Introdução ao IGRP

Índice

Introdução

Este documento introduz o Interior Gateway Routing Protocol (IGRP). Ele tem dois propósitos. Um é para formar uma introdução para a tecnologia IGRP, para aquelas que estão interessados em usar, avaliar e, possivelmente, implementá-lo. A outro é para dar uma exposição mais ampla a algumas ideias e conceitos interessantes que são personificados no IGRP. Consulte Configuração do IGRP, A Implementação do Cisco IGRP e Comandos do IGRP para obter informações sobre como configurar o IGRP.

Objetivos para IGRP

O protocolo de IGRP permite que um número de gateways coordenem seu roteamento. Seus objetivos são os seguintes:

- Roteamento estável até mesmo em redes muito grandes ou complexas. Nenhum loop de roteamento deve ocorrer, mesmo como transeuntes.
- Resposta rápida às alterações na topologia da rede.

- Overhead baixo. Ou seja, o próprio IGRP não deve usar mais largura de banda que o limite realmente necessário para sua tarefa.
- Divisão de tráfego entre várias rotas paralelas quando elas são, em termos gerais, equivalentes ao desejado.
- Considerar as taxas de erros e o nível de tráfego em caminhos diferentes.

A implementação atual do IGRP processa o roteamento para TCP/IP. Contudo, o design básico é pretendido poder segurar uma variedade de protocolos.

Ninguém ferramenta está indo resolver todos os problemas de roteamento. Convencionalmente, o problema de roteamento está dividido em várias partes. Os protocolos tais como o IGRP são chamados “protocolos internal gateway” (IGP). Eles foram planejados para uso em um único conjunto de redes, seja em um único gerenciamento ou em gerenciamentos coordenados. Esses conjuntos de redes estão conectados por "Protocolos de gateways externos" (EGPs). Um IGP foi projetado para supervisionar a riqueza de detalhes da topologia de rede. A prioridade em projetar um IGP é colocada em produzir rotas ótima e na responder rapidamente às mudanças. Um EGP tem a intenção de proteger um sistema de redes contra erros ou interpretação incorreta intencional por outros sistemas; o BGP é um protocolo de gateway externo desse tipo. A prioridade em projetar um EGP está na estabilidade e nos controles administrativos. Freqüentemente, é suficiente que um EGP produza uma rota razoável, em vez da rota ideal.

O IGRP possui algumas similaridades com protocolos mais antigos, como o Routing Information Protocol da Xerox, RIP da Berkeley e o Hello de Dave Mills. Ele se distingue desses protocolos principalmente por ser projetado para redes maiores e mais complexas. Consulte a seção Comparação com RIP para obter uma comparação mais detalhada com RIP, que é o mais amplamente utilizado dos protocolos da geração mais antiga.

Como esses protocolos mais antigos, o IGRP é um protocolo de vetor de distância. Em tal protocolo, os gateways trocam a informação de roteamento somente com os gateways contiguos. Esta informação de roteamento contém um sumário de informações sobre o resto da rede. Pode-se mostrar matematicamente que todos os gateways tomados junto estão resolvendo um problema de otimização por que quantidades a um algoritmo distribuído. Cada gateway precisa apenas resolver parte do problema e apenas receber uma parte do total de dados.

A principal alternativa ao IGRP é o EIGRP (IGRP Avançado) e uma classe de algoritmos chamada SPF (caminho mais curto primeiro). O OSPF usa este conceito. Para aprender mais sobre o OSPF referem o guia de design de OSPF. O OSPF que estes são é baseado em uma técnica da inundação, onde cada gateway seja mantido atualizado sobre o estado de cada relação em cada outro gateway. Cada gateway soluciona de forma independente o problema de otimização do seu ponto de vista, usando dados de toda a rede. Existem vantagens em cada abordagem. Em algumas circunstâncias, o SPF pode conseguir responder às alterações mais rapidamente. Para evitar circuitos de roteamento, o IGRP precisa ignorar novos dados por alguns minutos após certos tipos de mudança. Como o SPF recebe informações diretamente de cada gateway, ele consegue evitar esses Routing Loops. Dessa forma, pode atuar imediatamente sobre as novas informações. Entretanto, o SPF precisa lidar substancialmente com mais dados que o IGRP, tanto em estruturas de dados internos quanto em mensagens entre gateways.

