Gwarancja niezawodności Twojej sieci!

Routing i switching

Praktyczny przewodnik

HELION

O'REILLY®

Bruce Hartpence

Tytuł oryginału: Packet Guide to Routing and Switching

Tłumaczenie: Grzegorz Pawłowski

ISBN: 978-83-246-5119-1

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: http://helion.pl (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/routin
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

SPIS TREŚCI

ROZDZIAŁ 5.

Protokół RIP

Oczywiście, aby określić, która trasa jest najlepsza, musimy posiadać jakiś sposób mierzenia jakości tras.

— RFC 1058

Protokół informowania o trasach, znany jako protokół RIP (ang. *Routing Information Protocol*) jest wewnętrznym (ang. *interior*) protokołem działającym na podstawie wektora odległości, przeznaczonym dla małych sieci. Jest on zdefiniowany w dokumentach RFC organizacji IETF o numerach: 1058, 1388 i 1723. Był jednym z pierwszych protokołów trasowania używanych w Internecie. W celu wprowadzenia obsługi przestrzeni adresów bezklasowych opracowano drugą wersję tego protokołu. Niniejszy rozdział obejmuje budowę protokołu, jego działanie i zawartość generowanych przez niego pakietów, poznawaną dzięki ich przechwytywaniu. Dokumenty uaktualniające protokół RIP do wersji 2 powstały około 1998 roku. Nawet w tamtym czasie często utrzymywano, że protokół RIP był protokołem trasowania gorszego gatunku i że ma już za sobą swoje pięć minut. Jednakże protokół RIP nadal miał fanów. Przytoczmy cytat z dokumentu RFC 2453:

> Wraz z pojawieniem się protokołów OSPF i IS-IS znaleźli się tacy, którzy sądzą, że protokół RIP jest przestarzały. Chociaż jest prawdą, że nowsze protokoły routingu z rodziny IGP są o wiele lepsze od protokołu RIP, to protokół RIP ma pewne atuty. Przede wszystkim w małej sieci protokół RIP generuje bardzo mały narzut pod względem zużywanego pasma oraz czasu potrzebnego na konfigurację i zarządzanie. Protokół RIP jest również bardzo łatwy w implementacji, szczególnie w stosunku do nowszych protokołów IGP.

> Ponadto istnieje o wiele, wiele więcej funkcjonujących implementacji protokołu RIP niż protokołów OSPF i IS-IS razem wziętych. Prawdopodobnie taka sytuacja utrzyma się jeszcze przez kilka lat. Przyjąwszy, że protokół RIP będzie użyteczny w wielu środowiskach przez pewien czas, rozsądnym jest zwiększenie jego użyteczności. Jest to tym bardziej słuszne, że korzyść jest o wiele większa niż koszt zmiany.

A taki był stan rzeczy przed implementacją protokołu RIPv2. Tymczasem protokół RIP został włączony w inne standardy, takie jak *High Assurance Internet Protocol Encryptor Interoperability Standard* (standard interoperacyjności dla wysokiej niezawodności szyfratora protokołu internetowgo), czyli HAIPE IS. Ponadto w dokumentach RFC 2082 i 4822 wykonano pracę mającą na celu poprawienie bezpieczeństwa protokołu RIPv2. Te wysiłki wskazywałyby na to, że protokołowi RIPv2 pozostało jeszcze trochę życia. W każdym razie nawet przy braku dominacji na skalę światową protokół RIP stanowi dość dobry punkt odniesienia i środowisko szkoleniowe dla routingu.

Wersja 1 kontra wersja 2

Protokół RIP jest już używany przez długi czas. Chociaż odniósł sukces, nie obyło się bez problemów i wersja 1 protokołu RIP została zastąpiona przez wersję 2. Dokument RFC 1923 analizuje stosowalność czy brak stosowalności protokołu RIPv1. Wszystkie problemy związane z protokołem RIPv1 wywodzą się z jego klasowej natury, czyli ścisłego związku z sieciami podzielonymi na klasy A, B i C wyznaczające ich rozmiar. Komunikaty protokołu RIPv1 nie zawierają masek sieci i dlatego brakuje im elastyczności nowoczesnych podejść do zarządzania przestrzenią adresów. Podsumowując dokument RFC 1923, stwierdzamy, że:

- protokół RIPv1 zakłada, że lokalnie używana maska jest maską dla całego zbioru sieci;
- protokół RIPv1 nie może być używany razem z wykorzystaniem podsieci o zmiennej długości adresu (ang. *variable length subnetting*), łączeniem sieci w nadsieć (ang. *supernetting*) i bezklasowym routingiem międzydomenowym (ang. *classless interdomain routing*).

W dodatku protokół RIPv1 jest nazywany prostym protokołem wektora odległości, co oznacza, że nawet mimo rozszerzeń, takich jak podzielony horyzont i zatrucie wstecz, być może będzie musiał korzystać z czasochłonnych technik, takich jak zliczanie do nieskończoności, w celu osiągnięcia konwergencji. Dokument RFC konkluduje, że jeśli musimy użyć protokołu

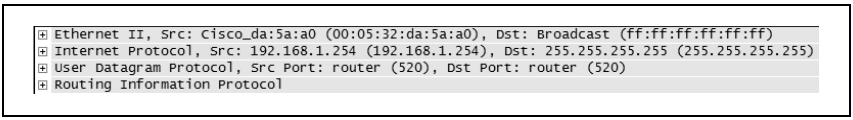
opartego na wektorze odległości, to użyjmy protokołu RIPv2 i rozważmy uaktywnienie jego skromnych mechanizmów bezpieczeństwa. W niniejszym rozdziale omówimy obie wersje protokołu pod względem używanych pakietów, jako że RIPv1 jest protokołem domyślnym. Jednakże wyraźna rekomendacja zaleca stosowanie protokołu RIPv2. Koncepcje podzielonego horyzontu, zatrucia wstecz i zliczania do nieskończoności zostaną omówione w dalszej części tego rozdziału.

Opis protokołu

Początek historii protokołu RIP jest zwykle łączony z dokumentem RFC 1058, ale ten dokument RFC to w gruncie rzeczy próba konsolidacji koncepcji, które już były w użyciu, z których jedna (program „routed" systemu Berkeley Unix, korzystający z wektora odległości) stanowiła de facto standard trasowania w tamtym czasie. Ale nawet w 1988 roku generalnie przyjęto, że protokół RIP nie będzie odpowiedni dla routingu w dużych intersieciach. Proponowane w zamian rozwiązanie polegałoby na tym, że system autonomiczny (**AS**, ang. *Autonomous System*) wykorzystuje protokół bram wewnętrznych (**IGP**, ang. *Interior Gateway Protocol*), taki jak protokół RIP, a następnie jakiś inny protokół trasowania w celu komunikowania się z sieciami innych systemów autonomicznych. Tu warto zacytować dokument RFC 1058:

> Protokół RIP został zaprojektowany do współpracy z sieciami umiarkowanego rozmiaru, używającymi w miarę jednorodnej technologii. Dlatego jest on odpowiedni jako protokół IGP dla wielu kampusów i sieci regionalnych używających łączy szeregowych, których szybkości nie różnią się znacznie.

Protokół RIP jest protokołem wektora odległości. Protokoły wektora odległości opisuje się zwykle jako protokoły implementujące algorytm Bellmana-Forda służący do znajdowania najlepszych ścieżek. Ale sama klasa protokołów została uprzednio zdefiniowana w książce Forda i Fulkersona *Flows in Networks*. Chociaż protokół RIP ma długi rodowód sięgający wstecz do sieci Xerox, został on zaprojektowany do routingu IP. Protokół RIP jest protokołem trasowania, który korzysta z wymiany tablic w celu aktualizacji sąsiednich routerów. Pomysł polega na tym, że każdy router wysyła swoją własną tablicę trasowania z aktywnych interfejsów, korzystając z protokołu datagramów użytkownika (UDP). Rysunek 5.1 przedstawia stosowaną enkapsulację.



Rysunek 5.1. Enkapsulacja protokołu RIP

Routery odbierające te informacje decydują, czy aktualizować swoje własne tablice, czy nie. Routery wykorzystują źródłowy adres IP znajdujący się w nagłówku IP jako adres routera przekazującego. Przypomnijmy sobie z rozdziału 1, że adresy IP routera przekazującego mają krytyczne znaczenie dla określenia następnego przeskoku. Informacja poprawiająca albo długość prefiksu, albo metrykę zostanie zapamiętana. Przyjmuje się, że dystans administracyjny będzie taki sam w całej sieci RIP. Ta nowa informacja o sieci może stanowić część przyszłych aktualizacji. Prosta wymiana tablic routingu może stworzyć tyle samo problemów, ile może rozwiązać przejście do trasowania dynamicznego. Z tego powodu protokół RIP zawiera również kilka mechanizmów służących do przyśpieszenia konwergencji i uniknięcia pętli, w tym wspomniane wyżej techniki podzielonego horyzontu, zatruwania i zliczania do nieskończoności.

Intersieci protokołu RIP są ograniczone pod względem rozmiaru do 15 przeskoków. To oznacza, przynajmniej dla protokołu RIP, że 16 równa się nieskończoność lub nieosiągalność. To liczenie przeskoków określa metrykę używaną przez protokół RIP do mierzenia odległości. Protokół RIP nie bierze pod uwagę żadnych danych czasu rzeczywistego, takich jak koszt, stopień wykorzystania czy szybkość. W ten sposób każda ścieżka jest mierzona przy użyciu tego samego standardu. Routery otrzymują aktualizacje RIP od bezpośrednio z nimi połączonych sąsiednich routerów. Router otrzymujący aktualizację wysyła z kolei swoją własną aktualizację. Zanim router będzie mógł wysłać zaktualizowane ogłoszenie routingu, musi zwiększyć metrykę wszystkich poznanych ścieżek o 1. Nowa aktualizacja zostanie wysłana z adresem IP nowego routera. Ten adres IP będzie adresem routera „następnego przeskoku" wprowadzonym do tablicy routingu sąsiadów, a metryka będzie określać odległość do miejsca docelowego trasą prowadzącą przez ten adres IP.

