;
- poprawy skalowalności poprzez wykorzystanie dla tras reflektorów i konfederacji;
- współdziałanie z protokołami IGP poprzez redystrybucję i synchronizację.

Agregacja tras jest realizowana podobnie jak dla protokołu OSPF, z tą różnicą, że dla BGP zagregowane adresy sieci i ich maski wyznaczane są na poziomie systemu autonomicznego, a nie obszaru. Dzięki funkcji agregacji tras można zredukować liczbę tras (sieci) w ramach systemów autonomicznych, które rutery BGP będą ogłaszać dla swoich zewnętrznych partnerów. Proces BGP pracujący na ruterze musi być specjalnie poinformowany poprzez odpowiednie polecenia konfiguracyjne, że ma obsługiwać agregację tras. Koncepcja agregacji tras jest bardzo prosta, aczkolwiek szczegóły implementacji i opcje konfiguracyjne są bardzo złożone. Pomiędzy procesami realizującymi różne protokoły rutingu możliwa jest redystrybucja tras. Można tutaj dystrybuować trasy statyczne zapisane w tabelach tras rutera (redystrybucja statyczna) jak i trasy otrzymywane od innych ruterów i różnych protokołów rutingu (redystrybucja dynamiczna). Redystrybucja dynamiczna polega na zleceniu procesowi BGP akceptacji tras zgłaszanych przez protokół typu IGP (RIP, OSPF, IGRP...). Wymaga to jednak takiego skonfigurowania procesu IGP, aby dystrybuował on swoje trasy dla BGP. Możliwa jest wzajemna redystrybucja tras, zarówno statyczna jak i dynamiczna, pomiędzy protokołami BGP a IGP. Na rysunku 1 umieszczonym na kolejnej stronie przedstawiony został przykład środowiska, w którym możliwe jest zastosowanie redystrybucji statycznej i dynamicznej między protokołami OSPF i BGP. Liniami ciągłymi zaznaczone zostały sesje BGP, liniami przerywanymi sesje OSPF. Jak widać, na ruterach ASBR (*Autonomous System Border Router*) powinny być uruchomione dwa procesy: OSPF i BGP. Podstawowy przepływ danych o osiągalnych sieciach dokonuje się z IGP (tutaj procesu OSPF) do BGP. Proces BGP uruchomiony na ASBR dowiaduje się o sieciach w systemie AS za pomocą redystrybucji statycznej, dynamicznej lub za pomocą odpowiedniego polecenia konfiguracyjnego (np. *network*, udostępnianego przez system siecioy IOS Cisco).

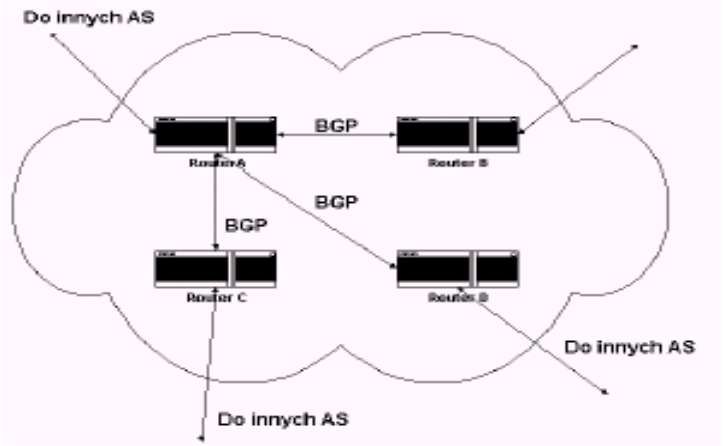


Rys. 2.1.1. Routing OSFP i BGP wewnątrz systemu autonomicznego [2]

W przypadku jakiejkolwiek niestabilności w pracy sieci obsługiwanych np. przez protokół OSPF dane o trasach redystrybuowane są w sposób dynamiczny. Jakakolwiek zmiana w trasach OSPF powoduje wygenerowanie danych do aktualizacji dla BGP. Poziom ruchu w sieci staje się w tym momencie znaczny. Scenariusz ten nosi nazwę „trzepotania tras". Jedynym sposobem uniknięcia trzepotania tras jest redystrybucja statyczna. Jeśli wewnątrz AS znajduje się bardzo dużo sieci OSPF dostarczanie informacji o każdej z nich do zewnętrznego rutera BGP jest niepożądane. Sytuacja ta kwalifikuje się do przedstawienia tych sieci za pomocą metody agregacji tras.

Aby rutery BGP mogły komunikować się ze sobą muszą być skonfigurowane jako sąsiedzkie. Liczba sesji TCP w ruterach przy konfiguracji połączeń typu każdy z każdym (tzw. „full-meshed") może być znaczna. Aby zminimalizować liczbę sesji stosuje się metodę odzwierciedlania tras i metodę konfederowania .

