Universidade Federal do Rio de Janeiro
Departamento de Engenharia Eletrônica

Aluno: Pedro Magalhães Ascenção
Professor: Otto Duarte
Disciplina: Redes I

Protocolos de Roteamento - RIP

- Introdução

Roteamento é um processo que tem como objetivo determinar por onde mandar um pacote destinado a um endereço fora da rede local. Cabe aos roteadores manter e divulgar as informações de roteamento que possibilitem a transmissão e recebimento destes pacotes. Todas estas informações ficam armazenadas na tabela de roteamento, sendo que cada linha desta tabela corresponde a uma rede identificada. O administrador da rede pode estaticamente (manualmente) configurar linhas desta tabela ou pode configurar o roteador para que este utilize protocolos de roteamento para criar e atualizar sua tabela dinamicamente, fazendo com que o roteador perceba mudanças na rede assim que elas ocorrem. Para se ter um gerenciamento de uma rede IP mais eficiente, deve-se entender como os diversos protocolos de roteamento operam e, entender também, os benefícios e limitações de cada protocolo.

- Utilização

Quando devem ser utilizados (rotas estáticas x rotas dinâmicas) ?

Existem duas maneiras de se configurar um roteador para "ensina-lo" como transmitir um pacote para uma rede que não está diretamente conectada a ele. Pode-se utilizar rotas estáticas ou rotas dinâmicas (esta, utiliza protocolos de roteamento).
Na rota estática é necessário que o administrador diga para o roteador como chegar a uma dada rede. Sempre que houver alterações na rede o administrador deve manualmente fazer as atualizações no roteador. A simples adição de uma nova rota, exigiria a alteração das tabelas de roteamento em todos os roteadores da rede. Com isso é possível ver que a configuração manual das tabelas de roteamento é um método que somente se aplica a pequenas redes, com um número reduzido de roteadores e de rotas. Por outro lado, rotas configuradas manualmente permitem que se tenha um controle bem preciso sobre o comportamento de roteamento desta rede IP.
Já nas rotas dinâmicas, o roteador dinamicamente aprende rotas (uma vez que o administrador configurou um protocolo de roteamento nele). Diferente das rotas estáticas, após o administrador configurar o roteamento dinâmico, o roteador automaticamente atualiza suas rotas sempre que alguma mudança na rede for informada. Os roteadores aprendem e mantém suas tabelas de roteamento atualizadas através da troca de pacotes de atualizações entre eles.

Rotas estáticas são bastante utilizadas em redes *stub* e como gateways de saída para onde todos os pacotes com destino desconhecido serão mandados. Denomina-se rede *stub,* uma rede acessada por um único roteador como na figura abaixo.

Na figura, o roteador A será configurado com uma rota estática para alcançar a rede 172.16.1.0 através de sua interface serial. Já o roteador B deve ser configurado com uma rota estática, ou melhor, rota padrão para alcançar as redes atrás do roteador A, através de sua serial.

Como mencionado acima, existe um tipo especial de rota estática conhecida como rota padrão (*default route*). Esta rota serve para o roteador enviar qualquer pacote cujo destino não se encontre em sua tabela de roteamento.

- Classificação

Existem algumas maneiras de se classificar um protocolo de roteamento. Uma delas seria quanto a localidade onde ele é empregado. Para entender esta classificação deve-se conhecer o conceito de sistema autônomo (*autonomous system* ou SA).

Sistema autônomo: É um conjunto de redes sob uma mesma administração.

Existem dois grandes conjuntos de protocolos de roteamento.

IGP (*Interior Gateway Protocols*) - Conjunto de protocolos que são utilizados para comunicação intra SA, ou seja, usados para comunicação entre roteadores dentro de um mesmo sistema autônomo. Os principais exemplos deste grupo são RIP, IGRP, OSPF, entre outros.

EGP (*Exterior Gateway Protocols*) - Conjunto de protocolos que são utilizados para a comunicação inter AS, ou seja, usados para a comunicação entre roteadores que se encontram em diferentes sistemas autônomos. São usados para que todos os sistemas autônomos pela Internet mantenham informações atualizadas para garantir o funcionamento do roteamento global. O principal exemplo deste grupo seria o BGP.