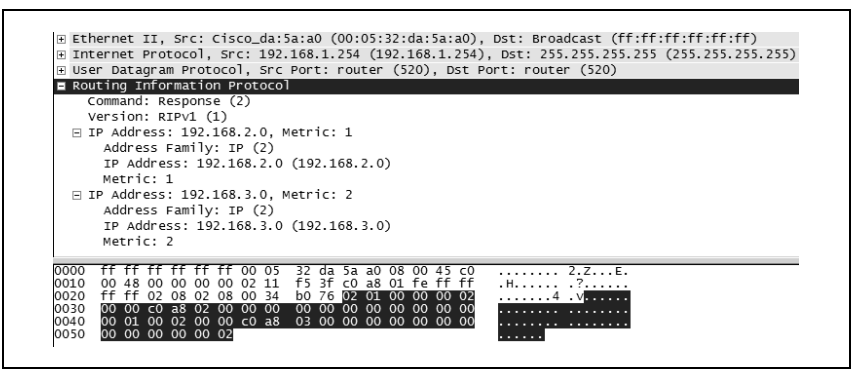
Pamiętajmy, że pozycja w tablicy routingu utrzymuje dane o wieku informacji, adresie docelowym, następnym przeskoku lub bramie z punktu widzenia routera, lokalnym interfejsie używanym do osiągnięcia następnego przeskoku oraz koszcie trasy. Korzystając z tych informacji, router może podjąć opartą na wektorze odległości decyzję dotyczącą efektywności trasy. Ponieważ te informacje są przesyłane do sąsiednich routerów,

a wszelkie wynikające stąd aktualizacje są także rozsyłane, możliwe jest „zrozumienie" topologii całego zbioru sieci dzięki dialogowi prowadzonemu tylko przez sąsiadujące ze sobą routery.

Dystans administracyjny, czyli wartość przypisana do protokołu RIP, wynosi 120. Informacja ta pojawi się w tablicy routingu obok długości prefiksu i metryki.

Struktura

Jak można zobaczyć na rysunku 5.2, pakiety protokołu RIPv1 mają prostą strukturę. Ten konkretny pakiet został przechwycony we wczesnym etapie konfiguracji topologii wykorzystywanej w tym rozdziale. W tym momencie sieć była konfigurowana jedynie przy użyciu protokołu RIP w wersji 1.



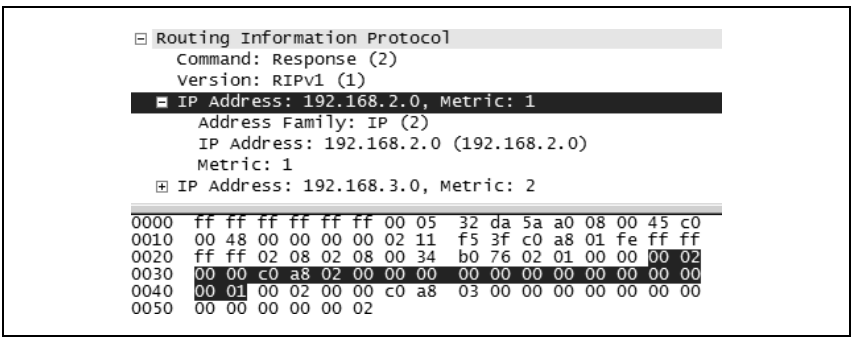
Rysunek 5.2. Pakiet protokołu RIPv1

Polecenie (ang. *command*)
: 1-bajtowe pole, które opisuje typ komunikatu. **Żądanie** domaga się przesłania tablicy routingu, a **odpowiedź** zawiera tablicę trasowania routera. Zostało zdefiniowanych kilka innych komunikatów, ale straciły one obecnie swoją aktualność.

Wersja (ang. *version*)
: Jest to również pojedynczy bajt przeznaczony do wskazania używanej odmiany protokołu.

Pole zerowe
: Za polem wersji i za identyfikatorem rodziny adresów znajdują się pola obligatoryjnie wyzerowane. Mają one po 2 bajty długości. 8-bajtowe pole zawierające obowiązkowo same zera występuje również po adresie IP sieci docelowej.

Każda pozycja w tablicy trasowania zawiera miejsce na informację o sieci i jej metrykę. Wartości heksadecymalne dla sieci `192.168.2.0` zostały pokazane na rysunku 5.3.



Rysunek 5.3. Przykład zapisu w formacie heksadecymalnym dla sieci 192.168.2.0

Identyfikator rodziny adresów AFI (ang. *Address Family ID*)
: Wartość ta wskazuje typ protokołu komunikacyjnego używanego w bieżącej sieci. Chociaż zarezerwowano miejsce dla wymienienia innych protokołów, żadne inne wartości nie zostały zdefiniowane w dokumencie RFC 1058. Wartość AFI dla IP wynosi 2.

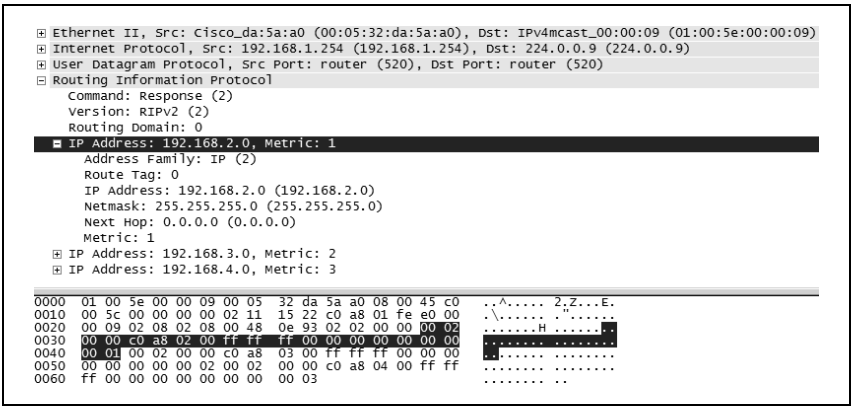
Adres IP
: Jest to adres IP dla sieci docelowej w tablicy routingu. W przykładzie pokazującym dane komunikatu RIP w postaci heksadecymalnej sieci `192.168.2.0` odpowiada zapis `c0 a8 02 00`.

Metryka (ang. *metric*)
: Jest to odległość od sieci docelowej mierzona liczbą przeskoków. W przykładzie liczba przeskoków wynosi 1. Jest to pole 4-bajtowe.

Pakiety protokołu RIPv1 są ograniczone do 512 bajtów całkowitej długości. W przypadku dużych tablic trasowania ich pozycje mogą być rozdzielone między wiele pakietów.

Struktura pakietu protokołu RIPv2, pokazana na rysunku 5.4, jest podobna z wyjątkiem dodanych kilku pól dotyczących podsieci. Ze względu na spójność naszej analizy badany pakiet zawiera ten sam adres sieci.

Format komunikatu dla tych dwóch wersji jest zasadniczo taki sam, z polami zdefiniowanymi w dokumencie RFC 1058 pozostawionymi bez zmian. Porównując heksadecymalną część przedstawienia zawartości pakietów



Rysunek 5.4. Pakiet protokołu RIPv2

widocznych na rysunkach 5.3 i 5.4, widzimy, że w każdej wersji została przydzielona taka sama liczba bajtów dla każdej pozycji. Zmiany dotyczące całego pakietu w protokole RIPv2 obejmują wartość wersji i pole domeny routingu.

Domena routingu (ang. *routing domain*)
: Razem ze znacznikiem trasy określonym dla poszczególnych miejsc docelowych domena routingu protokołu RIP pozwala na odróżnienie aktualnego zbioru sieci protokołu RIP od sieci, które zostały poznane dzięki protokołom zewnętrznym.

Dla poszczególnych sieci zostały dodane pola maski sieci, znacznika trasy i następnego przeskoku.

Maska sieci (ang. *netmask*)
: Jest to maska sieci docelowej. Istnieje pewna obawa, że pole to może być niewłaściwie interpretowane przez routery używające protokołu RIPv1, należy więc podjąć pewne środki ostrożności w środowisku korzystającym z różnych wersji; lub po prostu używać protokołu RIPv2.

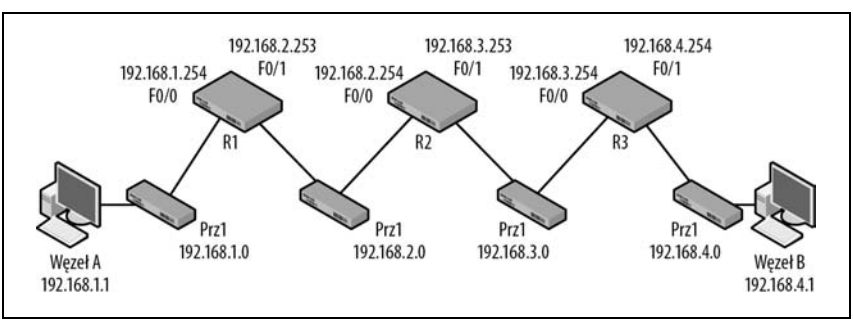
Znacznik trasy (ang. *route tag*)
: Pole znacznika trasy jest atrybutem wykorzystywanym do identyfikacji trasy, która została poznana dzięki zewnętrznemu źródłu, takiemu jak inny protokół z rodziny IGP. Taka trasa nie pochodzi z aktualnego zbioru sieci protokołu RIP.

Następny przeskok (ang. *next hop*)
: Normalnie router odbierający komunikat RIP używa źródłowego adresu IP otrzymanego pakietu jako adresu następnego przeskoku, aktualizując pozycje w tablicy routingu. Jeśli pole to ma wartość `0.0.0.0`, router użyje adresu źródłowego pakietu zawierającego aktualizację jako adresu następnego przeskoku. Zdarzają się sytuacje, że istnieje więcej niż jedna ścieżka do miejsca docelowego, kiedy źródłowy adres IP i adres następnego przeskoku mogą się nie zgadzać. We wszystkich przypadkach adres następnego przeskoku musi być dostępny z sieci, w której został ogłoszony.

Końcowa uwaga na temat identyfikatora rodziny adresów dla protokołu RIP2: protokół RIPv2 umożliwia uwierzytelnianie swoich komunikatów. Jeśli pole AFI otrzyma wartość `0xFFFF`, to obszar, normalnie przydzielany pojedynczej sieci docelowej (20 bajtów), zostanie użyty na informacje związane z uwierzytelnieniem. Będzie obejmował 2-bajtowy typ uwierzytelnienia oraz 16 bajtów danych uwierzytelniających.

Podstawowe działanie

Jak wynika z wcześniejszego omówienia, protokół RIP korzysta z wymiany tablic do przekazania sąsiadom aktualnych informacji dotyczących dostępnych sieci. Topologia przedstawiona na rysunku 5.5 zostanie wykorzystana do analizy krok po kroku podstawowego działania protokołu RIP i niektórych technik używanych do zoptymalizowania protokołu RIP pod względem wydajności. Jako że protokół RIPv1 nie powinien być używany, wszystkie omawiane przykłady będą korzystać z protokołu RIPv2. Topologia ta zawiera cztery sieci. Zostały dołączone adresy IP interfejsów routerów. Prawdopodobnie rozpoznajesz w niej topologię z rozdziału 1 — to omówienie rozpocznie się w ten sam sposób.



Rysunek 5.5. Topologia korzystająca z protokołu RIP

Na początku zostały skonfigurowane routery — otrzymały swoje adresy IP. Jednak protokół RIP w tym momencie jeszcze nie działa. Tablice trasowania routerów (patrz tabela 5.1) zawierają tylko trasy bezpośrednio podłączone. Każdy router wie wyłącznie o tych dwóch sieciach, do których ma interfejsy. Jako uwaga na marginesie: termin „trasa bezpośrednio podłączona" pojawia się we wczesnych dokumentach RFC, więc niekoniecznie pochodzi od firmy Cisco.

