

Qvo vadis pakiecie...

...a dokładniej rzecz ujmując – którądy. Założę się, że przeciętny internauta niezwykle rzadko zadaje sobie pytanie. Zwykłego użytkownika nie interesuje przecież jakimi drogami wędrują informacje pomiędzy jego komputerem a aktualnie przezeń przeglądany serwerem WWW, ftp itd. On po prostu wpisuje adres i czeka aż odpowiednie mechanizmy zaimplementowane w oprogramowaniu i sprzęcie wyślą jego zapytanie pod odpowiedni adres i dostarczą mu odpowiedź.

Na co dzień traktujemy całą procedurę odnajdywania i przesyłania informacji przez Sieć jako rodzaj „czarnej skrzynki” (ang. Black Box) do której wkładamy zapytania lub dane a wyjmujemy inne dane i odpowiedzi. W poniższym artykule chciałbym przybliżyć szanownym czytelnikom zagadnienia związane z wyznaczaniem dróg dla pakietów z danymi czyli z trasowaniem (ang. routing), urządzeniami i mechanizmami biorącymi udział w tym procesie oraz pewnymi zasadami doboru tych dróg, zwanymi protokołami trasowania (ang. routing protocols).

Router – co to i po co to ?

Definicji routera IP jest bardzo wiele, i każda z nich może być poprawna. Ogólnie rzecz ujmując routery to urządzenia określane mianem sprzęgów sieciowych lub sprzęgów warstw sieciowych. Klasyczne routery działają w warstwie 3 (Sieci) Modelu OSI, łącząc ze sobą sieci/podsieci lokalne i/lub rozległe. Jeśli między dwoma punktami końcowymi w sieci istnieje więcej niż jedna ścieżka, routery sterują ruchem pakietów i umożliwiają ich filtrację. W tej definicji mieszają się trzy główne kategorie urządzeń.

Pierwsza to tradycyjne urządzenia sieciowe pracujące normalnie w warstwie drugiej, jak na przykład mosty (ang. bridge), koncentratory (ang. hub) oraz przełączniki (ang. switch), z dodanymi funkcjami trasowania (np. brouter = router + bridge)

Drugą kategorią są komputery ogólnego zastosowania, najczęściej oparte na systemie unixowym, wyposażone w dwa lub więcej interfejsów sieciowych i oprogramowanie obsługujące trasowanie IP.

Trzecią grupę stanowią dedykowane urządzenia (tzw. routery sprzętowe) zawierające oprogramowanie wyłącznie do obsługi trasowania IP. Ta grupa jest najczęściej utożsamiana z pojęciem „router” i dalsze rozważania będą bazowały na tych właśnie urządzeniach dedykowanych.

Gdy router odbiera pakiet, musi go „spreparować” do dalszej obróbki. Rozpakuje go, sprawdza na podstawie sum kontrolnych (CRC) czy pakiet nie zawiera błędów. Następnie odrzuca nieistotne dla niego informacje umieszczone przez protokoły niższych warstw modelu OSI (Fizycznej i Łącza danych).

Tak przygotowany pakiet może być przesłany dalej na podstawie informacji dodanych przez protokoły warstwy sieciowej. Informacje te zawierają adres przeznaczenia oraz, w przypadku stosowania trasowania źródłowego, listę węzłów pośrednich wyznaczających „najlepszą” trasę do punktu docelowego.

Na podstawie tych informacji router podejmuje jedno z poniższych działań :

- jeśli pakiet jest adresowany do samego routera, zaczyna przetwarzać pozostałe informacje zawarte w pakiecie
- jeśli adres docelowy znajduje się w sieci przyłączonej bezpośrednio, router przesyła go dalej
- jeśli dostępna jest jakakolwiek lista filtracji (w przypadku routerów opartych na IOS firmy CISCO listy takie noszą nazwę *access-list*), router porównuje pakiet z daną listą i ewentualnie go odrzuca (np. ze względów bezpieczeństwa)
- jeśli w pakiecie zawarta jest informacja trasowania źródłowego, wskazująca na kolejny węzeł (router) na trasie do punktu docelowego, przesyła go do tego routera
- jeśli dany router stosuje mechanizmy trasowania dynamicznego, aktualizuje na podstawie danych zawartych w pakiecie informacje o ścieżkach istniejących w sieci
- jeśli router nie wie jak dostarczyć pakiet pod adres przeznaczenia, odrzuca pakiet i przesyła stosowną informację do jego nadawcy.