Odzwierciedlanie tras jest techniką podobną do stosowania rutera desygnowanego. Poniżej rysunek 2 przedstawia powiązania między ruterami BGP przy zastosowaniu odzwierciedlania tras.



Rys. 2.1.2. Technika odzwierciedlania tras w BGP [2]

Zakłada się, że Ruter A jest skonfigurowany do pełnienia roli zwierciadła tras i przyjmuje zewnętrzne dane aktualizacyjne BGP. Rozpowszechnia je do wszystkich swoich partnerów. Jeśli inny ruter zostanie skonfigurowany jako klient zwierciadła, będzie przesyłał dane aktualizacyjne tylko do rutera odzwierciedlającego. Ten zaś odbije (ponownie ogłosi) je do swoich partnerów. Redukowana w ten sposób jest liczba sesji BGP. Grupa ruterów skonfigurowana do uczestnictwa w odzwierciedlaniu tras nazywana jest „klastrem".

Inną metodą redukowania wzajemnych powiązań wewnętrznych BGP w ramach systemu AS zawierającego dużą liczbę speakerów są „konfederacje". W metodzie tej poszczególne speakery grupuje się w mini-ASy. Konfederacje BGP definiowane są za pomocą poleceń konfiguracyjnych ruterów. BGP jest protokołem typu *path-vector*. Ścieżka odnosi się do serii kroków, które muszą być podjęte pomiędzy punktem początkowym, a docelowym. Ścieżka BGP jest więc serią liczb z numerami AS, przez które będą przechodzić pakiety, aby dotrzeć do miejsca przeznaczenia. Kompletny opis ścieżki dokonywany jest poprzez zestawienie jej atrybutów, co nie będzie tutaj omawiane. Atrybuty ścieżek przenoszone są w komunikatach aktualizacyjnych (update messages), wymienianych między speakerami BGP [2].

2.1.1. Opis działania protokołu BGP

Przy wyborze optymalnej trasy protokół BGP posługuje się algorytmem *distance-vector*. W trakcie inicjacji połączenia równorzędne routery BGP wymieniają kompletne kopie swoich tablic routingu, które mogą być obszerne. Jednak wtedy wymieniane są tylko zmiany (*delty*), co sprawia, że długie sesje BGP są bardziej efektywne od krótkich.

2.1.2. Routing protokołu BGP

Jedną z najważniejszych funkcji protokołu BGP jest wykrywanie pętli na poziomie systemu autonomicznego.

Protokół BGP wykonuje trzy typy routingu:

1. 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;

2. Na zewnątrz systemów autonomicznych - między dwoma lub większą liczbą routerów w różnych systemach autonomicznych;

3. Przez systemy autonomiczne - między dwoma lub większą liczbą routerów BGP, które wymieniają ruch przez system autonomiczny, nie obsługujący protokołu BGP.

Podobnie jak każdy protokół routingu, BGP utrzymuje tablice routingu, przesyła aktualnienia routingu i podejmuje decyzje o trasie kierowania ruchu, opierając się na miarach routingu. Główną funkcją systemu BGP jest wymiana z innymi systemami BGP informacji o dostępności sieci, w tym informacji o ścieżkach systemów autonomicznych. Informacja ta jest niezbędna do konstrukcji grafu połączeń systemów autonomicznych, z którego można eliminować pętle i wprowadzać w życie strategiczne decyzje z poziomu systemów autonomicznych [4].

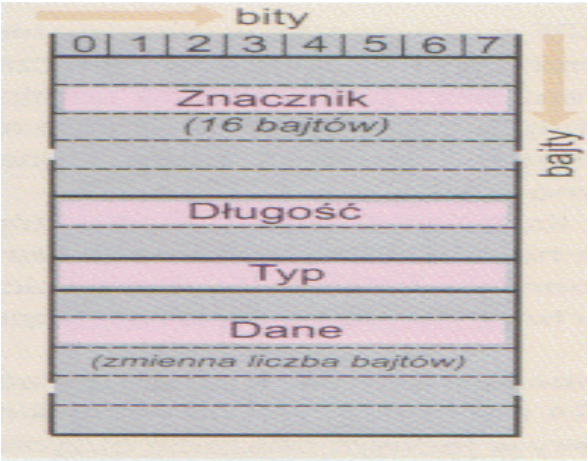
Każdy router utrzymuje tablicę routingu, zawierającą wszystkie możliwe ścieżki do poszczególnych sieci. Jednak router nie odświeża tej tablicy. Zamiast tego informacja o routingu, otrzymana od równorzędnego routera, jest przechowywana do czasu, gdy zostanie odebrane przyrostowe uaktualnienie.

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 [3].

