RFC2453 RIP Version 2

情報工学専攻 廣川研究室 修士 2 年 古賀 康則

平成 13 年 9 月 21 日

1 概要

RIPVersion2(以下 RIP2) はルーティングプロトコルの一つである。ルーティングとはネットワークにおいて、ルータがパケットを送信すべき方向へ正しく配送することである。したがってこのプロトコルはネットワーク上のルータで実装されている。RIP2 が対象にしているのは任意のホスト間のパスの長さが 15 を越えない程度の中小規模のネットワークである。

ルーティングに関する方針を決めているある程度の大きさのまとまりを自律システム (AS) と呼ぶ。ルーティングプロトコルの内、AS 内部で利用されるものを IGP(Interior Gateway Protocol)、AS 間で利用されるものを EGP(Exterior Gateway Protocol) と呼び、RIP2 は IGP の一種である。

RIP2 では距離ベクトルアルゴリズム (distance vector) に基づいてルーティングを行なう。ルータは宛先ネットワークへパケットを送るのに必要な情報をルート情報として表(ルーティングテーブル)にして格納している。隣り合うルータはルート情報を定期的に交換し、処理して、ルーティングテーブルを更新する。これにより最適なルートが求まるようなアルゴリズムになっている。しかし、ネットワークの変更や障害が発生した場合に、隣り合うルータ間のみでの情報交換とルート情報のタイマーによる管理のため、ルート情報が正しい状態に収束するのに時間かかる。このような問題を解決するために RIP が採用しているメカニズムについて簡単なネットワークを例にとって説明する。また、ルーティング情報の詳細や、ルート情報交換時のルーターの処理について述べる。

RIP を実装した代表的なプログラムは 4.3BSD で標準配布される routed で、最新のものは RIP2 にも対応している。また、gated や GNU の zebra などでも実装されている (http://www.zebra.org/)。

2 距離ベクトルアルゴリズム

RIP、RIP2 で採用されているルーティングアルゴリズムは距離ベクトルアルゴリズムと呼ばれる。ルータは配送すべきパケットの宛先とルーティングテーブルを参照し、どのルータ(方向)にパケットをフォワードするかを決定する。一般に宛先ネットワークへは複数のルートが存在すると考えられるが、どのルートを使うべきかはメトリック(距離)によって判断する。

RIP はルータを経由しない単一のネットワーク上、たとえばイーサネットにおける同一セグメント上のパケット配送については感知しない。

ルーティングテーブルの内容

ルーティングテーブルに保存される情報には次のようなものがある。

・ネットワークアドレス
・次ホップルータ
・インターフェース
・メトリック
・タイマー
・サブネットマスク

ネットワークアドレス

宛先ネットワークのアドレスである。ホストアドレスとはサブネットマスクによって区別することができる。

次ホップ

宛先ネットワークへのパケットを送信する時に利用する隣り合うルータ。

インタフェース

次ホップルータと共有しているネットワークに接続されたネットワークインタフェース。

メトリック

あるルートを利用した時にかかるコスト (距離) を表す。コストという概念には、物理的距離や時間、金銭的なコストなどが考えられるが、ここでは単純に宛先ネットワークまでのルータのホップ数である。回線の速度などを考慮して管理者が値を設定することも可能である。RIP では 1 から 15 が有効な値であり、16 より大きな値は存在せず、16 は到達不能と解釈される。RIP が対象としているのはこの制限に収まる程度のネットワークである。この制限は RIP のルーティングテーブルの収束を早めるためのものである。

タイマー

RIP ではルート情報をタイマーとフラグによって管理している。タイマーには 2 種類ある。ルータは３０秒ごとに自分の持つルート情報をアップデートメッセージとして、隣接するルータに送信する。タイマーのうち一つは隣接ルータが定期的にアップデートメッセージを送信しているかどうかを監視している。180 秒間隣接ルータからのメッセージが途絶えると、そのルートは無効であるというフラグをセットする。二つめのタイマーは無効になったルート情報を削除するかどうかを決定する削除タイマーである。無効フラグがセットされた後 120 秒間待ってルート情報を削除する。もし、この間に再びアップデートメッセージを受け取れば、フラグをリセットしてルート情報を復活させる。このように 2 段階のタイマーを持っているのはネットワーク上で偶然パケットが失われてしまった場合や一時的なネットワークの切断に対応するためである。