Outra forma de se classificar os protocolos de roteamento é quanto ao algoritmo por ele utilizado. Existem dois grupos:

a) **Vetor distância** (*Distance vector*): Também conhecido como algoritmo de Bellman-Ford, este grupo trabalha baseado na idéia que cada roteador propaga periodicamente uma tabela com todas as redes conhecidas e a distância para alcançá-las. Geralmente, a distância é calculada pelo número de "saltos" (*hops*) necessários para alcançar uma determinada rede. Logo, diz-se que a métrica que este grupo utiliza para a escolha do melhor caminho é o número de "saltos". O termo "saltos" significa a passagem entre um roteador e outro. Vale lembrar também, que cada roteador ao receber as informações de outras redes incrementa o número de "saltos" e anuncia as rotas divulgadas para os demais roteadores.

b) **Estado de enlace** (*Link state*): Este algoritmo trabalha baseado na idéia de que cada roteador possui informações sobre as redes que estão conectadas a ele e, periodicamente, testa para determinar se cada enlace está ativo. Com estas informações cada roteador divulga uma lista sobre o status de cada conexão, dizendo se estas estão ativas ou inativas. Baseado nessas informações, quando um roteador recebe um conjunto de mensagens sobre o estado dos enlaces das redes próximas a ele, é aplicado o algoritmo SPF de Dijskstra (*Shortest Path First*). Este algoritmo é aplicado baseado nas informações de cada roteador e é feito localmente a cada um destes, para o cálculo das melhores rotas para todos os destinos a partir de uma mesma origem. É como se cada roteador montasse internamente a topologia da rede em torno dele, sabendo todas as rotas existentes para um dado destino.

- RIP

O RIP (*Routing Information Protocol*) foi um dos primeiros protocolos IGP e foi muito popularizado pela implementação da ferramenta routed, muito usada em sistemas UNIX 4BSD. Este protocolo é derivado de um protocolo da Xerox para redes locais. Basicamente, ele trata da implementação direta do algoritmo de vetor distância. A RFC do RIP, saiu em 1988 (RFC 1058).

Por ser baseado no algoritmo de vetor distância, este protocolo envia copias periódicas de sua tabela de roteamento para seus vizinhos diretamente conectados (utiliza o endereço *broadcast* de cada rede diretamente conectada). Roteadores que estão utilizando esse protocolo enviam atualizações periódicas mesmo que não ocorram alterações na rede.
As mensagens periódicas do RIP são cópias da tabela de roteamento completa de cada roteador. Quando um roteador recebe a tabela de roteamento completa de seu vizinho, ele verifica cada rota, acrescentando as que ele ainda não conhecia em sua tabela e comparando as já existentes para escolher aquela com o menor número de saltos para colocar em sua tabela ou atualizar entradas já existentes.

Porém existem situações onde ocorre a transmissão de informações erradas. A seguir vamos mostrar um caso destes, assim como as ferramentas utilizadas pelo RIP para tentar evitar tais inconsistências.

Temos o ambiente abaixo.

Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

Ocorre, porém, uma falha e a rede 10.4.0.0 não está mais disponível. O roteador C, diretamente conectado a esta rede, detecta a falha e para de enviar pacotes para ela. Porém, os roteadores A e B ainda não receberam o aviso de que a rede 10.4.0.0 caiu. O

roteador A, ainda acredita que pode acessar esta rede através do roteador B (sua tabela de roteamento continua a marcar uma distancia de 2 saltos até ela).

Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	Down
10.2.0.0	S0	1
10.1.0.0	S0	2

Quando o roteador B envia a copia periódica de sua tabela de roteamento para o roteador C, este acredita que agora ele consegue novamente alcançar a rede 10.4.0.0, porém, agora, a partir do roteador B. O roteador C atualiza sua tabela de roteamento com a rota de destino a rede 10.4.0.0 via roteador B com número de saltos igual a 2.

Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	2
10.2.0.0	S0	1
10.1.0.0	S0	2

Agora, o roteador B recebe a atualização vinda do roteador C. Como o roteador B já possui em sua tabela uma entrada para a rede 10.4.0.0 aprendida a partir da sua interface serial 1, ao receber esta atualização (também vinda via serial 1), ela irá atualizar a distância para esta entrada. Logo, o roteador B irá atualizar sua tabela com o novo custo, agora de 3, para alcançar esta rede. O mesmo irá ocorrer com o roteador A, ao receber a tabela do roteador B. O roteador A também detecta uma alteração na distância da rede 10.4.0.0 e atualiza sua tabela, colocando como 4 a distância até esta rede.

Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	4

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	3
10.1.0.0	S0	1

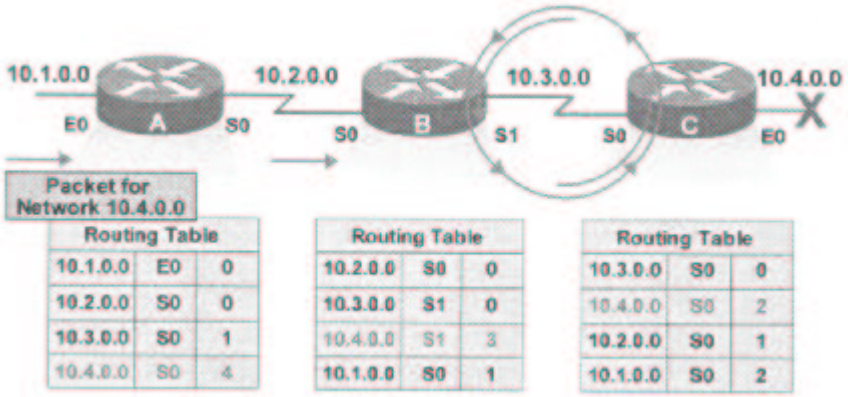
Routing Table		
10.3.0.0	S0	0
10.4.0.0	S0	2
10.2.0.0	S0	1
10.1.0.0	S0	2

Neste momento, temos todas as 3 tabelas de roteamento incorretas. Todas prometem alcançar a rede 10.4.0.0 por caminhos inexistentes. Estas atualizações erradas vão se repetir e a contagem de saltos vai crescer cada vez mais. Este problema é conhecido como **contagem para o infinito** (*count to infinity*). Pacotes destinados a rede 10.4.0.0 nunca alcançaram o destino mas vão ficar trafegando continuamente na rede (*loop* de roteamento) desperdiçando banda.
A seguir serão apresentadas algumas soluções para minimizar os problemas apresentados pelo algoritmo de vetor distância.

Este problema apresentado como contagem para o infinito acontece, como vimos, sempre que as tabelas de roteamento continuam a aumentar a métrica para um destino que não pode ser alcançado, ao invés de marcar este destino como inalcançável. Para que isto não ocorra, o protocolo define um **número máximo de saltos**, este número máximo, no caso do RIP, é 16. Agora, o protocolo de roteamento irá permitir que, no caso de ocorrência de *loop* de atualização, este irá ocorrer até a métrica alcançar este valor máximo permitido. Quando a métrica exceder o valor máximo permitido a rede é considerada inalcançável, parando a proliferação de atualizações de roteamento que aumentem esta métrica. Isso de um lado limita o tamanho da rede, mas evita que um pacote permaneça na rede infinitamente.

Temos ainda soluções para eliminar estes *loops* de roteamento. *Loops* de roteamento ocorrem quando dois ou mais roteadores tem informações erradas de roteamento indicando um caminho válido para uma rede inalcançável passando pelo outro.

Exemplo:



Neste exemplo, um pacote destinado a rede 10.4.0.0 chega ao roteador A. Este olha na sua tabela de roteamento e manda o pacote pela sua interface serial 0. Ao chegar no roteador B, este manda o pacote pela sua interface serial 1, como indicado na sua tabela de roteamento. O roteador C recebe o pacote e checa sua tabela de roteamento, a qual especifica que o pacote deve ser enviado pela interface serial 0. O pacote então, acaba voltando ao roteador B que novamente o envia para o roteador C. O pacote ficará então trafegando de B para C.

Existem algumas técnicas disponíveis para eliminar *loop* de roteamento como: estreitamento de horizontes (*split horizon*), envenenamento de rotas (*route poisoning*), envenenamento reverso (*poison reverse*), tempo de espera (*holddown timers*) e atualizações imediatas (*triggered updates*). A seguir tem-se uma explicação de cada uma destas técnicas.

Estreitamento de horizontes (Split Horizon)

Uma maneira de se eliminar os *loops* de roteamento a aumentar a velocidade de convergência é utilizando a técnica de estreitamento de horizontes. Esta técnica diz que não é útil mandar informações sobre uma rota de volta na mesma direção por onde a informação original chegou. Ou seja, evita que um roteador RIP propague rotas para a mesma interface que ele aprendeu, evitando *loop* entre estes nós.