2.1.3. Rodzaje komunikatów protokołu BGP

Wszystkie komunikaty protokołu BGP mają nagłówek podstawowy pakietu - rysunek 2.1.3.1. przedstawia format nagłówka pakietu BGP (Header Format).



Rys. 2.1.3.1. Format nagłówka pakietu BGP [8].

Nagłówki komunikatu otwierającego, uaktualniającego i zgłoszeniowego mają dodatkowe pola; komunikat podtrzymujący ma tylko nagłówek podstawowy pakietu.

Opis głównych pól rysunku 2.1.3.1. - jest następujący:

Znacznik - zawiera wartość autoryzacji, którą może przewidzieć odbiorca komunikatu.

Długość - wskazuje całkowitą długość komunikatu w bajtach.

Typ - określa rodzaj komunikatu.

Dane - zawiera informacje warstwy wyższej (pole opcjonalne) [8].

Definiuje się tu w/w cztery typy komunikatów: otwierający, uaktualniający, zgłoszeniowy i podtrzymujący.

1) Komunikat otwierający (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 [3].

Rys. 2.1.3.2. Format komunikatu otwierającego [8].

Opis pól rysunku 2.1.3.2.:

Wersja - dostarcza numer wersji protokołu (aktualna wersja to 4).

Mój system autonomiczny - dostarcza numer systemu autonomicznego nadawcy.

Czas utrzymania – wskazuje maksymalną liczbą sekund, które mogą upłynąć bez otrzymania komunikatu nadający zostanie uznany za niedziałającego.

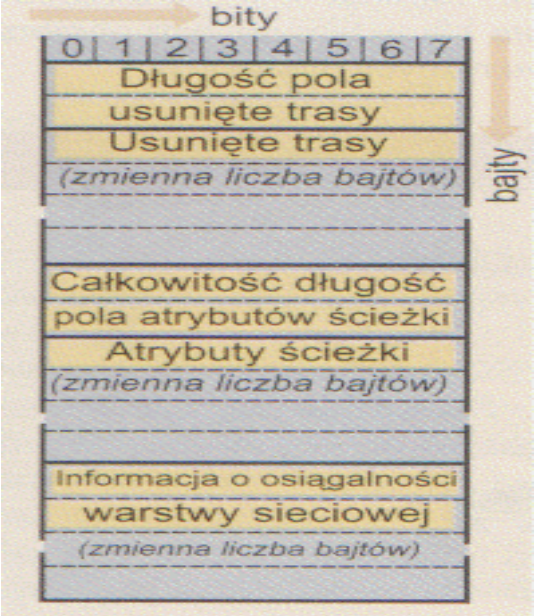
Identyfikator BGP – dostarcza identyfikator BGP nadawcy (adres IP), który jest określony przy inicjacji i jest taki sam dla wszystkich lokalnych interfejsów i wszystkich równorzędnych partnerów BGP.

Długość parametrów opcjonalnych – wskazuje całkowitą długość pola parametrów opcjonalnych (w bajtach). Jeśli wartość tego pola jest równa 0, oznacza to, że pole parametrów opcjonalnych jest niewykorzystane.

Parametry opcjonalne – pole to może zawierać listę parametrów opcjonalnych. Każdy parametr jest zakodowany jako uporządkowana trójka <typ parametru, długość parametru, wartość parametru>. Dotychczas zdefiniowano tylko informację autoryzującą (parametr typu 1). Składa się ona z 2 pól:

- Kod autoryzacji – wskazuje użyty mechanizm autoryzacji.
- Dane autoryzacji – forma i znaczenia tego pola [8].

2) Komunikat uaktualniający (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 (Transmission Control Protocol). Komunikaty otwierające mogą wycofywać z tablicy routingu jedną lub więcej niewykonalnych tras i podczas ich wycofywania zgłaszać nowe [3].



Rys. 2.1.3.3. Format komunikatu uaktualniającego [8].

Opis pól rysunku 2.1.3.3.:

Długość pola nieosiągalnych tras – wskazuje całkowitą długość pola usuniętych tras. Wartość 0 tego pola wskazuje, że żadna trasa nie została usunięta i nie ma tego pola w komunikacie.

Nieosiągalne trasy – wskazuje całkowitą długość pola usuniętych tras lub nie wykorzystanie tego pola (wartość 0).

Usunięte trasy – zawiera listę prefiksów adresów IP tras, które są niedostępne.

Całkowita długość pola atrybutów ścieżki – wskazuje całkowita długość pola atrybutów ścieżki lub niewykorzystanie tego pola (wartość 0).

Atrybuty ścieżki – pole o zmiennej długości znajduje się w każdym komunikacie uaktualniającym. Każdy atrybut ścieżki jest uporządkowaną trójką o zmiennej długości: <typ atrybutu, długość atrybutu, wartość artybutu>.