Tabela 5.1. Początkowe tablice routingu

R1	R2	R3
C 192.168.1.0 F0/0	C 192.168.2.0 F0/0	C 192.168.3.0 F0/0
C 192.168.2.0 F0/1	C 192.168.3.0 F0/1	C 192.168.4.0 F0/1

Posuwając się od lewej strony topologii w prawo, konfigurujemy w routerach protokół RIPv2. Polecenia dla urządzeń Cisco są nieskomplikowane, a w przypadku routera R1 wyglądałyby następująco:

```
router rip
    version 2
    network 192.168.1.0
    network 192.168.2.0
```

Kiedy tylko te polecenia zostaną wprowadzone, z obydwu interfejsów routera R1 zostaną wysłane pakiety RIP. Nawet jeśli router R2 zobaczy te pakiety, nie zaktualizuje jeszcze swojej tablicy routingu, ponieważ nie działa w nim protokół RIP.

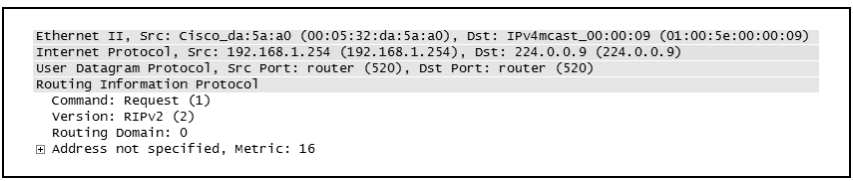
Współczesne wersje systemu Cisco IOS zawierają polecenie `auto-summary` dla protokołu RIP. Polecenie to jest domyślnie aktywne i „podsumowuje podprefiksy do granicy sieci klasowej przy przekraczaniu granic sieci klasowych". Przy trasowaniu pomiędzy nieciągłymi podsieciami polecenie to powinno być wyłączone, by umożliwić ogłaszanie podsieci.

Pakiety generowane przez router mają swoją kolejność i podlegają regule podzielonego horyzontu (ang. *split horizon*), o czym się przekonamy. Pierwsze pakiety zostały pokazane na rysunku 5.6 i zostały przechwycone w sieci 192.168.1.0.

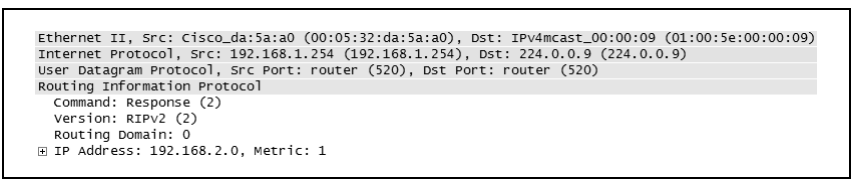
12	192.168.1.254	224.0.0.9	RIPv2	9.996674	Request
57	192.168.1.254	224.0.0.9	RIPv2	17.821149	Response
58	192.168.1.254	224.0.0.9	RIPv2	18.041530	Response
71	192.168.1.254	224.0.0.9	RIPv2	47.610498	Response
78	192.168.1.254	224.0.0.9	RIPv2	75.023898	Response
83	192.168.1.254	224.0.0.9	RIPv2	102.317097	Response
89	192.168.1.254	224.0.0.9	RIPv2	129.021237	Response
95	192.168.1.254	224.0.0.9	RIPv2	154.547572	Response
102	192.168.1.254	224.0.0.9	RIPv2	180.903084	Response

Rysunek 5.6. Wymiana pakietów przy uruchomieniu protokołu RIPv2

W przypadku wyświetlonych danych pakiety były filtrowane pod kątem przynależności do protokołu RIP, więc wydaje się, jakby niektóre pakiety zostały pominięte. Pierwszy wysłany pakiet jest żądaniem. Ten typ komunikatu stanowi prośbę do sąsiedniego routera o przesłanie jego własnej tablicy routingu. Wszystkie pakiety pochodzą z routera R1, co oznacza, że nie została otrzymana żadna odpowiedź. Kiedy tylko router R1 ma sieć do ogłoszenia, generuje odpowiedź, która zawiera jego własną tablicę trasowania. Te komunikaty zostały przedstawione na rysunkach 5.7 i 5.8.



Rysunek 5.7. Żądanie protokołu RIP

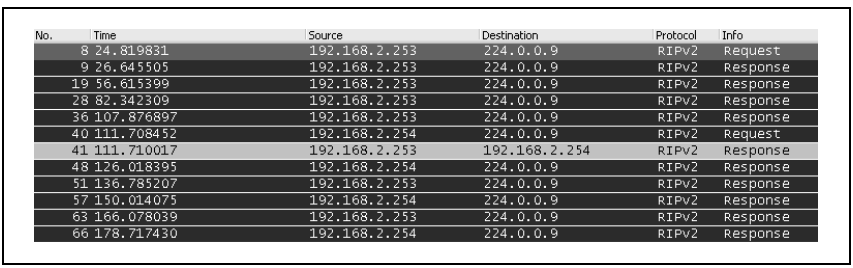


Rysunek 5.8. Odpowiedź protokołu RIP

Komunikaty żądania mogą prosić o całość lub o część tablicy routingu i są przetwarzane pozycja po pozycji. W przypadku gdy istnieje tylko jedna pozycja odpowiadająca sieci docelowej z wartością pola AFI równą 0 i metryką równą 16, mamy do czynienia z żądaniem przesłania całej tablicy trasowania. Komunikaty odpowiedzi są przesyłane, ilekroć zostanie odebrane żądanie, w ramach aktualizacji oraz w czasie wykonywania normalnych operacji stanu ustalonego.

Po odebraniu komunikatu odpowiedzi router powinien sprawdzić poprawność zawartości komunikatu, ponieważ zawarte w nim informacje mogą trafić do tablicy trasowania. Na przykład może zostać sprawdzony źródłowy adres IP oraz format poszczególnych pozycji. W tym momencie zostaną sprawdzone metryki i długości prefiksu. Jeśli nie istnieją podobne wpisy w tablicy routingu lub jeśli wartości zawarte w komunikacie odpowiedzi okażą się lepsze, dane trasy zostaną zainstalowane. Zostaną zaktualizowane także liczniki czasu (omawiane poniżej), a po zwiększeniu metryk zostanie wysłana aktualizacja.

Kiedy routery R2 i R3 zostaną skonfigurowane za pomocą podobnych zestawów poleceń (sieci będą się różnić), ich tablice trasowania zostaną zaktualizowane na podstawie odebranych informacji. W dodatku między routerami zostaną wygenerowane i przesłane podobne pakiety. Istnieje jedna różnica w stosunku do ruchu występującego do tej pory: kiedy routery już wiedzą o sąsiadach, także używających protokołu RIPv2, komunikaty mogą być adresowane bezpośrednio do sąsiedniego routera, jak to pokazuje rysunek 5.9.



No.	Time	Source	Destination	Protocol	Info
8	24.819831	192.168.2.253	224.0.0.9	RIPv2	Request
9	26.645505	192.168.2.253	224.0.0.9	RIPv2	Response
19	56.615399	192.168.2.253	224.0.0.9	RIPv2	Response
28	82.342309	192.168.2.253	224.0.0.9	RIPv2	Response
36	107.876897	192.168.2.253	224.0.0.9	RIPv2	Response
40	111.708452	192.168.2.254	224.0.0.9	RIPv2	Request
41	111.710017	192.168.2.253	192.168.2.254	RIPv2	Response
48	126.018395	192.168.2.254	224.0.0.9	RIPv2	Response
51	136.785207	192.168.2.253	224.0.0.9	RIPv2	Response
57	150.014075	192.168.2.254	224.0.0.9	RIPv2	Response
63	166.078039	192.168.2.253	224.0.0.9	RIPv2	Response
66	178.717430	192.168.2.254	224.0.0.9	RIPv2	Response

Rysunek 5.9. Wymiana pakietów między routerami R2 i R3

Ta grupa pakietów rozpoczyna się od początku naszej konfiguracji — od pierwszego żądania (pakiet 8) wysłanego po tym, jak router R1 został skonfigurowany do obsługi protokołu RIP. Zwróćmy uwagę na źródłowy adres IP dla tego pakietu. Pakiet 40 został wyemitowany, kiedy do obsługi protokołu RIP został skonfigurowany router R2. Wynikający z tego pakiet odpowiedzi (41) zamiast adresu rozsyłania grupowego protokołu RIPv2 zawiera adres routera R3. Adresy IP emisji pojedynczej są używane w powiązaniu z flagami polecenia/odpowiedzi. Kiedy tylko ta wymiana zostaje zakończona, routery wracają do adresu rozsyłania grupowego, który będzie odczytany przez routery ewentualnie dodane do sieci.

Kiedy router R3 także zostanie skonfigurowany do obsługi protokołu RIPv2, tablice routingu zostaną całkowicie wypełnione za pośrednictwem pakietów żądania/odpowiedzi, jak pokazuje tabela 5.2.

Tabela 5.2. Tablice routingu całkowicie wypełnione po działaniach protokołu RIP

R1	R2	R3
C 192.168.1.0 F0/0	C 192.168.2.0 F0/0	C 192.168.3.0 F0/0
C 192.168.2.0 F0/1	C 192.168.3.0 F0/1	C 192.168.4.0 F0/1
R 192.168.3.0 [120/1] via 192.168.2.254	R 192.168.1.0 [120/1] via 192.168.2.253	R 192.168.1.0 [120/2] via 192.168.3.253
R 192.168.4.0 [120/2] via 192.168.2.254	R 192.168.4.0 [120/1] via 192.168.3.254	R 192.168.2.0 [120/1] via 192.168.3.253

Wszystkie szczegóły tablic trasowania są ważne, ale kilka elementów jest wartych szczególnej uwagi. Dystans administracyjny (AD) i metryka zostały zawarte w nawiasach. Dystans administracyjny protokołu RIP wynosi 120, a metryka jest równa liczbie przeskoków. W naszej małej sieci największa metryka ma wartość 2. Możemy wyśledzić pochodzenie tych informacji, przypisując je pakietom źródłowym protokołu RIP, takim jak te, które można zobaczyć na rysunkach od 5.2 do 5.4.