O Problema de Roteamento

O IGRP tem como objetivo ser usado em gateways conectando várias redes. Nós supomos que as redes usam a tecnologia com base em pacotes. De fato os gateways atuam como switch de pacotes. Quando um sistema conectado a uma rede precisar enviar um pacote para um sistema

em uma rede diferente, ele endereçará o pacote para o gateway. Se o destino estiver em uma das redes conectadas ao gateway, este encaminhará o pacote ao destino. Se o destino é mais distante, o gateway enviará o pacote a um outro gateway que seja mais perto do destino. Tabelas de roteamento do uso dos gateways para ajudá-los a decidir que fazer com pacotes. Está aqui uma tabela de roteamento do exemplo simples. (Os endereços usados nos exemplos são endereços IP de Um ou Mais Servidores Cisco ICM NT tomados da Universidade Rutgers. Observe que o problema básico de roteamento é semelhante em outros produtos também, mas essa descrição pressupõe que o IGRP esteja sendo utilizado para IP Routing.)

Figura 1

```
network      gateway     interface
  -------      -------     ---------
  128.6.4      none        ethernet 0
  128.6.5      none        ethernet 1
  128.6.21     128.6.4.1   ethernet 0
  128.121      128.6.5.4   ethernet 1
  10           128.6.5.4   ethernet 1
```

(As tabelas de roteamento IGRP reais têm a informação adicional para cada gateway, porque nós veremos.) Este gateway é conectado a dois Ethernets, chamados 0 e 1. Foram números de rede IP dados (realmente números da sub-rede) 128.6.4 e 128.6.5. Assim os pacotes endereçados para estas redes específicas podem ser enviados diretamente ao destino, simplesmente usando a interface Ethernet apropriada. Há dois gateways próximos, o 128.6.4.1 e o 128.6.5.4. Os pacotes de redes diferentes de 128.6.4 e de 128.6.5 serão enviados a um ou ao outro daqueles gateways. A tabela de roteamento indica que gateway deve ser usado para que rede. Por exemplo, pacotes endereçados a um host na rede 10 devem ser encaminhados para o gateway 128.6.5.4. Se espera que este gateway é mais perto da rede 10, isto é que o melhor caminho à rede 10 atravessa este gateway. O principal objetivo do IGRP é permitir que os gateways criem e mantenham tabelas de roteamento como essa.

Resumo de IGRP

Como mencionado acima, o IGRP é um protocolo que permita que os gateways acumulem sua tabela de roteamento trocando a informação com outros gateways. Um gateway é iniciado com entradas para todas as redes conectadas diretamente a ele. Ele obtém informações sobre outras redes trocando atualizações de roteamento com gateways adjacentes. No caso o mais simples, o gateway encontrará um trajeto que representa a melhor maneira de obter a cada rede. Um caminho é caracterizado pelo próximo gateway ao qual os pacotes devem ser enviados, a interface de rede que deve ser utilizada e informações de métricas. A informação métrica é um conjunto de número que caracteriza como bom o trajeto é. Isso permite que o gateway compare os caminhos obtidos de vários gateways e decida o caminho a ser utilizado. Há frequentemente os casos onde faz o sentido rachar um tráfego entre dois ou mais trajetos. IGRP fará isso sempre que dois ou mais caminhos forem igualmente bons. O usuário pode igualmente configurar-lo para rachar o tráfego quando os trajetos são quase ingualmente bons. Nesse caso, mais tráfego será enviado junto com o caminho com a melhor métrica. A intenção é que o tráfego possa ser dividido entre uma linha de 9600 bps e outra de 19200 bps e a linha 19200 obterá aproximadamente duas vezes mais tráfego que a linha de 9600 bps.

O medidor usado pelo IGRP inclui o seguinte:

- Atraso relativo à topologia
- A largura de banda do segmento com a menor largura de banda do caminho
- Ocupação de canal do trajeto

- Confiabilidade do caminho

O tempo de retardo topológico é a quantidade de tempo que tomaria para obter ao destino ao longo desse trajeto, supondo uma rede descarregada. Há, obviamente, retardo adicional quando a rede é carregada. Contudo, a carga é esclarecida usando a figura da ocupação de canal, não tentando medir atrasos reais. A largura de banda do caminho é simplesmente a largura de banda por segundo do link mais lento do caminho. A ocupação de canal indica quanto dessa largura de banda é atualmente em uso. É medida, e mudará com carga. A confiabilidade indica a taxa de erros atual. É a fração dos pacotes que chegam no destino não danificado. É medido.