Informacja o dostępności warstwy sieciowej – to pole o zmiennej długości zawiera liste prefiksów adresów IP dla zgłoszonych tras [8].

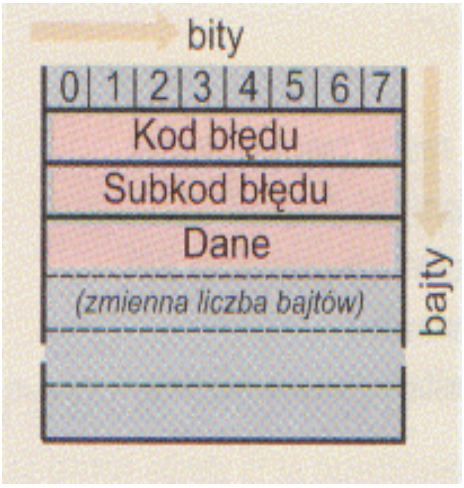
3) Komunikat zgłoszeniowy (notification message) jest wysyłany w przypadku wykrycia błędu. Zgłoszenia są używane do zamykania i otwierania sesji i informowania wszystkich przyłączonych routerów o przyczynie zamknięcia sesji [3].

Opis pól do rysunku 2.1.3.4. - zamieszczonego na kolejnej stronie:

Kod błędu – wskazuje typ błędu, który wystąpił. Pole to definiuje różne typy błędów.

Subkod błędu – dostarcza dokładniejszej informacji charakteryzującej wykazywany błąd.

Dane o błędzie – dostarcza dane oparte na polach kodu błędu i subskodu błędu. Pole to jest wykorzystywane do ustalenia przyczyn pojawienia się komunikatu zgłoszeniowego [8].



Rys. 2.1.3.4. Format komunikatu zgłoszeniowego [8].

4) Komunikat podtrzymujący (keep-alive message) powiadamia równorzędne routery BGP o tym, że router jest aktywny. Częstotliwość wysyłania komunikatu jest dobrana tak, aby zapobiec wygaszeniu sesji [3].

2.1.4. Wykorzystanie BGP

Użytkownicy Sieci rzadko myślą o systemach i urządzeniach infrastruktury, które umożliwiają właściwe działanie Internetu. Szybki rozwój Sieci wymusił zmiany w organizacji dostępu do poszczególnych komputerów. Sposoby organizacji tego dostępu to właśnie istotność protokoły routingu

Obecnie najbardziej zaawansowanym rozwiązaniem jest właśnie protokół BGP 4, który spełnia rolę protokołu uniwersalnego, który można wykorzystać do budowy tablic routingu wewnętrznego w systemie autonomicznym (IBGP) oraz ścieżek routingu pomiędzy dostawcami (EBGP). Rozróżnienie to jest umowne, stosowne do aktualnego obszaru działania protokołu.

Dane pochodzące z ubiegłego roku informują o ówczesnej dbywającej się instalacji najnowszych routerów Ericsson AXI 580 w sieci szkieletowej Polpak-T. Z informacji uzyskanych od zastępcy dyrektora TP SA ds. usług i marketingu, protokół BGP 4+ jest dostępny praktycznie w całej sieci Polpak już od w listopadzie tego roku. Jednocześnie przypomniał, że protokół wymaga nieprzerwanych sesji łączności routerów sąsiadujących ze sobą przerwa lub zakłócenie łączności powoduje, że domena może "zniknąć" z sieci, a jej odtwarzanie w skali globalnej może trwać nawet dwie doby [6].

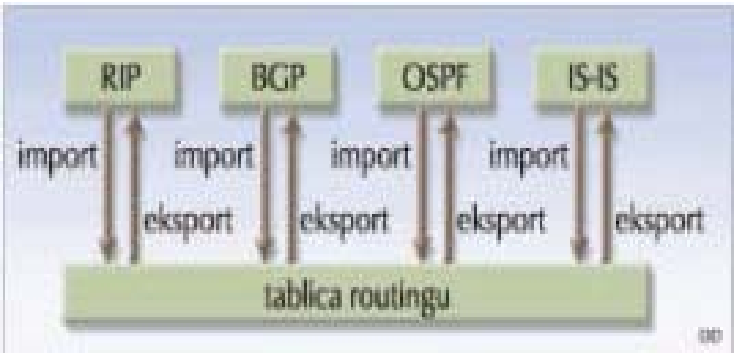
Routery BGP 4 definiują sesje sąsiedzkie, które wykorzystując standardowy TCP, służą do wymiany informacji o trasach sieciowych i ścieżkach w systemach autonomicznych. Routery takie nazywamy równorzędnymi, a sesja TCP trwa do chwili zerwania połączenia fizycznego. Po nawiązaniu połączenia routery wymieniają między sobą całe tablice routingu. W stosunku do dawniejszych IGP wprowadzono mechanizmy numerowania wersji tablic, co umożliwia ich aktualizację przez wymianę informacji różnicowych. Dzięki temu wszystkie routery równorzędne synchronizują się praktycznie natychmiast.