Envenenamento de rotas (Route Poisoning)

Esta técnica é uma ligeira modificação daquela utilizada no estreitamento de horizontes. Seu objetivo também é a prevenção de *loops* de roteamento causados por atualizações inconsistentes. Com essa técnica, o roteador seta a entrada da tabela que mantém o estado da rede consistente, enquanto os demais roteadores gradativamente convergem

corretamente após a ocorrência de uma mudança na topologia. Utilizado juntamente com o tempo de espera, uma outra técnica que será mostrada mais a frente, o envenenamento de rotas é uma solução para *loops* longos. Ou seja, no caso estudado, quando o enlace 10.4.0.0 fica indisponível, o roteador C (diretamente conectado a ele) envenena este enlace. Em sua tabela, ele coloca esta rede como inalcançável ou de métrica infinita (número de saltos igual a 16). Tendo envenenado a rota para este enlace, o roteador C não fica sujeito a atualizações incorretas a respeito deste enlace, vindas de roteadores vizinhos que acreditam ter rotas alternativas para ele.

Envenenamento Reverso (Poison Reverse)

Estreitamento de horizontes com envenenamento reverso faz com que a rede consiga convergir em menos tempo. Quando o roteador B recebe uma atualização mostrando que a métrica para se atingir a rede 10.4.0.0 foi alterada para infinito, ele manda uma atualização, chamada de envenenamento reverso, de volta para o roteador C avisando que a rede está inalcançável. E ainda coloca este enlace como possivelmente inalcançável em sua tabela de roteamento. Essa é uma situação específica que se sobrepõe ao estreitamento de horizontes. Isso ocorre para ter certeza que o roteador C não ficará sujeito a atualizações erradas a respeito desta rede.

Tempo de Espera (Holddown Timers)

O tempo de espera é utilizado para evitar que atualizações inapropriadas ensinem caminhos inexistentes para enlaces que não estão disponíveis. Com esta técnica, os roteadores esperam por mudanças que devem afetar rotas, por algum período de tempo. Esse período, por padrão do RIP, é de 3 vezes o tempo da atualização periódica (por padrão, o RIP manda atualizações temporárias a cada 30s).
Situações onde este tempo é utilizado:

- Quando um roteador recebe uma atualização de um vizinho indicando que uma rede que era acessível agora não está mais. O roteador então, marca a rota como possivelmente inalcançável (*possible down*) e começa a marcar seu tempo de espera.

- Se a atualização de algum vizinho chegar com métrica melhor do que aquela que está na tabela de roteamento do enlace possivelmente inalcançável, o roteador marca o enlace como alcançável e retira o tempo de espera.

- Se em qualquer momento, antes do tempo de espera estourar, o roteador receber uma atualização de um vizinho diferente, com uma métrica mais fraca ou igual aquela da rede possivelmente inalcançável, esta será descartada. Ignorando estas atualizações de métricas piores enquanto estiver em tempo de espera, o roteador que percebeu a mudança

dá mais tempo aos demais roteadores para que estes sejam avisados de uma mudança na rede.

- Durante este tempo de espera, as rotas aparecem como possivelmente inalcançáveis nas tabelas de roteamento. Mesmo com a rota estando no estado de possivelmente inalcançáveis, os roteadores continuam tentando encaminhar os pacotes para essa rede (talvez esta rede só esteja tendo um problema de conexão intermediária, oscilação...)

Atualizações Imediatas (Triggered Updates)

Nos exemplos anteriores, os *loops* de roteamento foram causados graças as informações erradas obtidas como resultado de atualizações inconsistentes, convergência lenta e temporização. O fato dos roteadores esperarem por suas atualizações periódicas para notificar aos demais uma alteração na rede, faz com que a rede tenha um tempo de convergência mais lento.
Normalmente, as atualizações nas tabelas de roteamento são passadas aos demais em um intervalo de tempo constante. Essa ferramenta propõe que sejam mandadas atualizações imediatas assim que um roteador perceber uma alteração na rede. O roteador que percebe a mudança passa então imediatamente aos seus vizinhos esta atualização, estes ao receberem a atualização, também a passarão imediatamente para seus demais vizinhos e assim a atualização chega mais rapidamente aos roteadores envolvidos.
Essa idéia de atualização imediata seria suficiente se pudesse garantir que cada uma destas atualizações chegasse imediatamente aos roteadores apropriados. Porém, podem ocorrer dois problemas:

- Os pacotes de atualização podem ser descartados ou corrompidos ao longo de sua trajetória.

- As atualizações imediatas não ocorrem instantaneamente. É possível que um roteador que ainda não recebeu esta atualização imediata envie sua atualização periódica, fazendo com que seu vizinho que acabara de atualizar sua tabela devido a atualização imediata que ele recebeu, coloque a rota novamente em sua tabela.