Innym ważnym szczegółem jest router przekazujący, czyli następny przeskok. W tablicy routingu jest adres występujący po słowie „via". Ten adres jest poznawany na podstawie źródłowego adresu IP pakietu RIP. Jak można zobaczyć, niektóre z tras poznanych dzięki protokołowi RIP mają ten sam adres przekazujący. Na przykład router R3 wysyła na adres `192.168.3.253` zarówno ruch do sieci `192.168.1.0`, jak i ruch do sieci `192.168.2.0`. Jest to właściwe dla tej topologii, ale zgodnie z tym, co rozpatrywaliśmy w rozdziale 1, w punkcie dotyczącym trasowania statycznego, można by tu rozważyć utworzenie trasy domyślnej. Rzeczywista tablica trasowania dla routera R1 została pokazana na rysunku 5.10.

```
R1#
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.4.0/24 [120/2] via 192.168.2.254, 00:00:13, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
R    192.168.3.0/24 [120/1] via 192.168.2.254, 00:00:13, FastEthernet0/1
R1#
```

Rysunek 5.10. Rzeczywista tablica trasowania routera R1

Wyświetlone dane zostały uzyskane za pomocą polecenia `show ip route`. Router dodaje również czas do każdej dynamicznej pozycji. Pozwala to na śledzenie wieku poznanej trasy.

Liczniki czasu

Podobnie jak wiele innych protokołów, protokół RIP posiada zbiór liczników czasu, który zarządza wysyłaniem ogłoszeń oraz usuwaniem starych i niepoprawnych informacji dotyczących trasowania.

Licznik czasu odpowiedzi/odświeżania (ang. *response/update timer*)
W trakcie wykonywania normalnych działań proces routingu wysyła niewymuszoną (przez odebranie żądania) odpowiedź co 30 sekund, starając się utrzymywać świeżość informacji dotyczących trasowania.

Licznik czasu przeterminowania/unieważnienia trasy (ang. *route timeout/invalid timer*)
Po 180 sekundach każda trasa, która nie została odświeżona przez pakiet odpowiedzi, jest uważana za niedobrą i usuwana z tablicy routingu. Po wygaśnięciu tego licznika czasu sąsiednie routery zostają poinformowane, że trasa jest zła, za pośrednictwem aktualizacji i zostaje uruchomiony licznik czasu odzyskiwania pamięci zajmowanej przez nieużyteczne dane. W wysyłanych aktualizacjach metryka dla przeterminowanej trasy otrzymuje wartość 16.

Licznik czasu odśmiecania/usuwania zbędnych danych (ang. *garbage collection/flush timer*)
Po wygaśnięciu tego licznika czasu trasa jest ostatecznie wymazywana z tablicy routingu. W tym miejscu implementacje mogą być nieco zwodnicze. Dokument RFC 2453 podaje, że czas ten powinien być ustawiony na 120 sekund. Firma Cisco stosuje 60 sekund mierzonych od momentu wygaśnięcia licznika czasu przeterminowania lub 240 sekundy całkowitego wieku wpisu dotyczącego danej trasy. Cisco odwołuje się do licznika czasu przetrzymania (ang. *hold down timer*), opisując tę różnicę czasu. Jednakże dokumentacja podaje wartość 180 sekund.

Adresowanie

Kolejny ważny szczegół dotyczy nie tyle tablicy routingu, ile informacji adresowych zawartych w nagłówkach pakietów zawierających komunikat RIP. Rysunek 5.11 przedstawia zarówno pakiet RIPv1, jak i pakiet RIPv2.

Rysunek 5.11. Adresowanie w protokole RIP

Obydwa pakiety mają źródłowy adres IP, który odpowiada transmitującemu interfejsowi routera. Jednakże protokół RIP w wersji 1 używa adresu ograniczonego rozgłaszania (`255.255.255.255`) jako adresu docelowego, podczas gdy wersja 2 wykorzystuje zarezerwowany adres rozsyłania grupowego o wartości `224.0.0.9`. Adresowanie warstwy 2 często naśladuje adresowanie warstwy 3 i dlatego pakiet RIPv1 używa adresu rozgłoszeniowego dla ramki Ethernet. Pakiet RIPv2 korzysta z adresu MAC rozsyłania grupowego w ramce warstwy 2, który jest oparty na adresie IP rozsyłania grupowego używanym w warstwie 3.

Chociaż ten rozdział nie dotyczy adresowania stosowanego w rozsyłaniu grupowym, pożyteczna jest pewna znajomość kontekstu. Tabela 5.3 przedstawia ogólny schemat adresowania dla rozsyłania grupowego, który został naszkicowany w dokumencie RFC 1371.

Tabela 5.3. Adresowanie w rozsyłaniu grupowym według dokumentu RFC 3171

Adres	Zastosowanie
`224.0.0.0 – 224.0.0.255`	blok sterowania siecią lokalną
`224.0.1.0 – 224.0.1.255`	blok sterowania intersiecią
`224.0.2.0 – 224.0.255.0`	blok AD-HOC
`224.1.0.0 – 224.1.255.255`	grupy multiemisji protokołu ST
`224.2.0.0 –224.2.255.255`	blok protokołu SDP/SAP
`224.252.0.0 – 224.255.255.255`	blok DIS Transient
`225.0.0.0 – 231.255.255.255`	ZAREZERWOWANE
`232.0.0.0 – 232.255.255.255`	blok multiemisji z określonego źródła (ang. *source specific*)
`233.0.0.0 – 233.255.255.255`	blok GLOP
`234.0.0.0 – 238.255.255.255`	ZAREZERWOWANE
`239.0.0.0 – 239.255.255.255`	blok zakresów administracyjnych

W bloku sterowania siecią lokalną znajduje się kilka adresów, które są bliskie i drogie naszym sercom:

`224.0.0.1` — adres rozsyłania grupowego do wszystkich hostów,

`224.0.0.2` — adres rozsyłania grupowego do wszystkich routerów,

`224.0.0.5` — adres rozsyłania grupowego używany w protokole OSPF,

`224.0.0.9` — adres rozsyłania grupowego używany w protokole RIPv2.

Adres ten został przydzielony protokołowi RIPv2 przez dokument RFC. Ponieważ routery są zazwyczaj jedynymi urządzeniami, które wykonują protokół RIPv2, inne urządzenia na ogół nie przetwarzają tych pakietów. Rozsyłanie grupowe może stanowić interesujące wyzwanie dla administratorów sieci, ponieważ routery nie przekazują pakietów multiemisji, przynajmniej nie przekazują ich bez pomocy protokołu **PIM** (ang. *Protocol Independent Multicast* — rozsyłanie grupowe niezależne od protokołu) i protokołu **IGMP** (ang. *Interior Group Management Protocol* — wewnętrzny protokół zarządzania grupami). Na szczęście pakiety RIPv2 nie są w istocie przekazywane. Są modyfikowane i retransmitowane.

Ostatni element adresowania widoczny w analizowanym pakiecie jest konkretnie numerem portu UDP warstwy 4. Zarówno protokół RIPv1, jak i RIPv2 używa portu 520. Czasami zabawne jest obserwowanie początkujących administratorów sieci konfigurujących listy kontroli dostępu (ACL) lub reguły zapory sieciowej. Są często tak przejęci blokowaniem niepożądanego ruchu UDP/TCP, że czasem zostaje odfiltrowany ruch związany z protokołem RIP, a potem administrator się dziwi, dlaczego pojawia się tak dużo komunikatów ICMP „cel nieosiągalny".

Funkcje zaawansowane

Podstawowe działanie protokołu RIP łatwo zrozumieć po zajrzeniu do wnętrza pakietów. Pakiety RIP mogą być bardzo pouczające również ze względu na to, czego **nie** zawierają. W tym podrozdziale zbadamy niektóre spośród dodatkowych reguł wbudowanych w protokół, aby pomagały w uniknięciu problemów.

Podzielony horyzont

Jeśli zdarzyłoby Ci się obserwować dwoje ludzi przedstawiających się sobie wzajemnie przy pierwszym spotkaniu, rozmowa przebiegałaby zapewne jakoś tak:

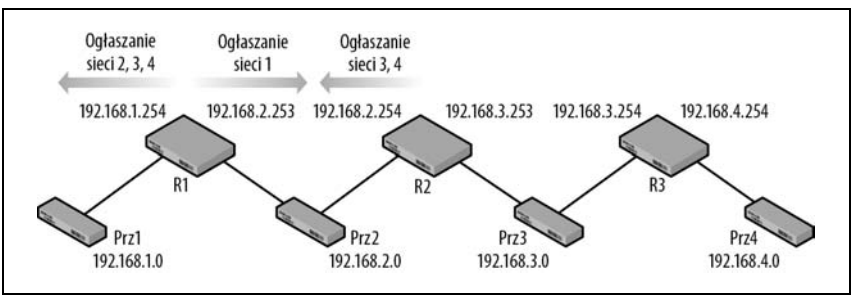
Osoba 1: Cześć, mam na imię Bob.
Osoba 2: Cześć, mam na imię Sally.

Nie spodziewalibyście się usłyszeć czegoś w rodzaju:

Osoba 1: Cześć, mam na imię Bob.
Osoba 2: Cześć, masz na imię Bob.

Bob jest już świadom, że ma na imię Bob, więc byłoby niemądre ze strony Sally mówienie Bobowi czegoś, co on jej właśnie powiedział. To samo odnosi się do routerów. A zatem routery nie powinny informować swoich sąsiadów o sieciach, dla których sąsiad właśnie rozesłał ogłoszenie. Mówiąc inaczej: nie ogłaszaj czegoś z tego samego interfejsu, poprzez który o tym czymś się dowiedziałeś. Nie ma także żadnego sensu wysyłanie informacji o dostępności danej sieci do tej sieci.

Na rysunku 5.12 router R1 jest bezpośrednio podłączony do sieci `192.168.1.0` i `192.168.2.0`. Router R1 nie będzie przekazywał informacji o sieci `192.168.1.0` do sieci `192.168.1.0`. Ta sama reguła ma zastosowanie do ogłoszeń wysyłanych przez router R2 do sieci `192.168.2.0`.



Rysunek 5.12. Ogłaszanie z użyciem techniki podzielonego horyzontu

Możemy następnie przedstawić graficznie działania występujące między routerami R1 i R2. Router R1 przekazuje informacje o sieci `192.168.1.0` w stronę prawą i o sieciach `192.168.2.0`, `192.168.3.0` oraz `192.168.4.0` w stronę lewą. Router R2 otrzymuje informacje o sieci `192.168.1.0` od routera R1 i jest bezpośrednio podłączony do sieci `192.168.2.0`. Dlatego ogłoszenie wracające do routera R1 zawiera tylko informacje o sieciach `192.168.3.0` i `192.168.4.0`. Funkcjonowanie techniki podzielonego horyzontu jest widoczne w pakietach. Na rysunku 5.13 została wyświetlona zawartość pakietów pochodzących z routerów R2 i R3 widocznych w sieci `192.168.2.0`.

Adresy IP zawarte w tych pakietach pokazują, że pochodzą one z routerów R1 i R2. Jak widzimy, routery przestrzegają reguł podzielonego horyzontu, minimalizując w ten sposób rozmiar pakietów. Ale rzeczywista korzyść wynikająca z zastosowania podzielonego horyzontu polega na przyśpieszeniu konwergencji, ponieważ ścieżki do sieci docelowych są klarowne.