Router przesyła pakiet do miejsca przeznaczenia na podstawie tzw. tablicy trasowania (ang. routing table) zawierającej adresy sieci o których „wie” dany router wraz z odległością (ilością „skoków” - ang. metric) do danej sieci.

Jako że fizycznie niemożliwym byłoby, aby w tablicy jednego routera zmieścić informacje o trasach do wszystkich sieci i podsieci, bardzo często poszukiwany jest inny router, który może mieć informacje o sieci o której „nasz” router nie wie.

Trasowanie statyczne a dynamiczne – wady i zalety. A może trasowanie hybrydowe?

Każda maszyna w sieci IP podejmuje decyzje o sposobie dostarczenia danych do odbiorcy na podstawie własnej tablicy trasowania. Zamiast wyznaczać całość trasy prowadzącej do adresata, maszyna wybiera adres miejsca, które przekaże dane dalej w odpowiednim kierunku. Niezależne trasowanie opierające się na kolejnych przeskokach wymaga, aby maszyna posiadała aktualne informacje o poszczególnych adresach przeznaczenia. Jeśli informacje te będą błędne, dwa lub więcej urządzeń pracujących w sieci może stworzyć tzw. pętlę trasowania czyli wymieniać pakiety między sobą na zasadzie „wg mnie to ty wiesz co z tym dalej zrobić”- „ależ skąd, moje dane mówią mi że to twoje zadanie”. W ten sposób wysłane pakiety nigdy nie dotrą do celu. Aby osiągnąć stan pełnej wymiany informacji o trasowaniu należałoby ręcznie skonfigurować przynajmniej większość maszyn podając im pewną liczbę tras, najczęściej do sąsiednich podsieci. Innym rozwiązaniem jest wymianianie informacji o trasowaniu pomiędzy pracującymi w sieci urządzeniami. Pierwszy sposób znany jest jako trasowanie statyczne, drugi – dynamiczne.

Trasowanie statyczne ma szereg ważnych zalet w stosunku do dynamicznego, ma też niestety jednak kilka znaczących wad. Do jego zalet należy zaliczyć przede wszystkim to, że jest w pełni konfigurowalne i przez to przewidywalne. Ponieważ administrator sieci wcześniej liczy wszystkie tablice trasowania, trasa którą przesyłany jest pakiet pomiędzy dwoma punktami jest zawsze dobrze znana. W przypadku trasowania dynamicznego wybrana w danym momencie trasa zależy od wielu czynników, np. od tego jakie urządzenia i łącza funkcjonują, zawartości tablicy trasowania routera w danym momencie, oraz od sposobu interpretacji przez router informacji o uaktualnieniach trasy nadesłanych przez inne urządzenia. Z drugiej strony zaletą trasowania dynamicznego jest skalowalność i zdolność dopasowywania się do zmieniających się warunków w sieci, co pozwala znaleźć alternatywną trasę w przypadku uszkodzenia na dotychczas używanej. Sieć obsługiwana przez dynamiczny protokół doboru trasy może się znacznie szybciej rozrastać, bez konieczności ciągłego uaktualniania danych przez administratora, która to rolę przejmują dynamiczne protokoły trasowania.

