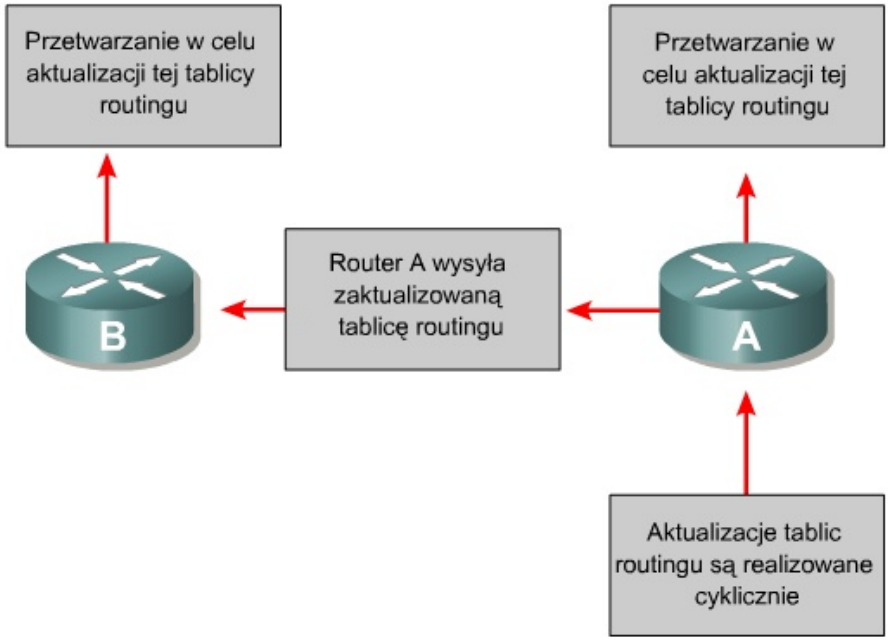
3. Routing z wykorzystaniem wektora odległości, RIP

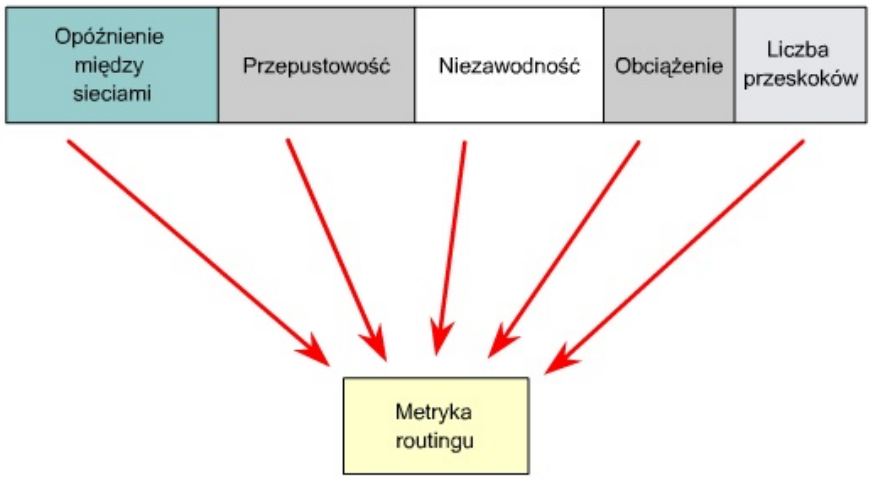
3.1. Aktualizacje routingu z wykorzystaniem wektora odległości

W routingu z wykorzystaniem wektora odległości tablice routingu są aktualizowane okresowo. W przypadku protokołu routingu bardzo ważne jest efektywne uaktualnianie tablic routingu. Tak jak w przypadku procesu wykrywania sieci, aktualizacje zmian są przesyłane systematycznie między routerami. Algorytmy działające z wykorzystaniem wektora odległości wymagają, aby każdy router wysłał całą swoją tablicę routingu do wszystkich przyległych sąsiadów.