Agora, juntando as atualizações imediatas com o tempo de espera o problema é solucionado. Por que com o tempo de espera, mesmo que o alguém envie uma atualização temporária antes de receber a atualização imediata, os demais roteadores que já haviam recebido as atualizações imediatas e haviam posto tal rota como possivelmente inalcançável, ao receberem um caminho alternativo com métrica pior ou igual a que eles conheciam, não atualizem suas tabelas enquanto o tempo não houver estourado. Isso faz com que a atualização imediata tenha mais tempo para percorrer todos os roteadores envolvidos antes destes tentarem divulgar um novo caminho até a rede que foi modificada.

Características

A seguir temos algumas das principais características do RIP:

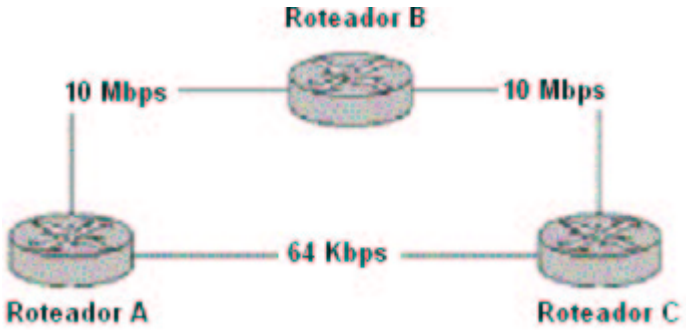
- É um protocolo relativamente antigo mais ainda é bastante utilizado em redes pequenas.

- Por se tratar de um protocolo antigo e simples, quase todos os roteadores podem utilizar o RIP.

- É de fácil configuração (pouca complexidade).

- É um protocolo baseado no algoritmo de vetor distancia.

- Contagem de saltos é utilizada como a única métrica para a seleção de caminhos. Isso faz com que nem sempre o melhor caminho seja armazenado na tabela de roteamento. Um exemplo dessa situação é mostrado abaixo, onde de A para C existem dois caminhos. Um deles é pelo roteador B, tendo custo em 2 saltos e o outro seria diretamente com custo 1. Mesmo que os links pelo roteador B sejam muito superiores em capacidade, ou ainda, mesmo que o link de 64 Kbps esteja totalmente utilizado, o melhor caminho escolhido pelo RIP sempre será pelo link de 64 Kbps já que a única métrica é o número de saltos.



Decisão do melhor caminho segundo o RIP

- O número máximo de saltos permitidos é 15. Isso limita o uso deste protocolo a redes não muito grandes, mas como ele é um IGP, este número parece razoável. O RIP é projetado para intercambiar informações de roteamento em uma rede de tamanho pequeno para médio.

- Atualizações periódicas de roteamento a cada 30 segundos por padrão. Mesmo que não exista nenhuma alteração nas rotas da rede, os roteadores baseados em RIP, continuarão a trocar mensagens de atualização nestes intervalos regulares. Dentre outros, este é mais um dos motivos pelos quais o RIP não é indicado para redes maiores, pois nestas situações o volume de tráfego gerado pelo RIP, poderia consumir boa parte da banda

disponível. Além disso, cada mensagem do protocolo RIP comporta, no máximo, informações sobre 25 rotas diferentes, o que para grandes redes, faria com que fosse necessária a troca de várias mensagens, entre dois roteadores, para atualizar suas respectivas tabelas, com um grande número de rotas.

- RIP é capaz de fazer balanceamento de carga em até 6 caminhos porém estes devem ser de custo iguais. Basta definir o número máximo de caminhos paralelos permitidos na tabela de roteamento. Com o RIP, estes caminhos devem ser de custo iguais. Caso não seja do interesse trabalhar com balanceamento de cargas, basta escolher esse número máximo de caminhos paralelos como 1.

- A primeira versão do RIP, o RIPv1 criada em 1988, que ainda é utilizada atualmente, é implementada como sendo um protocolo de roteamento *classful,* isso significa que ele não manda a máscara de rede das rotas que ele divulga em suas atualizações. Devido a essa característica, não podemos trabalhar com redes de tamanho de mascara variado. (Variable Lenght Subnet Mask- VLSM). O RIPv1 foi desenvolvido para trabalhar com redes baseadas nas classes padrão A, B e C, ou seja, pelo número IP da rota, deduzia-as a respectiva classe. Com o uso da *Internet* e o uso de um número variável de bits para a máscara de sub-rede (número diferente do número de bits padrão para cada classe), esta fato tornou-se um problema sério do protocolo RIP v1. O protocolo RIP v1, utiliza a seguinte lógica, para "descobrir" qual a máscara de sub-rede associada com determinada rota:

1. Se a identificação de rede coincide com uma das classes padrão A, B ou C, é assumida a máscara de sub-rede padrão da respectiva classe.