Kolejną zaletą trasowania statycznego jest znacznie mniejsze obciążenie sieci. Związane jest to z tym, że nie jest tu potrzebny żaden protokół dynamicznej wymiany informacji. Chociaż to dodatkowe obciążenie może być niezauważalne w szybkich sieciach opartych na segmencie Ethernet lub pierścieniu FDDI, to może ono stanowić znaczącą część informacji przesyłanych w paśmie wolnego łącza modemowego. Na pewno za to będzie w widoczny sposób obciążało router. Przykładowo stosując w małej sieci (3 podsieci, 30 komputerów, 2 modemy xDSL i 3 routery) protokół RIP obciążało to CPU głównego routera dodatkowo o około 7-10% przy częstej wymianie informacji między podsieciami. Związane było to z wysyłaniem teoretycznie co 30 sekund, zgodnie ze specyfikacją protokołu RIP, informacji o uaktualnieniach (których de facto nie było). Oczywiście jest to jaskrawy przykład nieoptymalizowania wymiany informacji między routerami (wszystkie pracowały w trybie wysyłanie/odbieranie, co było zbędne), niemniej jednak w przypadku dużej sieci pasmo przeznaczone na informacje o uaktualnieniach szybko rośnie.

Korzyścią płynącą z dynamicznej wymiany informacji między routerami jest możliwość w zasadzie bezbolesnego dodawania kolejnych routerów czy segmentów sieci. Pozostałe routery dowiedzą się o tym fakcie i odpowiednio uaktualnią swoje tablice trasowania bez konieczności ingerencji operatora. Jest to ważna zaleta trasowania dynamicznego i jednocześnie wada statycznego jeśli w grę wchodzi sieci o dużej złożoności.

Trasowanie statyczne jest łatwe do skonfigurowania w małych sieciach. Wystarczy ustalić na każdym z pracujących routerów, w jaki sposób może przysyłać dane do każdego segmentu sieci z którym jest bezpośredni połączony. Łatwo się jednak domyśleć, że o ile w sieci z kilkoma segmentami i niewielką liczbą routerów jest to bardzo łatwe do zrobienia, to w przypadku sieci z kilkudziesięcioma segmentami i kilkunastoma routerami stanowi niemały problem. Dochodzimy tu do jednej z bardzo poważnych wad trasowania statycznego, jaką jest bardzo mała skalowalność – cena za prostotę.

Kolejnym problemem trasowania statycznego, którego nie ma w trasowaniu dynamicznym, jest konieczność każdorazowego ręcznego przeliczania tablic trasowania podczas dokonywania zmiany połączeń między segmentami. Jest to bardzo duży problem w zaawansowanych sieciach posiadających kilka połączeń między dwoma punktami, np. kilka łączy internetowych o różnych przepustowościach czy łączenia segmentów w systemie „prawie każdy z każdym”.

Pozbawione tych wad trasowanie dynamiczne posiada jednak kilka innych. Jedną z nich jest znacznie większy stopień zawilgości sieci. Wymiana informacji o bieżącym układzie połączeń nie jest tak prosta jak powiedzenie „Hej, ja wiem jak trafić do...”. Każdy router uczestniczący w wymianie danych poprzez dynamiczny protokół trasowania musi jasno określić, jakie informacje będzie wysyłał do innych routerów. Jeszcze istotniejsze jest to, że na podstawie danych otrzymanych z innych routerów musi określić, jaka trasa będzie optymalna dla danego pakietu. Ponadto jeśli router ma płynnie reagować na zmiany zachodzące w sieci, musi mieć możliwość

usuwania bezużytecznych informacji ze swojej tablicy trasowania, co jeszcze bardziej go komplikuje. Stopień skomplikowania protokołu prowadzi do błędów w implementacji lub różnic w interpretacji tego protokołu w sprzeczności różnych producentów.

Pamiętać należy też, że niektóre z urządzeń pracujących w sieci mogą nie potrafić posługiwać się żadnym z protokołów trasowania dynamicznego lub nie obsługują stosowanego w całej sieci protokołu. W takim wypadku trasowanie statyczne będzie jedynym dostępnym rozwiązaniem.

Zastanawiając się nad wyborem sposobu trasowania na pewno dojdziemy do wniosku, że optymalnym byłoby połączenie obu sposobów trasowania. Pozwoliłoby to korzystać z dobrodziejstw trasowania dynamicznego znacznie zmniejszając stopień jego skomplikowania, ale nie ograniczając jego skalowalności.

Rozwiązanie takie nosi nazwę trasowania hybrydowego.