Bardzo ważną cechą BGP jest to, że ogłasza tylko trasę najlepszą, ale w osobnej tablicy przechowuje trasy zapasowe. Protokół BGP optymalizuje trasę na podstawie długości ścieżek do systemu docelowego, ale umożliwia także arbitralny wybór drogi [5].

2.1.5. Organizacja sieci z BGP

Każdy system autonomiczny musi mieć swój unikalny identyfikator ASN (Autonomic System Number), nadawany przez organizacje RIPE, APNIC lub ARIN. Numer ten jest identyfikatorem wszystkich routerów BGP danego systemu. Powielenie numeru na zewnątrz grozi wyłączeniem dużych obszarów sieci ze względu na wewnętrzne zabezpieczenia protokołu przed zapętleniem. Dla routerów BGP w sieciach prywatnych, niepołączonych z Internetem, wykorzystuje się numery z zakresu 32768- 64511. Elementem usprawniania działania sieci jest możliwość filtracji rozgłaszanych sieci, tak aby kierować połączenia na różne interfejsy fizyczne do różnych routerów fizycznych. Podobnie można wybrać i pogrupować informacje o trasach, które są rozgłaszane do poszczególnych routerów.

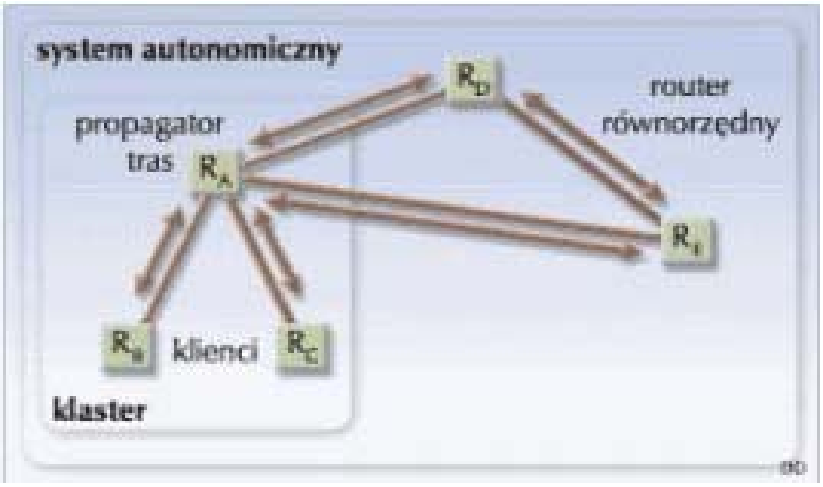
Możliwość tworzenie tablic routingu przez różne protokoły.
W systemach autonomicznych routery BGP mogą tworzyć konfederacje, które zmniejszają ruch wewnątrz systemu, tworząc automatycznie subsystemy o strukturze pierścieni. Inną metodą zmniejszania ruchu jest hierarchiczna konfiguracja routerów w strukturze drzewa nazywana klastrem, gdzie router nadrzędny pełni rolę propagatora tras (Route Reflector), a routery gałęzi nie prowadzą działalności rozgłoszeniowej.



Rys. 2.1.5.1. Tablica routingu z BGP [5].

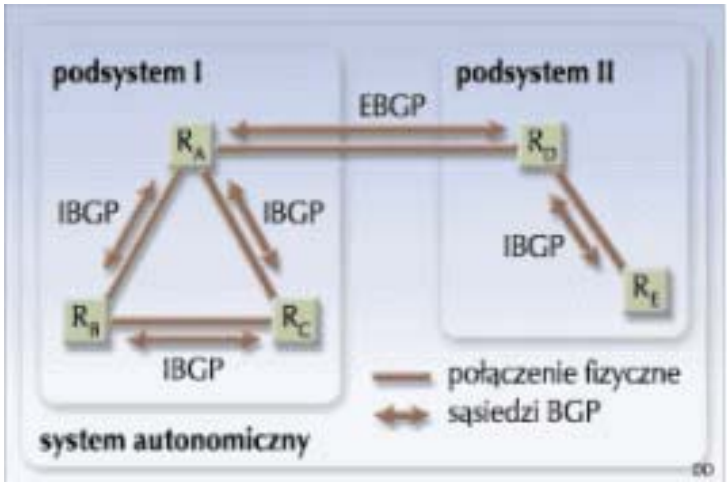
Bardzo interesującą możliwością jest także przekazywanie ruchu BGP poprzez autonomiczny system, który wewnątrz nie obsługuje tego protokołu. W znacznym stopniu można skorzystać z dobrodziejstw BGP, jeżeli firma mająca więcej niż jedno połączenie z Internetem wymieni routery brzegowe na takie, które obsługują BGP 4.