サブネットマスク

RIP2 では RIP のルート情報にサブネットマスクが追加されている。サブネットマスクは多数のネットワークが混在し、それぞれが異なるマスク値を持っている場合、ネットワークアドレスとホストアドレスを区別するために重要である。

RIP2 のパケットフォーマット

RIP2 は UDP ベースのプロトコルで送受信に 520 番のポートを利用する。パケットフォーマットは図 1 のようになる。各フィールドの括弧の数字はオクテット数を表している。ヘッダ部分のコマンドフィールドには 1 または 2 が入る。1 はリクエストパケットを表し、2 はレスポンスパケットを表す。通常のアップデートメッセージはレスポンスパケットである。リクエストパケットはルータが起動直後にルート情報を要求する場合などに利用される。

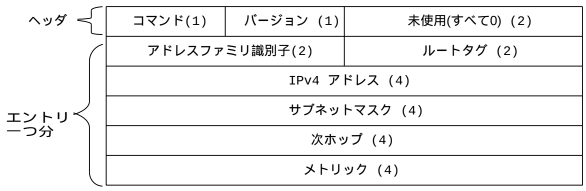

図 1: RIP2 のパケットフォーマット

エントリ部分は 25 個分が 1 つのパケットに入るが、4 節で述べる認証機能を用いる場合には最初のエントリを除く 24 個分となる。

アップデートメッセージの処理

アップデートメッセージは隣接するルータに３０秒毎に送信される。その中に、既にルーティングテーブルに登録してある宛先のルート情報よりも、メトリックが優れているものがあれば採用する。また、宛先と次ホップルータが同じでもメトリックが変更されていれば、ルーティングテーブルを更新する必要がある。ルータがアップデートメッセージを受け取った時の動作をまとめると図 2 のようになる。アップデートメッセージを受け取り、パケットにあるルート情報のエントリを順に一つずつ処理していく。

3　ルート情報の変化

ネットワークに変更があった場合や、障害などによってルートが消滅してしまった場合にはルート情

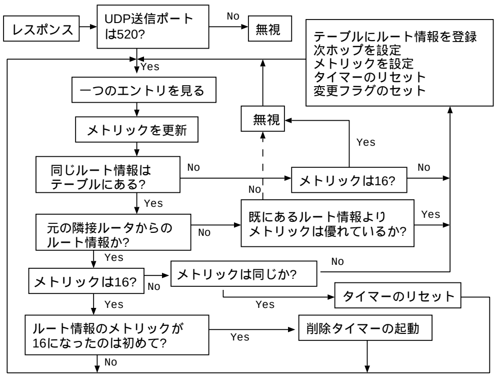

図 2: アップデートメッセージの処理

報は自動的に最適な状態へ収束する。しかし、ルート情報の収束には時間がかかるため、RIP は収束を早めるためにスプリットホライズンやポイズンドリバース、トリガー更新のメカニズムを持っている。ここではそれらを説明するために図 3 のようなネットワークについて考察する。

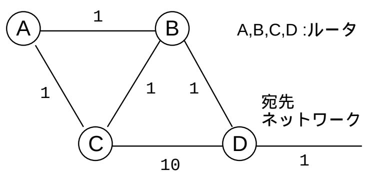

図 3: 障害発生とその処理

図 3 において A,B,C,D の各ルータから右側の宛先ネットワークへのルート情報を考える。ルータを結ぶリンクのメトリックは 1 とする。ただし、例外的に C,D 間のリンクについては 10 としておく。初期状態では表 1 のようになっている。

表 1: 各ルータにおける宛先ネットワークへのルート情報

ルータ	隣接ルータ	メトリック
D	直接	1
B	D	2
C	B	3
A	B	3

B と D が共有するネットワークに障害が発生した場合を考えてみる。この場合には自動的に C から D へのネットワークを利用するようにルート情報を更新しなければならない。ルート情報の変更は B が D へのルートのメトリックを 16（到達不能）として送信することで始まる。簡単のためにルート情報の送信は全てのルータで同時であると考えると、ルート情報の変化は表 2 のようになる。この表では時間の経過を左から右に表している (dir は直接接続、unreach は到達不能)。