W hybrydowym schemacie trasowania niektóre części sieci wykorzystują trasowanie statyczne, a inne dynamiczne. To, która część używa którego sposobu trasowania, jest w zasadzie nieistotne, możliwe są różne kombinacje. Jednym z najczęściej stosowanych rozwiązań jest użycie trasowania statycznego na końcach sieci (w podsieciach, gdzie zwykle są dołączane komputery użytkowników), a trasowania dynamicznego w jej rdzeniu (szkieletie sieci).

W rzeczywistości oznacza to, że w przeważającej większości przypadków schemat ten będzie obowiązywał na zasadzie: końce sieci – nasze sieci LAN i szkielet sieci – sieć dostawcy internetu (np. POLPAK). Wyjątkiem od tego będą duże firmy z mocno rozwiniętą infrastrukturą sieciową (np. zajmujące cały biurowiec gdzie istnieje wyodrębniony szkielet sieci) czy też np. duże dobrze(!) zorganizowane sieci osiedlowe. Tak więc koniec końców znacznie częściej będziemy używać trasowania opartego na schemacie hybrydowym sprowadzonego do trasowania statycznego wewnątrz naszej sieci, a częścią z trasowaniem dynamicznym zajmie się nasz prowajder. W praktyce sprowadza się to do ustalenia w opcjach konfiguracyjnych protokołu TCP/IP parametru **domyślna brama** (ang. default gateway) i podania adresu routera brzegowego łączącego naszą sieć z siecią prowajdera. W przypadku połączeń typu DialUp lub dobrze zorganizowanych sieciach LAN nawet tego nie musimy podawać, gdyż dostarczy nam to protokół DHCP.

„Osiołkowi w żłobie dano” czyli przegląd dynamicznych protokołów trasowania

Sama decyzja wykorzystania dynamicznego protokołu trasowania to nie wszystko. Z biegiem lat powstało kilka różnych rodzajów tych protokołów.

Można je sklasyfikować na kilka sposobów. Aby nie zanudzać technicznymi aspektami problemów związanych z dynamicznymi protokołami trasowania, o których zainteresowani mogą poczytać w specjalistycznych publikacjach, wybrałem podział na protokoły wewnętrzne i zewnętrzne, czyli w jakiej sieci stosować protokół; w lokalnej sieci czy pomiędzy sieciami.

Pierwsze z nich, wewnętrzne, nazywane są z języka angielskiego *Interior Gateway Protocol (IGP)*, zewnętrzne zaś to *Exterior Gateway Protocol (EGP)*

Protokół sklasyfikowany jako zewnętrzny odpowiada za wymianę informacji pomiędzy dwiema niezależnymi administracyjnie sieciami, np. sieci dwóch korporacji czy uczelni. Każda z nich ma odrębną strukturę sieciową i wykorzystuje EGP do wymiany informacji z innymi jednostkami. Najpopularniejszym obecnie, opracowanym specjalnie dla sieci Internet, protokołem tej klasy jest *BGP (Border Gateway Protocol)*

BGP jest następcą starego i nieużywanego już obecnie protokołu **EGP** (od którego zresztą wzięła nazwę cała rodzina zewnętrznych protokołów trasowania). **BGP** jest pozbawiony szeregu wad, które dyskwalifikowały protokół EGP do użycia go w sieci Internet. Największymi zmianami w stosunku do przestarzałego EGP są:

- wymiana informacji o pełnej tablicy trasowania tylko przy pierwszym uruchomieniu. W dalszej pracy wymieniane są tylko uaktualnienia zawierające zmiany w tablicy danego routera.
- eliminacja koncepcji rdzenia sieci Internet, związana z dużą ilością dostawców na całym świecie i posiadaniem przez nich wielu rdzeni sieci
- obsługa domenowego trasowania bezklasowego (CIDR) umożliwiająca stały rozrost Internetu i zmniejszenie obciążenia routerów poprzez zredukowanie wymiany informacji.

BGP zbiera z pakietów przesyłanych przez sieć informacje o dostępności sąsiadów. Ponadto dodaje atrybuty trasy, takie jak koszt lub poziom bezpieczeństwa połączenia. Jego pozytywny wpływ na ograniczenie pasma niezbędnego do przesyłania informacji do routerów polega tym, że informacja wymieniana jest porcjami, a nie poprzez jednorazowe przesłanie całej bazy danych tablicy trasowania.