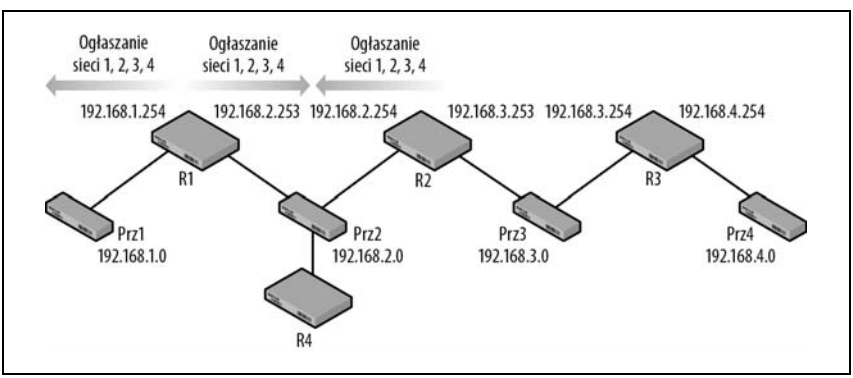
```
Ethernet II, Src: Cisco_da:5a:a1 (00:05:32:da:5a:a1), Dst: IPv4mcast_00:00:09 (01:00:5e:00:00:09)
Internet Protocol, Src: 192.168.2.253 (192.168.2.253), Dst: 224.0.0.9 (224.0.0.9)
User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
Routing Information Protocol
  Command: Response (2)
  Version: RIPv2 (2)
  Routing Domain: 0
⊞ IP Address: 192.168.1.0, Metric: 1

Ethernet II, Src: Cisco_28:02:80 (00:05:5e:28:02:80), Dst: IPv4mcast_00:00:09 (01:00:5e:00:00:09)
Internet Protocol, Src: 192.168.2.254 (192.168.2.254), Dst: 224.0.0.9 (224.0.0.9)
User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
Routing Information Protocol
  Command: Response (2)
  Version: RIPv2 (2)
  Routing Domain: 0
⊞ IP Address: 192.168.3.0, Metric: 1
⊞ IP Address: 192.168.4.0, Metric: 2
```

Rysunek 5.13. Porównanie pakietów ilustrujących działanie reguł podzielonego horyzontu

W jakim przypadku technika podzielonego horyzontu nie jest używana? Okazuje się, że istnieją pewne połączenia w sieciach WAN, które jej nie używają, ale zdarza się to rzadko. Wyłączenie algorytmu podzielonego horyzontu przynosi zazwyczaj złe skutki.

Używając tej samej topologii, przyjmijmy, że routery ogłaszają wszystkie sieci z każdego interfejsu, jak to pokazano na rysunku 5.14. Aby lepiej zilustrować zasięg problemu, został wstawiony jeszcze jeden router, ale wykorzystywane są te same sieci.



Rysunek 5.14. Ogłoszenia bez stosowania reguł podzielonego horyzontu

Załóżmy, że router R1 ulega awarii. Router R1 stanowił jedyną ścieżkę do sieci `192.168.1.0`. W gruncie rzeczy, jeśli router R4 nie przestrzega reguł podzielonego horyzontu, będzie również ogłaszał tę sieć. Pamiętajmy, że sieć `192.168.1.0` nie jest już dostępna. Zatem wszystkie routery w tej topologii będą nadal sądzić, że ta sieć jest wciąż dostępna, i zachowają ją w swoich tablicach trasowania. Inny możliwy scenariusz polega na tym, że zamiast

utraty całego routera awarii uległ tylko interfejs 192.168.1.254. Ponownie router R1 przestałby ogłaszać sieć 192.168.1.0, ale po otrzymaniu ogłoszenia od routera R2 będzie sądził, że sieć jest dostępna z przeciwnej strony topologii. Algorytm podzielonego horyzontu jest domyślnie włączony, aby zapobiec tego rodzaju problemom z konwergencją.

Zatruwanie

Jednym z pozostałych zabezpieczeń jest zatruwanie tras. W przypadku zmiany konfiguracji routera lub awarii sprzętu router może zatruć trasę, aby pozostałe routery wiedziały, że sieć (lub sieci) nie jest już dostępna. W celu zatrucia trasy router wstawia po prostu metrykę, która jest równoważna nieskończoności. Dla protokołu RIP jest to liczba 16.

Co by się wydarzyło w tej samej topologii, gdyby interfejs 192.168.3.253 utracił łączność z siecią 192.168.3.0? Dopóki router R2 zachowuje połączenie przez interfejs 192.168.2.254, może zatruć sieć 192.168.3.0. Routery odbierające pakiet z zatrutą trasą wiedzą natychmiast, że ścieżka jest zła, i usuną ją ze swoich tablic trasowania szybciej. Pakiet z zatrutą trasą został pokazany na rysunku 5.15.

```
Ethernet II, Src: Cisco_28:02:80 (00:05:5e:28:02:80), Dst: IPv4mcast_00:00:09 (01:00:5e:00:00:09)
Internet Protocol, Src: 192.168.2.254 (192.168.2.254), Dst: 224.0.0.9 (224.0.0.9)
User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
Routing Information Protocol
  Command: Response (2)
  Version: RIPv2 (2)
  Routing Domain: 0
⊟ IP Address: 192.168.3.0, Metric: 16
    Address Family: IP (2)
    Route Tag: 0
    IP Address: 192.168.3.0 (192.168.3.0)
    Netmask: 255.255.255.0 (255.255.255.0)
    Next Hop: 0.0.0.0 (0.0.0.0)
    Metric: 16
```

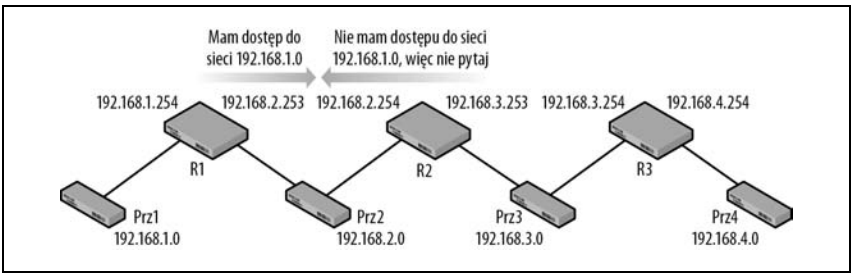
Rysunek 5.15. Pakiet zawierający zatrutą trasę

Jeśli router R2 uległby całkowitej awarii, pozostałe routery w topologii musiałyby przy rozwiązaniu tego problemu polegać na swoich własnych licznikach czasu. Zatruwanie tras jest wykonywane domyślnie.

Zatrucie wstecz

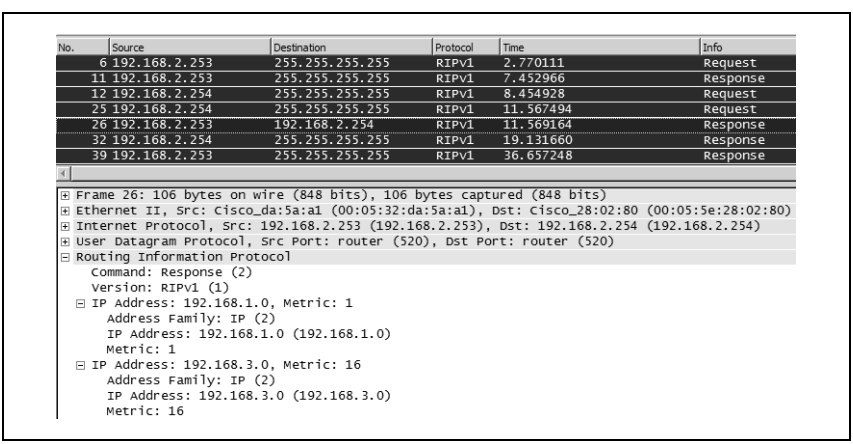
Zatrucie wstecz opiera się na koncepcji zatruwania, ale jest stosowane w czasie ustabilizowanego działania w celu zapewnienia, że nie zostanie podjęta próba uzyskania dostępu do sieci przez nieodpowiednią lub niepożądaną ścieżkę. W tej samej topologii, kiedy router R1 ogłosi dostępność

sieci 192.168.1.0, router R2 wyśle ogłoszenie o niedostępności tej samej sieci z powrotem do routera R1. Efekt polega na tym, że na wypadek gdyby z routerem R1 coś się stało, pozostałe routery jasno stwierdzają, że nie dysponują ścieżką do potencjalnie utraconych sieci, co widać na rysunku 5.16.



Rysunek 5.16. Komunikacja związana z zatruciem wstecz

Zatrucie wstecz nie jest domyślnie włączone, więc musi zostać uaktywnione w routerze. Niektóre implementacje routingu stosują zatrucie wstecz w fazie „odkrywania swoich sąsiadów". Rysunek 5.17 przedstawia pakiety żądań i odpowiedzi przepływające między routerami R2 i R3 przez sieć 192.168.2.0. Chociaż nie jest to częścią normalnego ruchu związanego z działaniem protokołu RIP, widzimy, że bezpośrednio po dowiedzeniu się o sieciach 192.168.3.0 i 192.168.4.0 od routera R2 router R1 (192.168.2.253) stosuje zatrucie wstecz, aby poinformować router R2, że nie ma żadnej innej ścieżki do tych miejsc docelowych. Po tej wymianie pakiety protokołu RIP wracają do normalności.



Rysunek 5.17. Wymiana pakietów charakterystyczna dla zatrucia wstecz

Aktualizacje wymuszone (ang. *triggered updates*)

Zawsze, kiedy informacja dotycząca pozycji w tablicy trasowania zostanie zmieniona, router wysyła natychmiast pakiet RIP zawierający tylko tę nową informację, nie czekając na wygaśnięcie licznika czasu odświeżania. Ten „szybki" pakiet RIP nazywa się aktualizacją wymuszoną. Uzasadnienie tego działania polega na tym, że informacja o złych lub zmienionych trasach może być rozprzestrzeniana w sieci o wiele szybciej, niż miałoby to miejsce, gdyby routery oczekiwały na wygaśnięcie licznika czasu standardowego odświeżania. Dodatkowo routery odbierające wymuszoną aktualizację mogą wysłać własne wymuszone aktualizacje. W ten sposób fala świeżej informacji dotrze do wszystkich punktów sieci. Pomaga to w skróceniu czasu konwergencji.