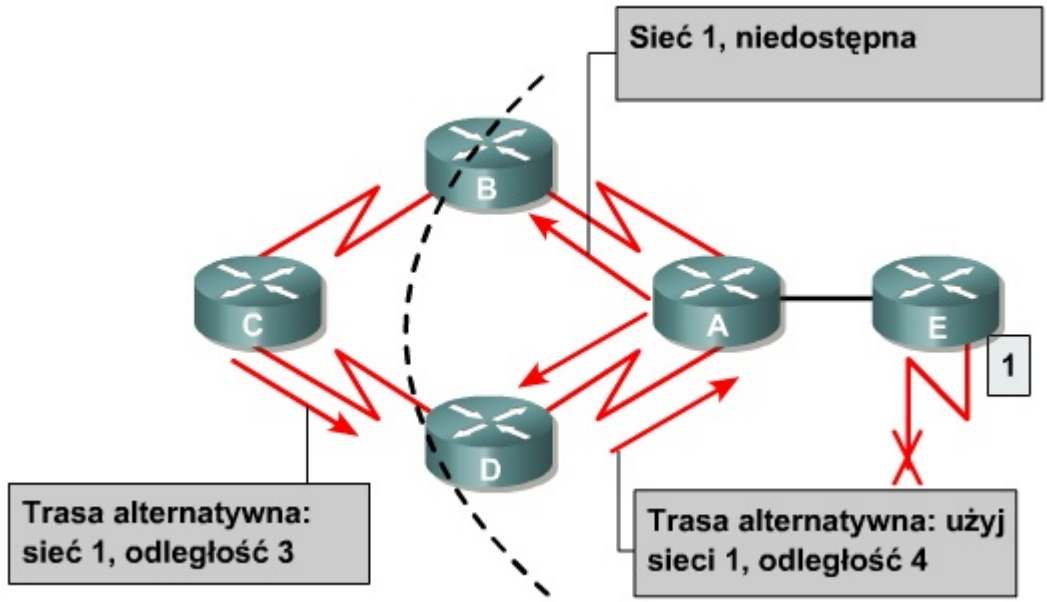
3.2. Metryki w routingu z wykorzystaniem wektora odległości

Na poniższym rysunku znajduje się wypis metryk, które mogą być wykorzystywane przez protokoły routingu:



3.3. Pętle routingu w protokołach z wykorzystaniem wektora odległości

Pętle routingu mogą powstawać, gdy niespójne tablice routingu nie są aktualizowane z powodu wolnej zbieżności w zmieniającej się sieci.

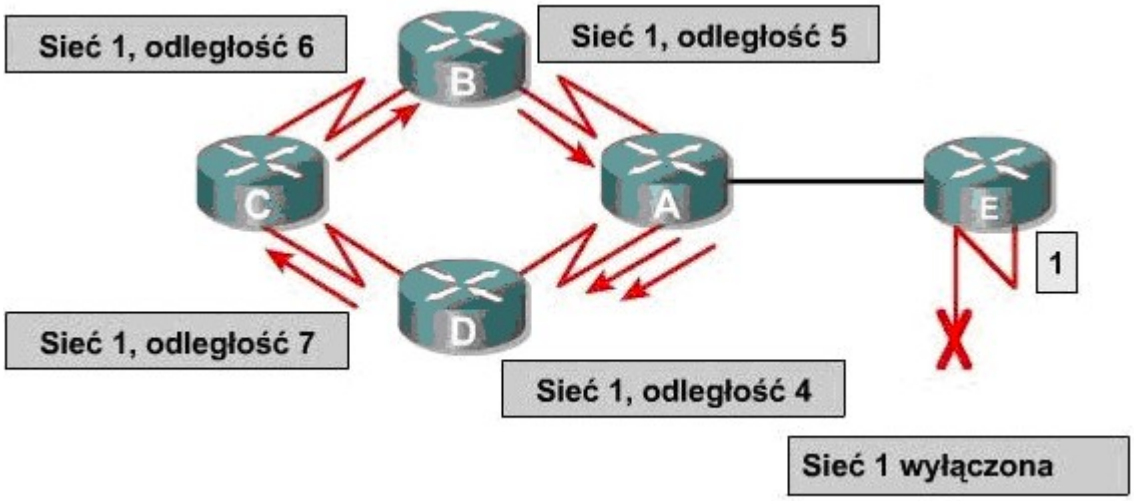


Przykład:

1. Tuż przed awarią sieci 1 wszystkie routery miały spójne informacje oraz prawidłowe tablice routingu. Sieć jest w stanie zbieżności. W przypadku routera C preferowana ścieżka do sieci 1 prowadzi przez router B, a odległość od routera C do sieci 1 wynosi 3.
2. Po awarii sieci 1 router E wysyła aktualizację do routera A. Router A przerywa wysyłanie pakietów routingu do sieci 1, ale routery B, C i D kontynuują wysyłanie, ponieważ nie zostały jeszcze poinformowane o awarii. Po wysłaniu aktualizacji przez router A routery B i D przerywają routing do sieci 1. Router C jeszcze nie otrzymał aktualizacji. Z punktu widzenia routera C sieć 1 jest nadal dostępna poprzez router B.
3. Teraz router C wysyła cykliczną aktualizację do routera D, która wskazuje ścieżkę do sieci 1 prowadzącą przez router B. Router D zmienia swoją tablicę routingu, aby uwzględnić tę nieprawidłową informację, a następnie wysyła informacje do routera A. Router A wysyła informacje do routerów B i E. Proces ten jest kontynuowany. Każdy pakiet przeznaczony dla sieci 1 będzie krążył w pętli od routera C do B, do A, do D i z powrotem do C.