2. Se a identificação de rede não coincide com uma das classes padrão, duas situações podem acontecer.

2.1 Se a identificação de rede coincide com a identificação de rede da interface na qual o anúncio foi recebido, a máscara de sub-rede da interface na qual o anúncio foi recebido, será assumida.

2.2 Se a identificação de rede não coincide com a identificação de rede da interface na qual o anúncio foi recebido, o destino será considerado um host (e não uma rede) e a máscara de sub-rede 255.255.255.255, será assumida.

- As atualizações periódicas do RIPv1 utilizam o endereço de *broadcast.* Com isto, todos os hosts da rede receberão os pacotes RIP e não somente os hosts habilitados ao RIP.

- O RIPv2, a versão 2 do RIP que surgiu em 1993, já é um protocolo de roteamento *classless* , ou seja, envia a mascara das redes divulgadas em suas atualizações. Já permitindo trabalhar com redes de tamanho de máscara variado.

- Outra melhora do RIPv2, é que este é mais seguro pois utiliza autenticação, o que visa proteger a rede contra utilização de roteadores não autorizados. Com o RIPv2 é possível implementar um mecanismo de autenticação, de tal maneira que os roteadores somente aceitem os anúncios de roteadores autenticados, isto é, identificados na rede. A autenticação pode ser configurada através da definição de uma senha ou de mecanismos mais sofisticados como o MD5 (*Message Digest* 5). Por exemplo, com a autenticação por senha, quando um roteador envia um anúncio, ele envia juntamente a senha de autenticação. Outros roteadores da rede, que recebem o anúncio, verificam se a senha está correta e somente depois da verificação, alimentam suas tabelas de roteamento com as informações recebidas.

- Os anúncios de atualização do protocolo RIPv2 são baseados em tráfego multicast e não mais broadcast como no caso do protocolo RIPv1. O protocolo RIPv2 utiliza o endereço de multicast 224.0.0.9. Com isso os roteadores habilitados ao RIPv2 atuam como um grupo multicast, registrado para "escutar" os anúncios do protocolo. Outros hosts da rede, não habilitados ao RIPv2, não serão "importunados" pelos pacotes deste protocolo. Por questões de compatibilidade (em casos onde parte da rede ainda usa o RIP v1), é possível utilizar broadcast com roteadores baseados em RIP v2. Mas esta solução somente deve ser adotada durante um período de migração, assim que possível, todos os roteadores devem ser migrados para o RIPv2 e o anúncio via broadcast deve ser desabilitado.

- É importante mencionar que tanto redes baseadas no RIPv1 quanto no RIPv2 são redes chamadas planas (*flat*). Ou seja, não é possível formar uma hierarquia de roteamento, baseada no protocolo RIP. Mais um motivo para o RIP não ser utilizado em grandes redes. A tendência natural do RIP, é que todos os roteadores sejam alimentados com todas as rotas possíveis (isto é um espaço plano, sem hierarquia de roteadores). Imagine como seria utilizar o RIP em uma rede como a Internet, com milhões e milhões de rotas possíveis, com *links* caindo e voltando frequentemente? Impossível. Por isso que o uso do RIP (v1 ou v2) somente é indicado para pequenas redes.

- O RIPv1 é descrito na RFC 1058 e a versão 2 (RIPv2) nas RFCs 1721 e 1722.

Bibliografia:

Interligação em rede com TCP / IP - Princípios, protocolos e arquitetura
Volume I
Douglas E Comer
Editora Campus

Designing for Cisco Internetwork Solutions
Volume II (v1.0)
Capitulo 6 – " *Selecting Routing Protocols for a Network*"

Interconnecting Cisco Network Devices
Volume II (v2.0)
Capitulo 5 – " *Determining IP routes*"

Páginas na *internet* :

http://mesonpi.cat.cbpf.br/naj/ripospf.pdf

http://www.juliobattisti.com.br/artigos/windows/tcpip_p14.asp

http://www.gtrh.tche.br/ovni/roteamento3/conteudo.htm