Kilka przykładów aktualizacji wymuszonych można zaobserwować w momencie wygaśnięcia liczników czasu. Załóżmy, że łącze między routerem R3 i przełącznikiem Prz3 ulegnie awarii, co oznacza, że router R2 już nie otrzymuje aktualizacji od routera R3 dotyczących sieci `192.168.4.0`. Po 180 sekundach trasa zostanie oznaczona jako prawdopodobnie nieczynna w tablicy routingu (pokazanej na rysunku 5.18) i zostanie wysłana wymuszona aktualizacja ogłaszająca sieć `192.168.4.0` z metryką równą 16. Te wymuszone aktualizacje będą propagować się niemal natychmiast poprzez całą sieć. Kiedy minie kolejne 60 sekund, trasa zostanie usunięta z tablicy routingu. Inny przykład dotyczyłby sytuacji, w której dochodzi do wyłączenia interfejsu `192.168.4.254`. W tym przypadku aktualizacja zostałaby wysłana natychmiast.

```
Gateway of last resort is not set

R    192.168.4.0/24 is possibly down, routing via 192.168.3.254, FastEthernet0/1
R    192.168.1.0/24 [120/1] via 192.168.2.253, 00:00:26, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/1
R2#
```

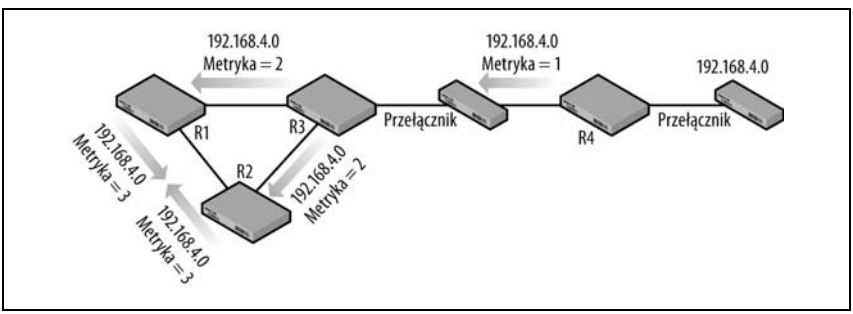
Rysunek 5.18. Sieć 192.168.4.0 jest prawdopodobnie nieczynna

Aktualizacje wymuszone są również wysyłane w przypadku poprawy sytuacji. Kiedy interfejs `192.168.4.254` zostanie z powrotem uaktywniony, niezwłocznie są wysyłane aktualizacje wymuszone, a następnie propagowane w całej sieci. Tablice trasowania sąsiednich routerów są również natychmiast aktualizowane.

Zliczanie do nieskończoności

Zliczanie do nieskończoności (ang. *count to infinity*) jest jeszcze jednym narzędziem służącym do wydobywania sieci z trudnej sytuacji, kiedy nie ma aktualizacji lub zatrutych tras. Jest to ostatnia deska ratunku w sytuacjach, kiedy ma miejsce utrata łączności lub awaria urządzenia. Na przykład, jak na rysunku 5.16, jeśli łącze między routerem R3 i przełącznikiem 3 zostałoby utracone, router R2 byłby nieświadomy powstania tego problemu, ponieważ nadal byłby obecny impuls łącza dla interfejsu `192.168.3.253`.

Rysunek 5.19 przedstawia nieco bardziej złożoną topologię. Została zainstalowana pętla, co skutkuje przepływem informacji związanej z routingiem w dwóch kierunkach. Router R4 ogłasza dostępność sieci `192.168.4.0` i stwierdza, że jest ona odległa o 1 przeskok.



Rysunek 5.19. Problem powodujący zliczanie do nieskończoności

Następnie router R3 ogłasza tę samą sieć po zwiększeniu liczby przeskoków o 1. Ponieważ router R3 jest połączony z kolejnymi routerami R1 i R2, ta sama informacja protokołu RIP jest przekazywana do obydwu z nich, chociaż z różnych interfejsów. Żeby dokończyć sprawę, obydwa routery R1 i R2 przesyłają ogłoszenie tej samej sieci wzajemnie do siebie po zwiększeniu liczby przeskoków. Po odebraniu tych pakietów protokołu RIP routery R1 i R2 odrzucają te informacje, ponieważ proponują one trasy gorsze od już posiadanych.

Co się stanie po katastrofalnej awarii routera R4? Nawet jeśli przyjmiemy, że mechanizmy podzielonego horyzontu, zatruwania i wymuszonych aktualizacji działają znakomicie, na niewiele nam się one przydadzą. Router R3 nie ma pojęcia o tym, że router R4 uległ awarii, więc może postępować, bazując tylko na już poznanych informacjach oraz licznikach czasu protokołu RIP. W końcu router R3 usunie trasę i zaprzestanie ogłaszania. Kiedy to się wydarzy, dalej położone routery (z perspektywy routera R4) R1 i R2

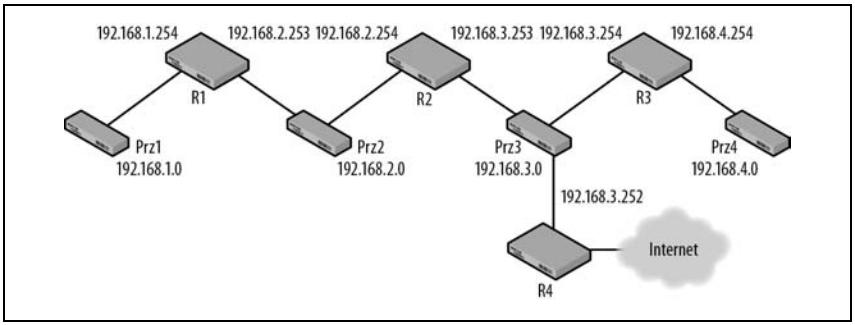
nie będą musiały się martwić o podzielony horyzont i **rozpoczną ogłaszanie, że sieć `192.168.4.0` jest dostępna**. Przedtem jednak zwiększy się metryka. Router R3 rozpoczyna ogłaszanie trasy drugiej stronie sieci po zwiększeniu liczby przeskoków o 1. Pierwotnie routery R1 i R2 dowiedziały się o sieci `192.168.4.0` od routera R3. Z ich perspektywy odległość do sieci docelowej (metryka) mogła się zmienić, ale źródłowy adres IP (wektor) nie uległ zmianie. Zwiększają więc liczbę przeskoków i wysyłają pakiety protokołu RIP ponownie w obieg. Ten proces potrwa tak długo, aż pakiet RIP będzie zawierać liczbę przeskoków równą 16, a ścieżka zostanie uznana za nieużyteczną.

Nadzieja jest w tym, że zatruwanie przeterminowanych tras i wymuszone aktualizacje rozwiążą ten problem i administratorzy sieci nigdy nie będą musieli polegać na tym czasochłonnym procesie. Ale dokument RFC 2453 ostrzega:

> Jeśli można by było sprawić, aby system pozostawał w bezruchu, w czasie gdy wykonuje się kaskada wymuszonych aktualizacji, możliwe byłoby udowodnienie, że zliczanie do nieskończoności nigdy się nie zdarzy. Złe trasy byłyby zawsze natychmiast usuwane, więc nie mogłyby tworzyć się żadne pętle w routingu. Niestety, sprawy nie wyglądają tak różowo. W czasie gdy wysyłane są aktualizacje wymuszone, może równolegle przebiegać regularne odświeżanie. Routery, które jeszcze nie odebrały aktualizacji wymuszonej, będą nadal wysyłać informację opartą na trasie, która już nie istnieje. Jest możliwe, że po przejściu przez router aktualizacji wymuszonej otrzyma on zwykłą aktualizację od jednego z tych routerów, które jeszcze nie zostały poinformowane. Mogłoby to reaktywować osieroconą pozostałość błędnej trasy.

Jak wydostanę się poza swoją sieć?

Do tego momentu protokół RIP był używany do docierania do miejsc docelowych położonych wewnątrz zbioru sieci opartych na protokole RIP, czyli czegoś, co dokument RFC nazywa systemem autonomicznym. Przy tym założeniu jednak ruch nie może popłynąć nigdzie dalej. W jaki sposób zatem topologia sieci umożliwia przejście od protokołu bram wewnętrznych (IGP) do reszty świata? Rozdział 1 zawierał omówienie ogólnego routingu oraz punkt poświęcony bramom ostatniej instancji i trasie domyślnej. Ponieważ topologia używana w tym rozdziale była dokładnie taka sama, mają zastosowanie te same reguły. Kandydująca trasa domyślna zazwyczaj występuje kilka razy w tablicach trasowania innych routerów. Przy nieco zmodyfikowanej topologii pojawia się oczywista ścieżka wyprowadzająca poza ten zbiór sieci, jak na rysunku 5.20.



Rysunek 5.20. Topologia protokołu RIP z trasą domyślną

Nawet mimo dodania routera R4 topologia jest wciąż nieskomplikowana. Z jednej strony administrator sieci mógłby po prostu zainstalować trasy domyślne we wszystkich routerach. Wówczas jednak sieć nie byłaby chroniona przed zmianami w topologii i nieczynnymi połączeniami.

Inną strategią, która może być użyta z protokołem RIP, jest koncepcja redystrybucji. Jako ścieżkę prowadzącą na zewnątrz router R4 może zainstalować trasę domyślną skierowaną do Internetu. Przez wykorzystanie protokołu RIP działającego po stronie sieci `192.168.3.0` ta trasa domyślna może być zakomunikowana routerom podrzędnym (R1, R2, R3) przez użycie polecenia `redistribute static`. Podstawowa konfiguracja routera R4 przedstawia się następująco:

```
router rip
    version 2
    redistribute static
    network 192.168.3.0
ip route 0.0.0.0 0.0.0.0 10.101.100.254
```

Kiedy tylko zostaje wprowadzone polecenie `redistribute`, pakiety protokołu RIP płyną do routerów podrzędnych z dołączoną trasą domyślną. Routery R1, R2 i R3 uaktualniają swoje tablice routingu, dołączając nową informację. Taki pakiet został pokazany na rysunku 5.21.

```
⊞ Ethernet II, Src: Cisco_28:1c:a0 (00:05:5e:28:1c:a0), Dst: IPv4mcast_00:00:09 (01:00:5e:00:00:09)
⊞ Internet Protocol, Src: 192.168.3.252 (192.168.3.252), Dst: 224.0.0.9 (224.0.0.9)
⊞ User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
⊟ Routing Information Protocol
    Command: Response (2)
    Version: RIPv2 (2)
    Routing Domain: 0
  ⊟ IP Address: 0.0.0.0, Metric: 1
      Address Family: IP (2)
      Route Tag: 0
      IP Address: 0.0.0.0 (0.0.0.0)
      Netmask: 0.0.0.0 (0.0.0.0)
      Next Hop: 0.0.0.0 (0.0.0.0)
      Metric: 1
```

Rysunek 5.21. Pakiet protokołu RIP zawierający trasę domyślną

Rysunek 5.22 przedstawia zmiany w tablicach trasowania routerów podrzędnych. Zauważmy, że routery R2 i R3 są podłączone do tej samej sieci co router R4 i wskazują bezpośrednio na niego jako swoją trasę domyślną z liczbą przeskoków równą 1. Jednak pakiet protokołu RIP został zaktualizowany przez router R2 i teraz router R1 używa routera R2 jako swojej bramy domyślnej ze zwiększoną liczbą przeskoków.

```
Gateway of last resort is 192.168.2.254 to network 0.0.0.0

R    192.168.4.0/24 [120/2] via 192.168.2.254, 00:00:06, FastEthernet0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
R    192.168.3.0/24 [120/1] via 192.168.2.254, 00:00:06, FastEthernet0/1
R*   0.0.0.0/0 [120/2] via 192.168.2.254, 00:00:06, FastEthernet0/1
R1#
```

```
Gateway of last resort is 192.168.3.252 to network 0.0.0.0

R    192.168.4.0/24 [120/1] via 192.168.3.254, 00:00:09, FastEthernet0/1
R    192.168.1.0/24 [120/1] via 192.168.2.253, 00:00:25, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/1
R*   0.0.0.0/0 [120/1] via 192.168.3.252, 00:00:05, FastEthernet0/1
R2#
```