Routery obsługujące BGP 4 są znacznie droższe niż ich poprzednicy. Trzeba pamiętać, że wbudowana funkcjonalność wymaga ogromnej mocy obliczeniowej oraz pamięci do obsługi złożonych funkcji routowania. Bez przesady można stwierdzić, że oprogramowanie routerów jest jednym z najbardziej złożonych współczesnych zagadnień programistycznych. Oprogramowanie to musi podejmować decyzje w złożonej i dynamicznie zmieniającej się topologii sieci.



Rys. 2.1.5.2. Propagator tras (Route Reflector) z routerami klienckimi i równorzędnymi [5].

Routing BGP wymaga, aby inne routery sieci także umiały go obsłużyć w miarę rozprzestrzeniania się technologii można będzie z niej korzystać na coraz niższym szczeblu.



Rys. 2.1.5.3. Konfederacja routerów BGP [5] .

W sieciach, które funkcjonują od dawna proces wymiany routerów musi potrwać, nie należy się więc dziwić, że nie nastąpi to jednego dnia jest to bardzo kosztowne i trudne organizacyjnie. Sieci dostawców wchodzących na rynek nie mają tych ułomności zawsze są najnowocześniejsze.

Czy BGP można czymś zastąpić? Teoretycznie tak można stosować stare protokoły, dodatkowe serwery nazw itp. Wymaga to jedynie zwiększania mocy obliczeniowych i pasma na informacje techniczne sieci, niezbędne dla jej funkcjonowania. Rozwój ekstensywny rzadko kończy się sukcesem, lepiej więc stosować rozwiązania "inteligentniejsze", efektywniejsze w działaniu[5].

2.2. Dlaczego właśnie BGP – poznajmy konkurencje".

Pojedyncze sieci są dołączone do routerów łączących je z innymi sieciami. Grupę sieci i routerów administrowanych przez ten sam ośrodek i stanowiących jednolity system wykorzystujący ten sam protokół reguły doboru tras nazywamy systemem autonomicznym lub systemem wewnętrznym lub też domeną. Przykładem takiego systemu autonomicznego może być sieć kampusowa lub sieć wojskowa. Protokoły reguł doboru tras są podzielone na dwie grupy, zależnie od tego w jakim obszarze sieci są wykorzystywane. Protokoły wewnętrznych reguł doboru tras są używane do przesyłania informacji związanych z reguła doboru tras stosowaną wewnątrz systemu autonomicznego, a na potrzeby reguł doboru tras wykorzystywanych do kierowania ruchem między systemami autonomicznymi stosowane są protokoły zewnętrznych reguł doboru tras.

2.2.1. Protokół zewnętrzny.

Protokoły zewnętrznych reguł doboru tras są wykorzystywane do wymiany informacji związanych ze sposobem przesyłania datagramów między systemami autonomicznymi. Do takich protokołów zaliczamy np. protokoły EGP lub omawiany już szczegółowo protokół BGP.

Protokół EGP (Exterior Gateway Protocol) umożliwia wymianę komunikatów między parą sąsiednich routerów zewnętrznych. Router zewnętrzny to taki sam router, który z jednej strony ma możliwość komunikowania się z innymi routerami wewnątrz systemu autonomicznego, a z drugiej z routerami zewnętrznymi innych systemów autonomicznych. System autonomiczny może posiadać jeden lub wiele routerów zewnętrznych.

Każdy router zewnętrzny wymienia informacje związane z wewnętrzną reguła doboru tras z routerami wewnętrznymi systemu autonomicznego korzystają z protokołu wewnętrznej reguły doboru tras. Pozwala to routerowi zewnętrznemu na uzyskanie informacji o adresach komputerów (użytkowników końcowych) znajdujących się w systemie autonomicznym. Ponadto każdy router zewnętrzny wymienia informacje związane z zewnętrzną regułą doboru tras z sąsiednimi routerami zewnętrznymi innych systemów autonomicznych.

Podstawowe procedury wykonywane przez router zewnętrzny pracujący według protokołu AGP to :

- poznanie sąsiada poprzez wymianę specjalnych komunikatów między sąsiednimi routerami zewnętrznymi
- okresowa wymiana informacji związanej z kierowaniem ruchem datagramów między dwoma sąsiednimi routerami zewnętrznymi
- monitorowanie dostępności sąsiednich routerów zewnętrznych realizowane przez wysyłanie odpowiedniego komunikatu i oczekiwanie na odpowiedź. Jeśli po trzykrotnym wysłaniu komunikatu ciągle brak odpowiedzi, to zakłada się, że sąsiedni router zewnętrzny przestał działać i wówczas usuwa się z tablicy kierunków wszystkie prowadzące przez niego trasy.