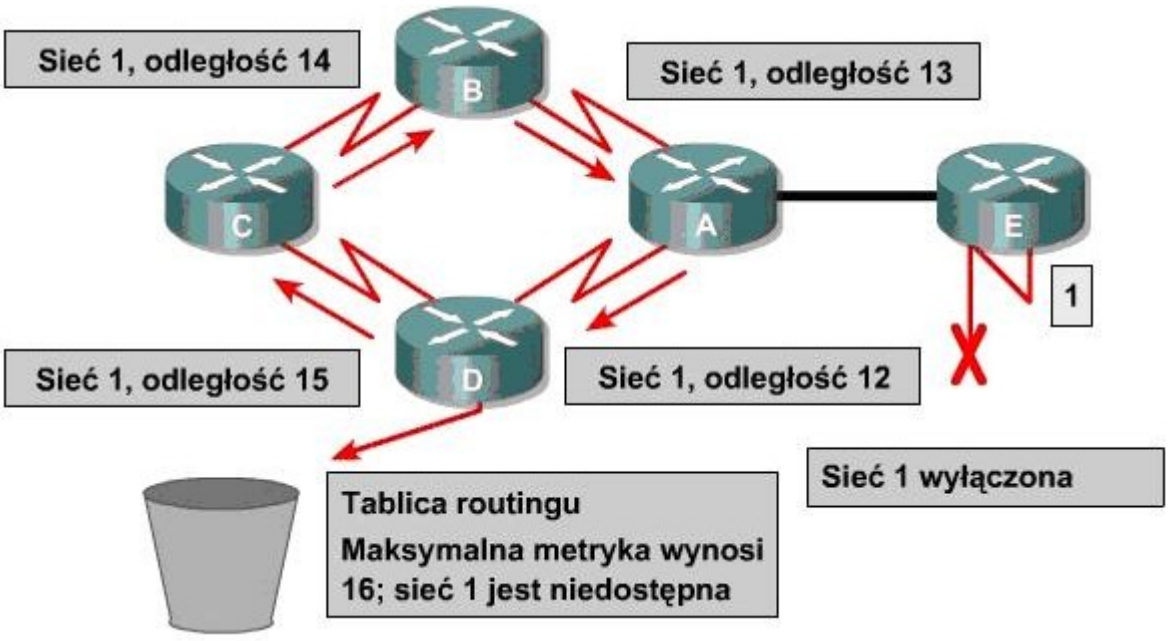
3.4. Definiowanie maksymalnej liczby przeskoków

Nieprawidłowe aktualizacje informacji o sieci 1 będą krążyć w pętli, dopóki inny proces tej pętli nie zlikwiduje. Sytuacja ta, nazywana odliczaniem do nieskończoności, powoduje krążenie pakietów w pętli pomimo tego, że sieć docelowa, którą jest sieć 1, nie działa. Podczas gdy routery odliczają do nieskończoności, nieprawidłowe informacje podtrzymują istnienie pętli routingu.



Bez podjęcia stosownych kroków, które miałyby na celu zatrzymanie procesu odliczania do nieskończoności, liczba przeskoków określona metryką wektora odległości wzrasta z każdym przejściem pakietu przez kolejny router. Pakiety te krążą w sieci, ponieważ tablice routingu zawierają nieprawidłowe informacje.