W przeciwieństwie do protokołu opisanego powyżej, wewnętrzne protokoły stosowane są wewnątrz jednej domeny administracyjnej. Ich budowa ma na celu mniejsze obciążenie routerów. Główną wadą tej grupy

protokołów jest to, że nie są one w stanie obsługiwać rozrastających się sieci. Najczęściej stosowanymi w sieciach IP protokołami są : Routing Information Protocol (RIP), Open Shortest Path First (OSPF) oraz Enhanced Interior Gateway Routing Protocol (EIGRP). Pierwsze dwa z nich są otwartymi standardami, które zostały zaadoptowane przez sieć Internet, natomiast trzeci jest protokołem opracowanym przez firmę CISCO Systems i stosowanym w routerach tej firmy.

RIP jest wewnętrznym protokołem trasowania stosującym algorytm dystans-wektor. Jest to obecnie najbardziej rozpowszechniony, mimo coraz częstszego stosowania protokołu OSPF, protokół wewnętrznego trasowania w sieci Internet. Podczas wymiany informacji o połączeniach w sieci złożonej, routery działające w oparciu o protokół RIP wykonują następujące działania :

- żądają aktualnych informacji o dostępności poszczególnych podsieci od innych routerów i aktualizują swoje tablice trasowania
- odpowiadają na podobne żądania przychodzące z innych routerów
- okresowo rozsyłają informacje o swojej obecności informując w ten sposób inne routery o stanie połączeń między sieciowymi
- w przypadku wykrycia zmian w sieci rozsyłają odpowiednią informację

Algorytm dystans-wektor uzależnia decyzję wyboru trasy od najmniejszej liczby skoków (*hops*) lub koszcie ścieżki, niezbędnych do osiągnięcia adresu docelowego, na podstawie wartości przypisanych danemu routerowi i jego sąsiadom. Jeśli pakiet wykona więcej niż 15 skoków, jego miejsce przeznaczenia jest klasyfikowane jako nieosiągalne i pakiet jest odrzucany.

Tablice routingu w protokole RIP są wymieniane z innymi routerami w przybliżeniu co 30 sekund. W przypadku braku takich komunikatów w czasie 180 sekund, dany router jest uznawany przez pozostałe za uszkodzony.

Powstała wersja 2 protokołu RIP (RIP v2), która od RIPv1 różni się m. inn.

- Obsługa podsieci – w wersji RIPv2 potrafi w przeciwieństwie do RIPv1 przekazywać do innych routerów informacje o maskach podsieci, również o maskach o zmiennej długości oraz potrafi obsługiwać trasowanie bezklasowe CIDR, o którym była mowa przy BGP.
- Autoryzacja – RIPv2 potrafi na podstawie dodatkowego pola w pakiecie informującym o zmianie w sieci ocenić czy informacja ta jest wiarygodna (czy pochodzi od „zaufanego” routera”
- Multicasting – RIPv1 używa do wysyłania uaktualnień adresu broadcast, co powoduje generowanie zbędnego ruchu w sieci. RIPv2 do tego celu używa adresów MAC konkretnych routerów lub transmisji typu multicast, ograniczając wysyłanie informacji do konkretnej grupy adresów.

OSPF jest algorytmem trasowania adaptacyjnego, wywodzącym się z prac nad protokołem Intermediate System-to-Intermediate System (IS-IS). Należy do protokołów stanu łącza. Trasowanie adaptacyjne wymaga, w porównaniu z trasowaniem za pomocą algorytm dystans-wektor, większej mocy obliczeniowej, oferując jednak skuteczniejszy nadzór nad przebiegiem procesu oraz znacznie szybciej reagując na zmiany. Stosowany jest tu algorytm Dijkstry uzależniony od następujących elementów:

- liczbę routerów na drodze do celu
- przepustowość pomiędzy podsieciami
- opóźnienia spowodowane przeciążeniami sieci
- koszty mediów transmisyjnych

Tablica trasowania OSPF aktualizowana jest tylko wtedy, gdy jest to konieczne, co pozwala wyeliminować zbędny ruch w sieci. Administrator może programować ścieżki w zależności od typu ruchu, uwzględniając wagę przesyłanych informacji i koszt ich przesłania.