Router zewnętrzny zwykle utrzymuje dwie tablice kierunków. Jedną dotyczącą kierowania ruchem datagramów wewnątrz systemu autonomicznego i drugą z trasami do innych routerów zewnętrznych. Tablica związana z ruchem datagramów wewnątrz sytemu autonomicznego jest wyznaczana (aktualizowana) z użyciem protokołów wewnętrznych reguł doboru tras, a tablica kierunków dotyczących wymiany datagramów między systemami autonomicznymi jest wyznaczana z użyciem procedur nie definiowanych przez protokół EGP.

2.2.2. Protokoły łączy szeregowych.

Protokoły TCP/IP mogą działać korzystając z wielu różnych mediów transmisyjnych. Jednym z jednych istotniejszych nośników są łącza szeregowe z uwagi na to, że wielu zdalnych użytkowników łączy się z sieciami TCP/IP poprzez np. łącza telefoniczne, a także z uwagi na rozwój sieci rozległych pracujących z protokołami TCP/IP. Te dwa powody wymusiły standaryzację komunikacji TCP/IP poprzez łącza szeregowe, co doprowadziło do powstania dwóch protokołów dla łączy szeregowych SLIP i PPP.

Protokół SLIP (Serial Line IP) został opisany w dokumencie RFC 1055. Umożliwia on asynchroniczny lub synchroniczny transfer danych przez łącza dzierżawione lub komutowane z szybkością transmisji do 19.2 Kb/s. Pozwala łączyć ze sobą komputery, routery i stacje robocze. Protokół SLIP w prosty sposób obudowuje datagramy IP podczas ich przesyłania przez łącza szeregowe. SLIP traktuje dane jako ciąg bajtów i używa następujących dwóch znaków specjalnych do oznaczania końca datagramu:

znak SLIP END (kod 192) oznacza koniec datagramu

znak SLIP ESC (kod 219) wskazujący, że następny znak nie jest znakiem specjalnym protokołu SLIP. W trakcie transmisji może zdarzyć się , że w nadawanym ciągu danych wystąpią sekwencje odpowiadające znakom specjalnym, co oznaczało błędną ich interpretację przez odbiornik. Aby się przed tym zabezpieczyć nadajnik bada wysyłany ciąg bajtów i wstawia dodatkowy znak ESC bezpośrednio przed bajtem odpowiadającym znakowi specjalnemu. Pozwala to zapobiec interpretowaniu przez protokół SLIP bajtu stanowiącego dane jako końca datagramu.

Protokół SLIP może przekazywać datagramy o długości do 1006 bajtów. Nie zawiera on w sobie mechanizmów detekcji i korekcji błędów, a także nie posiada mechanizmów adresowania. Oba komunikujące się systemy muszą znać wzajemnie swoje adresy i mogą przesyłać z użyciem protokołu SLIP wyłącznie datagramy IP. Protokół ten może być wykorzystywany jedynie w transmisji punkt-punkt. Ponadto komunikujące się systemy muszą mieć zainstalowane te same wersje protokołu SLIP.

Wymienione wyżej braki protokołu SLIP nie są istotne dla części zastosowań, a w innych zastosowaniach stanowią wielką przeszkodę. SLIP zaleca się stosować do odległych systemów, komputerów lub stacji roboczych przesyłających wyłącznie datagramy IP, nie zaleca się go stosować w środowisku sieci rozległych do łączenia routerów.

Protokół PPP (Point to Point Protocol) opracowano jako standard przeznaczony do użycia w sieci Internet. Można go również stosować w innych sieciach rozległych (RFC 1171 i 1172). Jest to protokół do transmisji synchronicznej i asynchronicznej po łączach dzierżawionych i komutowanych. Protokół PPP może przenosić pakiety pochodzące od różnych protokołów warstwy sieciowej: IP, IPX, AppleTalk, DECnet, CLNP oraz MAC. Inną właściwością PPP jest posiadanie mechanizmu adresacji IP co pozwala łączyć się zdalnym użytkownikom w dowolnym miejscu sieci, a także ograniczeń co do szybkości transmisji. Datagramy IP lub pakiety innych protokołów są przesyłane wewnątrz ramek protokołu PPP. Struktura tej ramki jest podobna do struktury ramki HDLC z tym, że ramka PPP ma dodatkowe pole określające od jakiego protokołu pochodzą dane zawarte w polu informacyjnym ramki.

2.2.3. Protokoły wewnętrzne.

Przykładami protokołów wewnętrznych reguł doboru tras są protokoły RIP i OSPF.