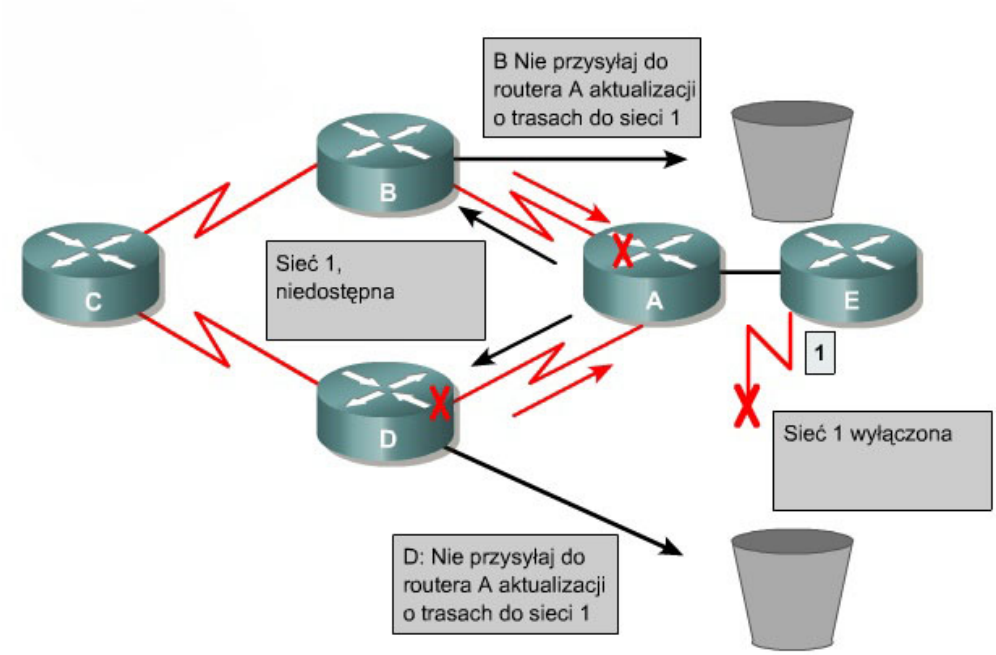
Aby uniknąć takiej sytuacji, w protokołach działających z wykorzystaniem wektora odległości nieskończoność jest zdefiniowana jako pewna liczba maksymalna. Liczba ta jest powiązana z metryką routingu, którą może być po prostu liczba przeskoków.



Dzięki temu pętla routingu istnieje do chwili przekroczenia przez metrykę dopuszczalnej wartości maksymalnej. Na rysunku wartość metryki wynosi 16 przeskoków. Gdy wartość metryki przekroczy wartość maksymalną, sieć 1 zostanie uznana za niedostępną.

3.5. Eliminacja pętli routingu przy użyciu metody split horizon

W celu uniknięcia pętli routingu stosowana jest także metoda split horizon (podzielony horyzont). Polega ona na nie wysyłaniu informacji o sieci z powrotem do routera, od którego przyszła informacja, że dana sieć jest niedostępna.



Jeśli aktualizacja o sieci 1 przybywa z routera A, routery B i D nie mogą wysłać informacji o sieci 1 z powrotem do routera A. Reguła split horizon zmniejsza liczbę nieprawidłowych informacji oraz narzut routingu.

3.6. Metody: route poisoning i poison reverse

Metoda route poisoning polega na nadaniu niedostępnej trasie metryki o jeden większej niż maksymalna, dopuszczalna wartość. Jest to tzw. „zatruwanie" trasy. „Zatruta" trasa traktowana jest przez rozgłaszające ją routery jako niedostępna.

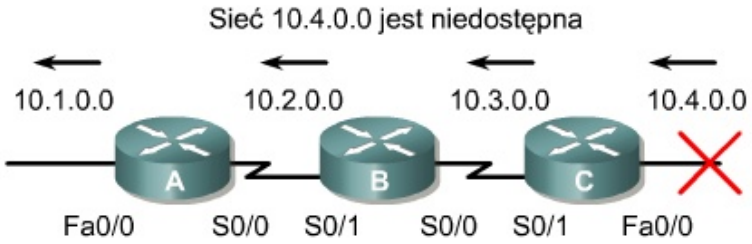
Metoda poison reverse pozwala routerom wbrew metodzie split horizon rozgłaszać informacje na temat danej trasy otrzymane z pewnego interfejsu ponownie na dany interfejs. Jednakże informacje te mogą dotyczyć tylko trasy „zatrutej".

Routery, które posiadają informacje o lepszej trasie prowadzącej do danej sieci, ignorują informacje o „zatrutej" trasie otrzymane z innych interfejsów.

3.7. Użycie wyzwalanych aktualizacji w celu uniknięcia powstawania pętli routingu

Wyzwalane aktualizacje są wysyłane natychmiast, gdy wystąpi zmiana w tablicy routingu. Użycie wyzwalanych aktualizacji razem z metodą route poisoning powoduje, że

wszystkie routery wiedzą o awariach ścieżek przez upłynięciem czasu na dowolnym zegarze przetrzymania (o zegarach przetrzymania jest mowa w następnym podrozdziale).



Router C wysyła wyzwalaną aktualizację, która zawiera informację o tym, że sieć 10.4.0.0 jest niedostępna. Po otrzymaniu tej informacji router B ogłasza na interfejsie S0/1, że sieć 10.4.0.0 nie działa. W odpowiedzi router A wysyła aktualizację poprzez interfejs Fa0/0.