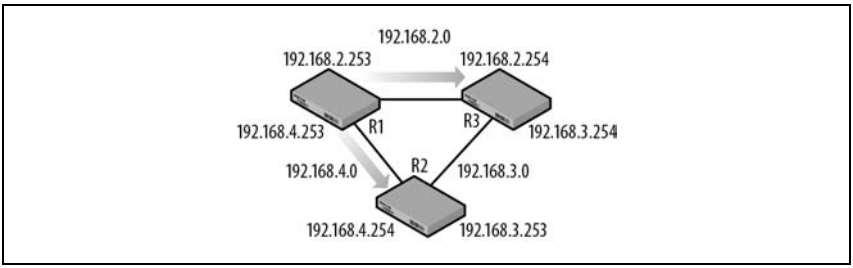
```
Gateway of last resort is 192.168.3.252 to network 0.0.0.0

C    192.168.4.0/24 is directly connected, FastEthernet0/1
R    192.168.1.0/24 [120/2] via 192.168.3.253, 00:00:24, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 192.168.3.253, 00:00:24, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
R*   0.0.0.0/0 [120/1] via 192.168.3.252, 00:00:00, FastEthernet0/0
R3#
```

Rysunek 5.22. Tablice routingu z zainstalowanymi trasami domyślnymi

Protokół RIP a pętle

Pętle w routingu mogą być tworzone przez połączenia fizyczne lub przez błędną konfigurację. Zapętlona architektura może poważnie utrudniać transmisję. Większość protokołów routingu, w tym RIP, stosuje techniki służące do ograniczenia wpływu pętli na przesyłanie pakietów IP, takie jak omawiane wcześniej w tym rozdziale. A co się wydarzy, jeśli pętla zostanie wprowadzona do topologii? Rysunek 5.23 przedstawia routery R1, R2 i R3 połączone w pętli. Została usunięta sieć `192.168.1.0`, a router R1 otrzymał adres w sieci `192.168.4.0`. W takiej topologii jak ta pakiety protokołu RIP przepływają dokładnie tak samo jak w topologiach już wcześniej omówionych.



Rysunek 5.23. Topologia tworząca pętlę

Badając tę topologię z perspektywy routera R1, stwierdzamy, że jest on bezpośrednio podłączony do sieci `192.168.2.0` i `192.168.4.0`. Jest on także w odległości jednego przeskoku od sieci `192.168.3.0`. Ale do tej sieci można uzyskać dostęp z dwóch różnych kierunków. Korzyść polega na tym, że gdyby przypadkiem jedna ścieżka została utracona, druga automatycznie przejmie jej zadanie. Rzeczywista tablica trasowania z routera R1 została pokazana na rysunku 5.24.

```
Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
R    192.168.3.0/24 [120/1] via 192.168.2.254, 00:00:06, FastEthernet0/1
                    [120/1] via 192.168.4.254, 00:00:15, FastEthernet0/0
R1#
```

Rysunek 5.24. Tablica trasowania routera R1

Pakiety przechwycone w obydwu bezpośrednio podłączonych sieciach ukazują, że jeśli ruch jest wysyłany do sieci `192.168.3.0`, to router R1 równoważy obciążenie sieci, wysyłając połowę ruchu przez router `192.168.2.254` i połowę przez router `192.168.4.254`.

Bezpieczeństwo

Dobry projekt zabezpieczenia sieci zawiera wiele aspektów, w tym bezpieczeństwo urządzeń sieciowych i protokołów funkcjonujących w sieci. O protokołach routingu powszechnie wiadomo, że łatwo je zakłócić. Jak pokazały wymuszone aktualizacje, kiedy router otrzymuje nowe lub lepsze informacje dotyczące miejsc docelowych, nie kwestionuje tych informacji, ale szybko je przyswaja, uaktualniając swoją tablicę trasowania. Dzięki temu

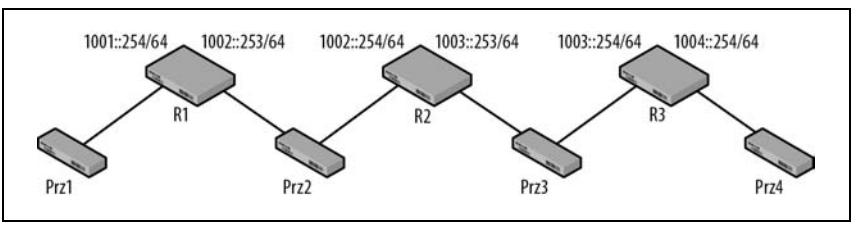
ruch może zostać skierowany w inną stronę, dobra informacja może zostać zastąpiona przez specjalnie podstawioną lub ruch może być wysyłany przez nieistniejące ścieżki. Weźmy pod uwagę, że intruz, uzyskując dostęp do sieci, może nie tylko przechwytywać ruch przesyłany w tej sieci, ale i wprowadzać do niej swój własny ruch. Routery odbierające informacje od napastnika nie potrafiłyby dokonać rozróżnienia między nimi a autentycznymi informacjami od sąsiednich routerów.

Z tym problemem można próbować sobie poradzić na kilka sposobów. Zarządzanie routerami może zostać ograniczone do konkretnych segmentów lub interfejsów. Ponadto ruch zmierzający do routerów może być filtrowany. Wtedy routery nie będą prowadzić nasłuchu aktualizacji routingu z konkretnego kierunku i mogą nie odpowiadać na komunikaty ICMP lub na inne żądania przesłania informacji. Innym cennym narzędziem będącym w dyspozycji administratora sieci jest interfejs pętli zwrotnej (ang. *loopback interface*), nazywany też interfejsem pseudosieci. Pętle zwrotne to programowe interfejsy, które nie są związane z żadnym konkretnym interfejsem fizycznym. To oznacza, że pętla zwrotna jest zawsze dostępna, nawet jeśli niektóre z portów fizycznych są zamknięte. Pętle zwrotne mogą również otrzymać adresy IP, które są odrębne w stosunku do adresów sieci danych, tak aby napastnik nie miał dostępu do interfejsu zarządzającego urządzenia. Wreszcie w interfejsach pętli zwrotnej mogą funkcjonować protokoły routingu. Techniki te zastosowane łącznie mogą skutecznie odizolować sieć zarządzania od sieci danych.

Protokół RIPv2 ma jedną dodatkową możliwość, która utrudnia nieco życie napastnikowi: uwierzytelnianie komunikatów RIP. Jak wcześniej wspomniano, kiedy pole AFI komunikatu RIP zawiera wartość `FFFF`, ten komunikat jest właśnie wykorzystywany do uwierzytelnienia pozostałych informacji zawartych w odpowiedzi protokołu RIP. Dane uwierzytelniające są skonfigurowane w każdym routerze znajdującym się w obrębie topologii systemu autonomicznego (AS). Dokument RFC 2453 precyzuje, że uwierzytelnienie jest prostym hasłem zapisanym otwartym tekstem, podczas gdy dokument RFC 2082 sugeruje zastosowanie uwierzytelnienia opartego na algorytmie MD5. Oba te dokumenty zostały uaktualnione przez dokument RFC 4822, który firmuje dodatkowe algorytmy oparte na kluczach. Jedna z ważnych różnic zawartych w tej aktualizacji polega na tym, że pakiet RIPv2 jest modyfikowany przez dołączenie informacji uwierzytelniających na końcu pakietu zamiast prostego umieszczenia ich w polach przeznaczonych na specyfikację sieci docelowej.

Protokół RIP a IPv6

Istnieje model wdrożeniowy dla protokołu RIP opartego na protokole IPv6. Protokół **IPv6 RIP** jest także znany jako **RIPng**, czyli RIP nowej generacji (ang. *next generation*). Dokument RFC 2080 ujawnia, że struktura i działanie protokołu nie różni się zbyt wiele od konfiguracji z protokołem IPv4. Odnotowujemy w tym miejscu niektóre z wprowadzonych modyfikacji. Rysunek 5.25 przedstawia topologię podobną do używanej wcześniej w tym rozdziale. Interfejsy routerów zostały zrekonfigurowane po otrzymaniu adresów IPv6. Wyjaśnienie routingu statycznego w topologii takiej samej jak przedstawiona na rysunku topologia IPv6 można znaleźć w rozdziale 1.



Rysunek 5.25. Topologia sieci używających protokołu IPv6

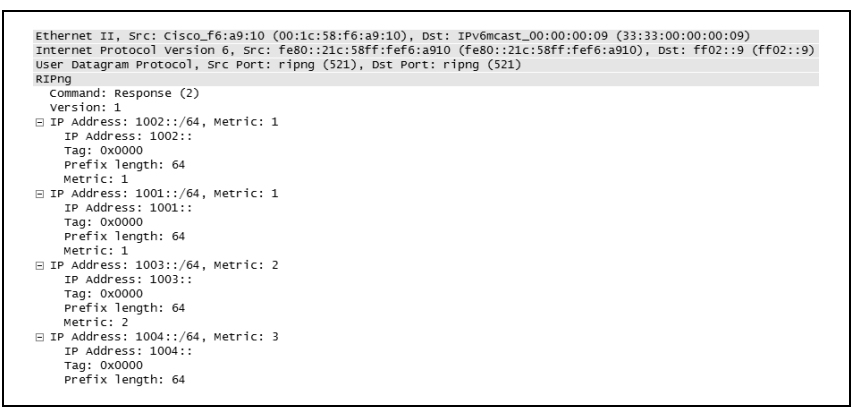
Podstawowa konfiguracja routera do obsługi protokołu IPv6 RIP jest prosta z jedną znaczącą różnicą: polecenia protokołu RIP są powiązane z interfejsem. Słowo „przewodnik" jest po prostu nazwą przyjętą dla danej instancji procesu RIP.

```
ipv6 unicast-routing
interface FastEthernet0/0
    ipv6 address 1001::254/64
    ipv6 rip przewodnik enable
!
interface FastEthernet0/1
    ipv6 address 1002::253/64
    ipv6 rip przewodnik enable
ipv6 router rip przewodnik
```

Rysunek 5.26 przedstawia tablice trasowania routera R1. Protokół IPv6 dodaje trasy łącza (ang. *link routes*), sieci 1001 i 1002 są bezpośrednio dołączone. Trasy do sieci 1003 i do sieci 1004 są oparte na wynikach działania protokołu RIP. Zauważmy, że dystans administracyjny i liczby przeskoków są wykorzystywane w ten sam sposób.