Protokół RIP (Routing Information Protocol) zaliczamy do kategorii protokołów dystansowo-wektorowych. Protokół ten zwykle wybiera trasy o najmniejszej liczbie "przeskoków", czyli najmniejszej liczbie routerów (węzłów), przez które muszą przejść datagramy na trasie od routera źródłowego do docelowego. Najdłuższa trasa może składać się z co najwyżej piętnastu przeskoków. Jeżeli wyznaczona trasa posiada więcej niż piętnaście przeskoków to protokół RIP przyjmuje, że router docelowy jest nieosiągalny. Z tego powodu protokół ten nie może być stosowany w systemach autonomicznych składających się z dużej liczby routerów.

Decyzje co do wyboru trasy w protokole RIP mogą być podejmowane nie tylko w oparciu o liczbę przeskoków, ale również na podstawie kosztu trasy. Koszt trasy może reprezentować np. opóźnienie, przepustowość trasy lub stopień zabezpieczenia przed niepowołanym dostępem. Decyzja co do dalszej tras datagramu podejmowana jest przez router na podstawie adresu przeznaczenia i tablicy kierunków. Na podstawie informacji otrzymanych od sąsiadów router modyfikuje swoje tablice kierunków. Następnie dla każdego docelowego routera wybierana jest trasa o najmniejszym koszcie. Jeśli otrzymane informacje dotyczą routera docelowego, który dotychczas nie występował w tablicy kierunków to tablica ta jest odpowiednio uzupełniana przez dodanie nowej trasy. Jeśli informacje o routerze docelowym już znajdują się w tablicy kierunków, to jej modyfikacja jest dokonywana tylko wtedy gdy koszt nowej trasy jest mniejszy od kosztu trasy dotychczasowej.

Protokół OSPF (Open Shortest-Path-First) zaliczymy do protokołów stanu połączenia. W porównaniu z protokołami dystansowo-wektorowymi protokoły stanu połączenia wymagają większej mocy obliczeniowej, zapewniają większy stopień kontroli nad procesem kierowania ruchem datagramów w sieci i szybciej dostosowują się do zmian struktury sieci. Protokół OSPF jest przystosowany do pracy w dużych systemach autonomicznych. Każdy router pracujący z protokołem OSPF musi znać strukturę sieci, w której pracuje. W związku z tym wykonuje on dwa podstawowe zadania :

- testowanie stanów sąsiednich routerów i własnych linii wyjściowych w celu potwierdzenia ich sprawności. Wymiana informacji między sąsiednimi routerami jest dokonywana z użyciem protokołu "hello".
- okresowe przesyłanie (rozgłaszanie) informacji o stanie połączeń sąsiednimi routerami do wszystkich routerów pracujących w sieci.

Router, na podstawie otrzymywanych informacji, tworzy graf skierowany będący reprezentacją sieci fizycznej. Ponieważ każdy z routerów pracujących w sieci otrzymuje te same informacje o sieci, więc każdy z nich tworzy ten sam graf. Następnie każdy router wyznacza najkrótszą trasę do każdego innego routera.

Każdy router wewnątrz sytemu autonomicznego do wyznaczania najkrótszych tras korzysta z tych samych danych i stosuje ten sam algorytm, a zatem zapobiega to występowaniu pętli na trasach, po których przesyłane są datagramy. Zapobieganie występowaniu pętli na trasach jest bardzo ważną własnością protokołu OSPF, która między innymi wydatnie zwiększa efektywność działania sieci [7].

MATERIAŁ ŹRÓDŁÓWY

Informacji zawarte powyżej pochodzą z różnych stron internetowych zarówno publikowanych i oferowanych przez Internet Polski jak i Ogólnoświatowy, gdzie były to w większości dokumenty angielskojęzyczne, które zostały przetłumaczone na język polski, oraz z publikacji artykułów dostępnych na rynku wydawniczym.

Oto wykaz pozycji, z których zaczerpnąłem większość danych oraz adresy stron www:

[1] Bruce Hallberg – „Sieci komputerowe – kurs podstawowy" – Wydawnictwo Edition 2000.

[2] Tomasz Malinowski – „Protokoły rutingu dynamicznego**"** BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI - 2001- Zakład Teleinformatyki, Instytut Automatyki i Robotyki WAT, ul Kaliskiego 2, 00-908 Warszawa.

[3] Czasopismo „NetWorld" – (dostępne także: www.networld.com.pl)

[4] „W poszukiwaniu najlepszej trasy" Mariusz Dec - "Pckurier" – 22/2000

[5] "PRO – Magazyn Prawdziwych Interautów" nr 26. - 2002r.

[6] Dostawca usług używający sieci Cisco Powered Network - Polska - Cisco Systems (www.networld.com.pl/)

[7] Amatorska Sieć Komputerowa Skałka.htm - http://asks2001.republika.pl/sieci4.htm

[8] „Vademecum teleinformatyka" – Janusz Chustecki – Warszawa. 1999r