3.8. Zapobieganie występowaniu pętli routingu przy użyciu zegarów przetrzymania (hold down)

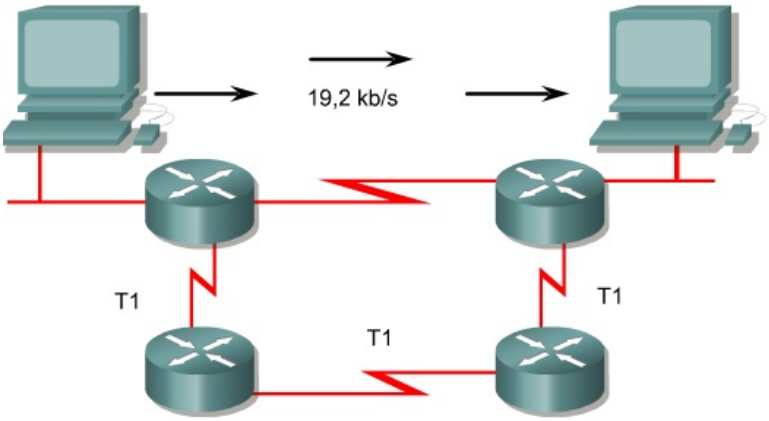
- Gdy router otrzymuje od sąsiada aktualizację, która wskazuje, że dotychczas dostępna sieć jest niedostępna, oznacza tę sieć jako niedostępną i uruchamia zegar przetrzymania. Jeśli przed upływem czasu na zegarze przetrzymania odbierze od tego samego sąsiada aktualizację, która wskazuje, że sieć jest znowu dostępna, oznacza ją jako dostępną i usuwa zegar przetrzymania.
- Jeśli od innego sąsiedniego routera odebrana zostanie aktualizacja zawierająca lepszą metrykę dla tej sieci, router oznacza tę sieć jako dostępną i usuwa zegar przetrzymania.
- Jeśli przed upłynięciem czasu zegara przetrzymania od innego routera zostanie odebrana aktualizacja z większą metryką, zostanie ona zignorowana. Aktualizacja ta jest ignorowana, aby przedłużyć czas propagacji w sieci informacji o szkodliwej zmianie.

3.9. Protokół RIP - podstawowe informacje

Protokół RIP został zaprojektowany jako protokół IGP w systemach autonomicznych o średniej wielkości. Nie jest przeznaczony do bardziej złożonych środowisk. Istnieją dwie wersje protokołu RIP: wersja 1 i wersja 2.

Obydwie wersje protokołu wykorzystują wektor odległości, rozgłaszający całą tablicę routingu do wszystkich sąsiednich routerów w określonych odstępach czasu. Domyślna wartość interwału wynosi 30 sekund. Jako metryki protokół RIP używa liczby przeskoków. Maksymalna liczba przeskoków wynosi 15. W celu zapobieżenia powstawaniu pętli routingu są wykorzystywane zegary przetrzymania. Wartość domyślna zegara wynosi 180 sekund. W tym samym celu jest używana metoda split horizon.

RIP został opracowany przez firmę *Xerox Network Systems*. Swoją dużą popularność zawdzięcza programowi (demonowi Unix'owemu) *routed* opracowanemu w *University of California* w *Berkeley*. Ponieważ *routed* wchodzi w skład wielu systemów Unix'owych, stał się w sposób naturalny najczęściej stosowanym programem tego typu.



Należy zaznaczyć, że protokół RIP został opracowany pod kątem wykorzystania go wyłącznie w sieciach lokalnych, jednak ze względu na popularność, jaką zdobył stosowany jest obecnie także w sieciach rozległych.

Ograniczenia protokołu RIP v1:

- W swoich aktualizacjach nie wysyła informacji o masce podsieci (jest protokołem klasowym);
- Aktualizacje wysyła w formie rozgłaszania na adres 255.255.255.255;
- Nie obsługuje uwierzytelniania.