EIGRP jest kolejnym protokołem opartym na algorytmie dystans-wektor. Jest następcą protokołu IGRP. Jako algorytm komercyjny stosowany jest w urządzeniach firmy CISCO. Jest to algorytm bardzo wydajny, szybko reagujący na zmiany w sieci. W porównaniu do protokołu OSPF wykorzystuje tak samo małe pasmo do przenoszenia informacji o zmianach w sieci, przy znacznie mniejszym zużyciu zasobów. Jako jedyny wymienionych protokołów umożliwia trasowanie pakietów innych niż IP (np. IPX czy AppleTalk). Ogólnie jest to chyba najwydajniejszy z dostępnych protokołów, niestety jego komercyjność ogranicza możliwości jego stosowania.

Podsumowując

Zagadnienie odpowiedniego trasowania w sieciach IP jest tematem-rzeką. Nie sposób go wyczerpać w jednej nawet sporej objętości książce, nie wspominając już o artykule. Dokładne informacje, wraz z przykładami konkretnych konfiguracji można znaleźć w podanej poniżej literaturze.

Pamiętajmy tylko o jednym : nie starajmy się na siłę stosować dynamicznych protokołów trasowania tam gdzie nie są one niezbędne. Jeśli sieć, którą konfigurujemy, nie będzie się zbyt często i w niekontrolowany sposób rozrastać poprzez powstawanie nowych podsieci, trasowanie statyczne jest naprawdę bardzo dobrym rozwiązaniem. Bardzo często wystarczy ustalić konkretne trasy do podsieci na routerze dostępowym oraz wyznaczyć domyślną trasę dla wszystkich pakietów nie zaadresowanych dla naszej sieci na router dostępowy naszego prowajdera, a on już sobie z tym poradzi. Przysłowiowe „polowanie armatą na mrówkę” czyli wymuszanie stosowania protokołu dynamicznego spowoduje tylko niepotrzebny tłok w sieci i może doprowadzić do opisanego wyżej zjawiska zapętlenia lub po prostu obniżyć wydajność połączenia. Jeśli jednak decydujemy się na jeden z protokołów dynamicznych, niech to będzie jeden protokół dla całej sieci, taki, z którym będą współpracowały wszystkie urządzenia. Stosowanie bardzo wydajnego EIGRP'a ma sens tylko jeśli wszystkie routery w naszej sieci są firmy CISCO lub potrafią ten protokół zinterpretować. Generalnie jeśli posiadamy w sieci różne urządzenia wypada zdecydować się na protokół RIP, który najprawdopodobniej będzie obsługiwany przez każde z nich. Istnieje oczywiście możliwość używania w danej sieci np. dwóch protokołów trasowania, ale należy to traktować jako rozwiązanie tymczasowe, dążąc do ujednoczenia protokołu dla całej sieci.

Michał Zimnicki

Literatura

1. Craig Hunt „TCP/IP – Administracja sieci - Wydanie drugie” Wydawnictwo ReadMe Warszawa 1998
2. Scott M. Ballew „Zarządzanie sieciami IP za pomocą routerów CISCO” Wydawnictwo ReadMe Warszawa 1998
3. A.Leinwand, B. Pinsky, M. Culpeper „Konfiguracja routerów CISCO cz. I i II” Wydawnictwo ReadMe Warszawa 2000
4. Tom Sheldon „Wielka Encyklopedia Sieci Komputerowych” Wydawnictwo Robomatic Wrocław 1995
5. Douglas E. Comer „Sieci komputerowe i intersieci” Wydawnictwo Naukowo Techniczne Warszawa 1999
6. Adam Wolisz „Podstawy lokalnych sieci komputerowych tom II” Wydawnictwo Naukowo Techniczne Warszawa 1992
7. „DSLPipe/CellPipe User's Guide” Lucent Technologies
8. „CISCO User's Manual” CISCO Systems Inc.