ルータ B はルート情報のタイムアウトによって D と共有するネットワークの障害を知ることができるので、A または C から送信されたメトリック 4 のルートを新たに採用する。（ここでは C とする）A,C は互いに B を利用するメトリック 4 のルート情報を送信しあっているので、B から送られて来たメトリック 16 のルート情報を破棄し、相互にルート情報を採用する。次のアップデートでは、B は A または C から送信されたルートのメトリックが更新されているのでこれを採用する。A,C は先程と同様に更新されたメトリック 5 のルートをお互いに送信し、お互いにルーティングテーブルを更新する。このようなルート情報のループが発生すると、ルート情報の収束が遅れてしまう。

表 2: ルート情報の変化

D	dir,1	dir,1	dir,1	dir,1	...	dir,1	dir,1
B	unreach	C,4	C,5	C,6	...	C,11	C,12
C	B,3	A,4	A,5	A,6	...	A,11	D,11
A	B,3	C,4	C,5	C,6	...	C,11	C,12

スプリットホライズン

問題は A や C が相互にお互いを経由するルートを送信しあっているところにある。スプリットホライズンは受け取ったルート情報を、それを送信した相手に送る自分のアップデートメッセージに含めないという簡単な約束である。これによってループの発生を抑えることができる。

ポイズンドリバース

ポイズンドリバースは、受け取ったルート情報を、それを送信した相手に送る自分のアップデートメッセージでメトリックを 16 にして送るという方法である。この場合は障害が発生した時点で宛先ネットワークへ経由できるルータそうでないルータが区別されているため、ルート情報の収束が早くなる。

しかし、欠点もある。それは、到達不能なルート情報も隣接ルータに送信するためにアップデートメッセージが肥大化することである。

トリガー更新

スプリットホライズン、ポイズンドリバースは二つのルータ間でおきるルート情報のループを防ぐことができる。しかし、例えば A が B を経由するルート、B が C を経由するルート、C が A を経由するルートを互いに送信しあうような、三つ以上のルータが関係するループには役に立たない。このようなループはメトリックが到達不能になるまで収束しない。トリガー更新はこの収束を早めるための仕組みである。ルート情報の更新規則に「メトリックを更新する場合はアップデートメッセージを即座に隣接ルータに送信する」という規則を付け加えることで実現できる。

4 RIP2 のその他の機能

RIP から RIP2 になった時に機能がいくつか追加されている。サブネットマスクについては 2 節のルート情報の所で説明した。

ルートタグ

ルートタグは拡張のために用意されているフィールドで、RIP ドメインで一貫性を持った使い方をすれば任意の値を設定しても良い。このフィールドは AS 間のルーティングプロトコルである EGP や BGP などと組み合わせて利用することも可能である。

認証機能

RIP2 では認証のために最初のエントリを利用することができる。この場合は最初のエントリが図 4 のようなフォーマットになっている。

0xFFFF(2)	認証タイプ（2）
認証文字列（16）	

図 4: 認証部分のフォーマット

エントリの最初の部分には 0xFFFF をいれる決まりになっている。認証タイプのフィールドに入る値は現在のところタイプ 2 の簡易パスワードだけが設定できる。したがって認証文字列のフィールドには平分のパスワードが入ることになる。

次ホップ

このフィールドはルーティングの際にパケットの余計なホップを減らす目的で利用される。例えば、RIP と OSPF が混在する場合、OSPF を実装したルータを経由するためには、同じネットワーク上の少なくとも 1 つのルータで RIP と OSPF の両方のプロトコルを実装する必要がある。OSPF を実装するルータを次ホップフィールドにいれておけば、直接パケットを送信できる。

マルチキャスト

RIP ではアップデートメッセージを隣接するルータにブロードキャストによって送信する。しかしこの方式はルーティングに無関係なホストなどにもパケットを送信し、余計な処理を要求してしまう。RIP2 では、224.0.0.9 というマルチキャストアドレスをつかってルーティングに関係するルーターにだけ、パケットを送信することが可能である。

5 まとめ

RIP2 は中小規模のネットワークに向いたルーティングプロトコルである。距離ベクトルアルゴリズムに基づき、定期的にルーティング情報を交換することで、自動的に最適なルート情報を求めることができる。しかし、タイマーによってルート情報を管理しているために、一旦変更が発生するとルート情報の収束に時間がかかるため、ホップ数 16 に制限し到達不能としなければならなかった。また、ルータ間でルート情報のループが発生した場合には、収束を早めるために 3 節で述べた仕組みを導入していた。今日のネットワークでも利用可能とするため、RIP に可変長サブネットマスクや認証機能などが導入されている。