3.10. Cechy protokołu RIP v2

Cecha	Opis
Razem z informacjami o trasie wysyła informacje o masce podsieci.	Aby umożliwić działanie techniki VLSM, protokół RIP razem z informacjami o każdej trasie wysyła informacje o masce, dzięki czemu podsieć jest dokładnie zdefiniowana.
Zapewnia uwierzytelnianie.	Protokół RIP umożliwia wykorzystanie zarówno jawnego tekstu, jak i szyfrowanie przy użyciu algorytmu MD5.
W wysyłanych aktualizacjach tras zamieszcza adres IP routera następnego przeskoku.	Router może ogłaszać trasę i kierować wszystkie routery nasłuchujące do innego routera w tej samej podsieci, który ma ustaloną lepszą trasę.
Wykorzystuje znaczniki tras zewnętrznych.	Protokół RIP może przekazywać informacje o trasach uzyskane ze źródła zewnętrznego i redystrybuowane następnie do tego protokołu. Mechanizm ten służy do oddzielania tras RIP od tras zidentyfikowanych na podstawie źródeł zewnętrznych.
Wysyła aktualizacje tras metodą rozsyłania grupowego.	Protokół RIP nie wysyła aktualizacji na adres 255.255.255.255. Docelowym adresem IP jest 224.0.0.9. Pozwala to zmniejszyć wymagania na moc obliczeniową hostów znajdujących się we wspólnej sieci, które nie korzystają z protokołu RIP.

3.11. Porównanie protokołów RIP v1 i v2

RIP v1	RIP v2
Jest łatwy w konfiguracji.	Jest łatwy w konfiguracji.
Obsługuje tylko klasowe protokoły routingu.	Obsługuje routing bezklasowy.
Wysyłane aktualizacje tras nie zawierają informacji o podsieciach.	Wraz z aktualizacjami tras wysyła informacje o maskach podsieci.
Nie obsługuje routingu z uwzględnieniem prefiksu, tak więc wszystkie urządzenia istniejące w jednej sieci muszą używać tej samej maski podsieci.	Po zastosowaniu techniki VLSM obsługuje routing z uwzględnieniem prefiksu, dzięki czemu różne podsieci w tej samej sieci mogą mieć różne maski podsieci.
Wysyłane aktualizacje nie mogą być uwierzytelniane.	Wysyłane aktualizacje mogą być uwierzytelniane.
Rozgłasza na adresie 255.255.255.255.	Aktualizacje tras są rozsyłane grupowo za pośrednictwem adresu klasy D 224.0.0.9, co zwiększa wydajność rozsyłania.

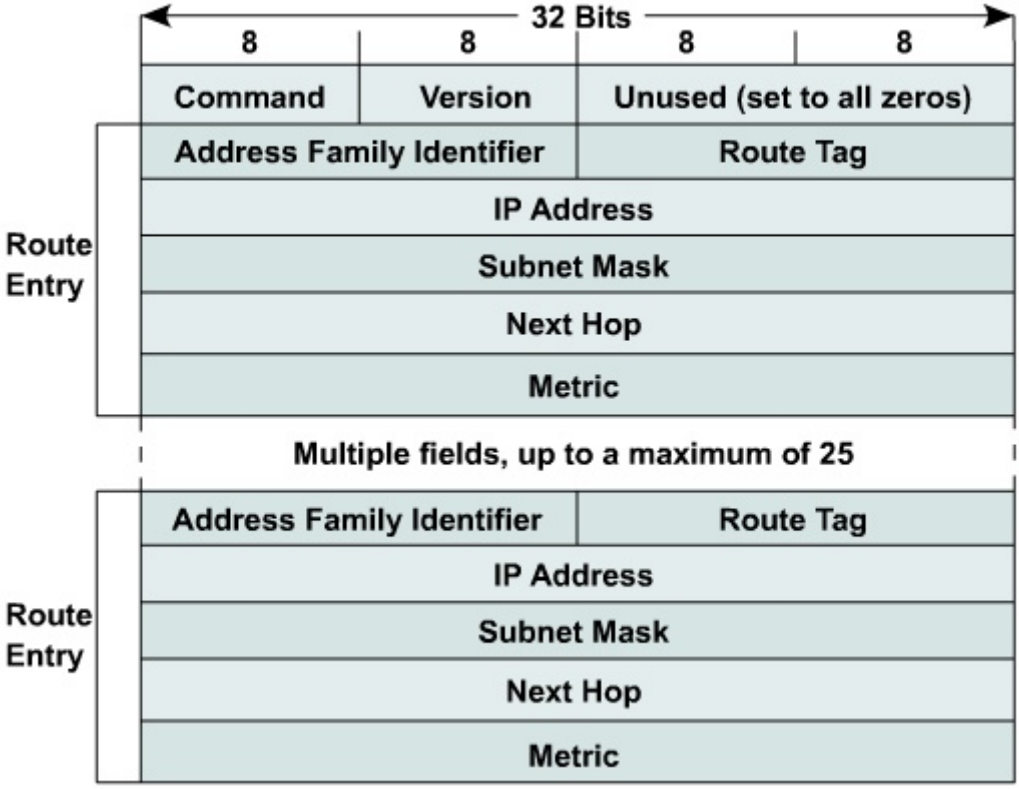
3.12. RIP - zależności czasowe

W celu dostosowania do potrzeb wydajności routingu, protokół RIP wyposażono w kilka zegarów (timers):