Rysunek 5.26. Tablica trasowania routera obsługującego protokół IPv6 RIP

Pod względem operacyjnym protokół IPv6 RIP jest prawie taki sam, chociaż pakiety musiały być nieco zmodyfikowane, aby dostosować się do innego protokołu warstwy 3. Ponadto ma miejsce zmiana w sposobie działania dotycząca techniki podzielonego horyzontu. Chociaż protokół IPv6 RIP przestrzega reguły podzielonego horyzontu, ogłasza sieć lokalną. Pakiet pokazany na rysunku 5.27 jest pakietem przechwyconym w sieci `1001::/64`. Protokół IPv6 ma inne spojrzenie na sieć i wykorzystuje adresowanie lokalne dla łącza, zamiast używać adresu IP o zasięgu globalnym.



Rysunek 5.27. Pakiet protokołu IPv6 RIP w sieci 1001

Pakiet ten ogłasza wszystkie cztery znane sieci, a nie tylko te, o których informacje pochodzą z przeciwnej strony routera. Adresem docelowym jest zarezerwowany adres rozsyłania grupowego protokołu IPv6 (`FF02::9`), a numer portu jest równy `521`. Jak można zauważyć, struktura jest bardzo podobna i chociaż jest określona jako wersja 1, zawiera informację o masce lub o długości prefiksu.

Lektura

RFC 1058 *Routing Information Protocol*.
RFC 1112 *Host Extensions for IP Multicasting*.
RFC 1256 *ICMP Router Discovery Messages*.
RFC 1812 *Requirements for IP Version 4 Routers*.
RFC 1923 *RIPv1 Applicability Statement for Historic Status*.
RFC 2080 *RIPng for IPv6*.
RFC 2453 *RIP Version 2* (dezaktualizuje dokumenty RFC 1723, 1388).
RFC 3171 *IANA Guidelines for IPv4 Multicast Address Assignments*.
RFC 4822 *RIPv2 Cryptographic Authentication* (dezaktualizuje dokument RFC 2082 *RIP-2 MD5 Authentication*).

Podsumowanie

Protokół RIP oraz routing oparty na wektorze odległości jest w użyciu od wczesnych dni komunikacji internetowej. Z powodu długiego czasu konwergencji protokół RIP ma dystans administracyjny równy 120. Sprawia to, że aktualizacje routingu pochodzące od protokołu RIP są mniej atrakcyjne niż te otrzymane od innych protokołów. Ponieważ został zaprojektowany do obsługi małego zbioru sieci, protokół RIP, używając metryki wyrażonej liczbą przeskoków, dopuszcza maksymalny rozmiar sieci wynoszący 15. Protokół RIP przetrwał głównie dzięki użyciu szeregu technik, takich jak podzielony horyzont, zatruwanie tras, zatrucie wstecz, zliczanie do nieskończoności i aktualizacje wymuszone. Obsługa uwierzytelniania dodaje bezpieczeństwo do starzejącego się protokołu, być może utrzymując go przy życiu.

Pytania sprawdzające

1. Kluczową różnicę miedzy protokołami RIPv1 i RIPv2 stanowi obsługa podsieci.
   a. PRAWDA
   b. FAŁSZ
2. Jaka metryka jest używana w protokole RIP?
   a. Koszt
   b. Liczba przeskoków
   c. Stopień wykorzystania łączy

3. Jaki jest dystans administracyjny dla protokołu RIP?
   a. 90
   b. 100
   c. 110
   d. 120
4. Zarówno protokół RIPv1, jak i protokół RIPv2 używają adresu rozsyłania grupowego jako adresu docelowego.
   a. PRAWDA
   b. FAŁSZ

   Dopasuj licznik czasu do jego wartości:

5. Odświeżanie A. 180
6. Przeterminowanie trasy B. 120
7. Odśmiecanie (na podstawie dokumentu RFC) C. 30
8. Reguła podzielonego horyzontu nakłania routery do przekazywania całej tablicy routingu we wszystkich kierunkach.
   a. PRAWDA
   b. FAŁSZ
9. W przypadku zatrutej trasy metryka ma wartość 16.
   a. PRAWDA
   b. FAŁSZ
10. Protokół RIP nie może być używany w topologiach zawierających pętle.
    a. PRAWDA
    b. FAŁSZ

Odpowiedzi do pytań sprawdzających

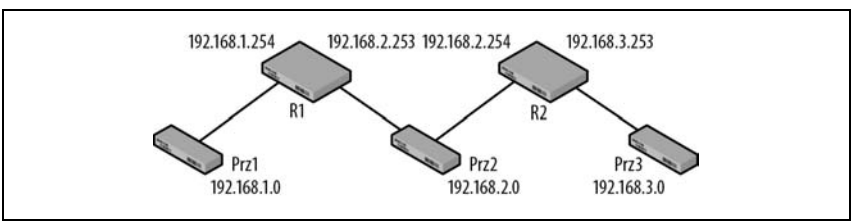
1. PRAWDA
2. b. Liczba przeskoków
3. d. 120
4. FAŁSZ
5. c. 30

6. a. 180
7. b. 120
8. FAŁSZ
9. PRAWDA
10. FAŁSZ

Ćwiczenia laboratoryjne

Ćwiczenie 1. Zbuduj topologię przedstawioną na rysunku 5.28

Materiały: dwa routery, dwa komputery, opcjonalne przełączniki (lub sieci VLAN) dla każdej sieci.



Rysunek 5.28. Topologia do ćwiczenia 1.

1. Połącz urządzenia kablami zgodnie z zadaną topologią i skonfiguruj adresy IP dla interfejsów routerów.
2. Podłącz po jednym komputerze do sieci `192.168.1.0` i do sieci `192.168.2.0`.
3. Skonfiguruj ręcznie adresy IP i bramy dla komputerów.
4. Czy w przypadku komputera w sieci `192.168.2.0` ma znaczenie, która brama domyślna jest używana? Dlaczego? Co się dzieje po uruchomieniu protokołu RIP?
5. Zbadaj tablice trasowania w routerach. Co zawierają? Przydatne polecenie dla urządzeń firmy Cisco: `show ip route`.

Ćwiczenie 2. Uaktywnij protokół RIP w routerach

Materiały: topologia z ćwiczenia 1., program Wireshark.

1. W każdym z routerów skonfiguruj używanie protokołu RIP. Użyj wersji 2 protokołu.
2. Przydatne polecenia dla urządzeń Cisco: `router rip`, `network _____`, `version`.
3. Przechwytuj ruch w obydwu komputerach i obserwuj, kiedy zaczną przepływać pakiety protokołu RIP. Kiedy konfiguracja zostanie zakończona, sprawdź ponownie zawartość tablic trasowania routerów.
4. Co się zmieniło w tablicach trasowania routerów? Jakie wartości znajdują się w nawiasach? Dlaczego?
5. Czy fakt, że w sieci jest aktywny protokół RIP, ma coś wspólnego z tablicami trasowania hostów?

Ćwiczenie 3. Podzielony horyzont

Materiały: topologia z ćwiczenia 1., program Wireshark.

1. Co to jest podzielony horyzont? A czym jest podzielony horyzont z zatruciem wstecz?
2. Zbadaj zawartość pakietów przechwyconych w sieciach topologii używanej w ćwiczeniu i znajdź dowody świadczące o tym, że metoda podzielonego horyzontu jest aktywna albo że nie jest aktywna.

Ćwiczenie 4. Utrata trasy

Materiały: topologia z ćwiczenia 1., program Wireshark.

1. Przy uruchomionym przechwytywaniu pakietów przez program Wireshark odłącz kabel łączący router R2 z siecią `192.168.3.0`.
2. Jaki ruch jest generowany w wyniku tego zdarzenia? Jak szybko pojawiły się te pakiety?
3. Zbadaj zawartość pakietów. Czy pojawiło się coś istotnego w informacjach dotyczących sieci `192.168.3.0`?
4. Przywróć poprzednią topologię dla potrzeb następnego ćwiczenia.

Ćwiczenie 5. Liczniki czasu

Materiały: topologia z ćwiczenia 1., program Wireshark, przełącznik pomiędzy routerami R1 i R2.

1. Monitoruj częstość, z jaką pakiety protokołu RIP są wysyłane przez routery. Czy odpowiada ona wartości licznika czasu opisanego w tym rozdziale?
2. Przy uruchomionym przechwytywaniu pakietów przez program Wireshark odłącz kabel łączący router R2 z siecią `192.168.2.0`. Jeśli patrzeć z perspektywy routera R2, jakie są różnice między aktualnym działaniem a działaniem zaobserwowanym w poprzednim ćwiczeniu?
3. Monitoruj tablicę trasowania routera R1. Jak dużo czasu upłynie, zanim zniknie pozycja dotycząca sieci `192.168.3.0`?
4. Czy w wyniku tego rozłączenia pojawiła się jakaś zmiana w pakietach? Wskazówka: czy router R2 sądzi, że sieć `192.168.3.0` jest nieczynna?
5. Jakie dokładnie liczniki czasu są związane z routerem R1? Przydatne polecenie dla urządzeń Cisco: `show ip protocol`.

Skorowidz

G

H

I

K

L

Ł

M

N

O

P

R

S

T

U

V

W

Ż

Sieci komputerowe

O'REILLY®

Routing i switching. Praktyczny przewodnik

Bez zaawansowanych mechanizmów trasowania i przełączania sieć – taka, jaką znamy – nie miałaby szans zaistnieć. To właśnie te mechanizmy gwarantują, że nasze dane docierają w odpowiednie miejsce. Niezwykle istotne jest więc ich zrozumienie i wykorzystanie w praktyce. Dzięki temu Twoja sieć będzie bardziej niezawodna, a użytkownicy bardziej zadowoleni.

W trakcie lektury tej wspaniałej książki zdobędziesz bezcenne informacje na temat strategii trasowania i przełączania, protokołu drzewa rozpinającego oraz sieci VLAN. Poznasz dogłębnie protokół RIP w wersji 1 i 2 oraz protokół OSPF. Autor na każdym kroku stara się uwypuklić zagadnienia związane z bezpieczeństwem tych rozwiązań, a przygotowane ćwiczenia laboratoryjne pozwolą Ci jeszcze lepiej zrozumieć poruszane problemy. Jeżeli Twoje codzienne zadania są związane z sieciami komputerowymi, ten przewodnik jest Twoją obowiązkową lekturą na najbliższe dni!

Dzięki tej książce:

- poznasz strategie trasowania i przełączania
- zobaczysz różnice pomiędzy wersją 1 i 2 protokołu RIP
- sprawdzisz atuty protokołu OSPF
- poprawisz bezpieczeństwo w Twojej sieci

Opanuj zagadnienia sieciowe dzięki uniwersalnym zasadom!

ISBN 978-83-246-5119-1

Cena 49,00 zł

9 788324 651191