1. update timer (30 sekund): jak często router wysyła uaktualnienia do routerów sąsiednich. Zmniejszenie wartości zegara może przyspieszyć konwergencję sieci. Ponieważ jednak, zgodnie z założeniami protokołu RIP, do sąsiednich routerów przesyłana jest cała tablica routingu i może ona mieć duży rozmiar, zmniejszenie wartości zegara może spowodować poważne problemy związane z obciążeniem sieci na wolniejszych łączach;
2. invalid timer (90 sekund): czas po upływie, którego możemy przypuszczać, że trasa jest nieaktualna jeśli jednostka nie otrzyma ponowienia jej oferty, jeśli tak się stanie, trasa jest oznaczana jako niedostępna, lecz nie jest usuwana z tablicy routingu.
3. flush timer (270 sekund): czas po upływie, którego nastąpi wykasowanie informacji o trasie jeśli jednostka nie otrzyma ponowienia jej oferty.

3.13. RIP v2 - format komunikatów

Podstawowa struktura formatu komunikatów protokołu RIP v2 nie odbiega od tej stosowanej w RIP v1. Wszystkie rozszerzenia protokołu RIP v2 zostały umieszczone w nieużywanych polach protokołu RIP v1. Polami nieużywanymi w RIP v1 są: Route Tag, Subnet Mask i Next Hop. RIP v2 podobnie jak RIP v1 może zawierać do 25 wpisów o połączeniach oraz operuje na 520 porcie protokołu UDP, ma 4-bajtowy nagłówek, a maksymalna wielkość jednego datagramu to 512 bajtów.



Pole „Command” oznacza czy informacja została wygenerowana jako prośba (request - wartość 1) czy też odpowiedź (response - wartość 2). Aktualizacje okresowe i aktualizacje wyzwalane są wysyłane jako odpowiedzi.

Pole „Version” jest ustawione na 2 dla RIP v2. Jeśli jest ustawione na 0 lub 1 i komunikat nie jest prawidłowy z RIP v1, to jest on odrzucany. RIP v2 akceptuje właściwe komunikaty RIP v1.

Pole „Address Family Identifier” (AFI) jest ustawiane na 2 dla protokołu routowanego IP.

Pole „Route Tag” dostarcza możliwości rozróżnienia pomiędzy wewnętrznymi a zewnętrznymi ścieżkami. Wewnętrzna ścieżka to taka, która jest wyuczona przez RIP v2 w obrębie sieci lub systemu autonomicznego. Zewnętrzna ścieżka zaś - przez inne protokoły routingu. Sugerowane używane tego pola to numer systemu autonomicznego ścieżek zaimportowanych przez inne protokoły routingu.

Pole „IP Address” to adres IP przeznaczenia. To może być zarówno adres sieci jak i podsieci czy też po prostu hosta.

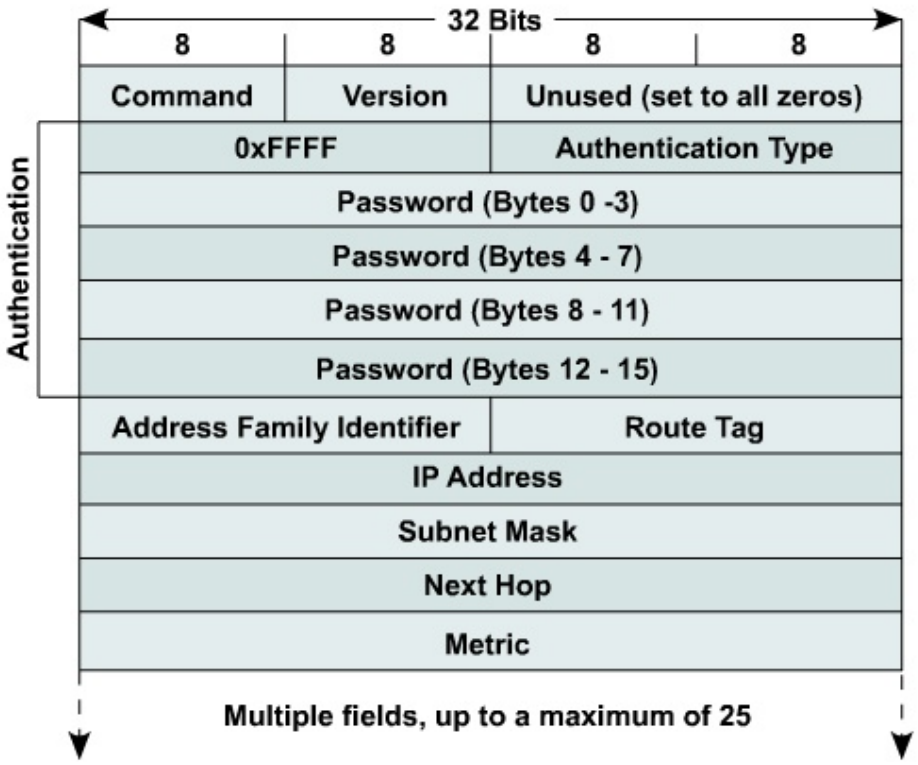
Pole „Subnet Mask” zawiera 32-bitową maskę, identyfikującą część sieciową adresu IP.

Pole „Next Hop” zawiera adres IP następnego przeskoku prowadzącego do adresu IP przeznaczenia.

Pole „Metric” oznacza ile już przeskoków zostało dokonanych z miejsca przeznaczenia do aktualnego routera. To pole przyjmuje wartości od 1 do 16, 16 oznacza, że ścieżka jest niedostępna.

3.14. Uwierzytelnianie

Uwierzytelnianie jest jednym z udoskonaleń protokołu RIP, które zostało wprowadzone w drugiej wersji standardu. Jeżeli router nie jest skonfigurowany by uwierzytelniać wiadomości RIP v2, to wiadomości RIP v1 i nie uwierzytelnione wiadomości RIP v2 będą akceptowane, zaś uwierzytelnione wiadomości RIP v2 będą odrzucone. Jeżeli router jest skonfigurowany do uwierzytelniania wiadomości RIP v2, to wiadomości RIP v1 i RIP v2, które przejdą uwierzytelnienie będą przyjęte, pozostałe będą odrzucone. Dla zwiększenia bezpieczeństwa wiadomości RIP v1 powinny być ignorowane, kiedy uwierzytelnianie jest włączone.



Uwierzytelnianie w RIP v2 jest rozwiązane poprzez modyfikację komunikatu. Obecność uwierzytelnionego komunikatu jest sygnalizowana poprzez ustawienie pola AFI na same jedynki. Z powodu niesienia informacji o haśle, komunikat może zawierać tylko do 24 wpisów. Hasło ma do 16 znaków i w komunikacie jest uzupełniane zerami z prawej strony (o ile jest krótsze).

Normalnie hasło jest przesyłane w formie czystego tekstu. Jednak ponieważ takie rozwiązanie jest mało bezpieczne, Cisco skorzystało z pola Authentication Type i umożliwia przesyłanie hasła zapisanego za pomocą szyfrowania MD5.

3.15. Uogólnianie tras w RIP

Jeśli kilka podsieci jednej sieci korzysta w routerze z tych samych tras i nie ma wśród nich innych podsieci korzystających z innych tras, to można zastosować uogólnienie tych podsieci do jednego adresu sieciowego.

Technika uogólniania tras ma dwie zasadnicze zalety. Po pierwsze, ogranicza rozmiar i złożoność tablicy routingu, co z kolei zmniejsza zajętość pamięci i przyspiesza przetwarzanie danych w routerach odbierających uaktualnienia. Po drugie, ukrywane informacje o podsieciach sprawia, że routery korzystające z danych nie są powiadamiane o okresowo niedostępnych interfejsach znajdujących się w innej części sieci, dzięki czemu działanie sieci staje się stabilniejsze. Minusem takiego uogólniania jest fakt, że podczas tego procesu nie ma ciągłości w adresach sieci. Jeżeli router rozpowszechnia informacje o uogólnionej trasie,

należy się upewnić, że żadna z podsieci wchodzących w skład sieci ogólnej nie znajduje się w tej części sieci, do której dane są wysyłane.

Protokół RIP v2 dokonuje automatycznego uogólniania tras z zakresu danej klasy sieci. Informacje o trasach do poszczególnych podsieci nie są wtedy przesyłane. Każde urządzenie odbierające dane z routera zostanie poinformowane jedynie o trasie ogólnej.

Należy pamiętać, że uogólnianie automatyczne działa tylko na podsieci w ramach sieci danej klasy.

Zawsze automatyczne uogólnianie w RIP v2 można wyłączyć i dokonać własnej konfiguracji uogólniania tras.