Embora não sejam usados como parte da métrica, duas partes de informação da adição são passadas com ela: contagem e MTU de salto. A contagem de salto é apenas o número de gateways pelo qual um pacote terá que passar para chegar ao destino. O MTU é o tamanho de pacote máximo que pode ser enviado ao longo de todo o caminho, sem fragmentação. (Ou seja, é o mínimo de MTUs de todas as redes envolvidas no caminho.)

Com base nas informações métricas, uma única "métrica composta" é calculada para o caminho. O métrica composta combina o efeito dos vários componentes métricos em um único número que representa os “bens” desse trajeto. É o métrica composta que está usado realmente para decidir no melhor caminho.

Periodicamente, cada gateway transmite sua tabela de roteamento inteira (com uma certa censura devido à regra de horizonte de divisão) a todos os gateways adjacentes. Quando um gateway obtém esta transmissão de um outro gateway, compara a tabela com sua tabela existente. Todos os destinos e trajetos novos são adicionados à tabela de roteamento do gateway. Os trajetos na transmissão são comparados com os trajetos existentes. Se um trajeto novo é melhor, pode substituir existente. As informações na difusão também são utilizadas para atualizar a ocupação do canal e outras informações sobre caminhos existentes. Esse procedimento geral é semelhante ao utilizado por todos os protocolos de vetor de distância. É referido na literatura matemática como o algoritmo Bellman-Ford. Refira o RFC 1058 para um desenvolvimento detalhado do procedimento básico, que descreve o RASGO, um protocolo de vetor de distância mais velho.

No IGRP, o algoritmo geral de Bellman-Ford é modificado em três aspectos críticos. Primeiramente, em vez de uma métrica simples, um vetor do medidor é usado para caracterizar trajetos. Segundo, em lugar de escolher um único caminho com a menor métrica, o tráfego é dividido entre vários caminhos, cujas métricas caem em uma faixa especificada. Em terceiro lugar, diversas características são introduzidas para fornecer a estabilidade nas situações onde a topologia está mudando.

O melhor caminho é selecionado com base em uma métrica composta:

```
[(K1 / Be) + (K2 * Dc)] r
```

Em que K1, K2 = constantes, Be = largura de banda do pacote descarregado x (1 ocupação do canal), Dc = retardo topológico e r = confiabilidade.

O caminho que tiver a métrica composta menor será o melhor caminho. Onde há caminhos múltiplos ao mesmo destino, o gateway pode distribuir os pacotes sobre mais de um trajeto. Isso é feito de acordo com a métrica composta para cada caminho de dados. Por exemplo, se um caminho tiver uma métrica composta de 1 e outro caminho tiver uma métrica composta de 3, três vezes mais pacotes serão enviados pelo caminho de dados que tenha a métrica composta de 1.

Há duas vantagens a usar um vetor de informação métrica. A primeira é que ele dá a capacidade de suportar vários tipos de serviço do mesmo conjunto de dados. A segunda vantagem é a

precisão aprimorada. Quando uma métrica única é usada, ela normalmente é tratada como se houvesse um atraso. Cada link no trajeto é adicionado à métrica total. Se há um link com uma largura de banda baixa, está representada normalmente por um grande atraso. Contudo, as limitações de largura de banda não acumulam realmente a maneira que os atrasos fazem. Tratando a largura de banda como um componente separado, pode ser segurada corretamente. De maneira semelhante, a carga pode ser controlada por um número de ocupância de canal separado.

O IGRP fornece um sistema interconectando as redes de computador que podem estavelmente segurar uma topologia de gráfico geral que inclui laços. O sistema mantém a informação métrica do caminho cheio, isto é, conhece os parâmetros de caminho a todas redes restantes a que todo o gateway é conectado. O tráfego pode ser distribuído ao longo de caminhos paralelos, e parâmetros de caminho múltiplo podem ser computados simultaneamente em toda a rede.

Comparação com RIP

Esta seção compara o IGRP com o RASGO. Essa comparação é útil porque o RIP é amplamente utilizado para finalidades similares ao IGRP. Entretanto, fazer isso não é totalmente justo. O RASGO não foi pretendido encontrar todos os mesmos objetivos que o IGRP. O RASGO foi pretendido para o uso em redes pequenas com razoavelmente tecnologia uniforme. Nesses aplicativos, geralmente é adequado.

A maioria de diferença básica entre o IGRP e o RASGO é a estrutura de seu medidor. Infelizmente, esta não é uma mudança que possa ser simplesmente encaixada retroativamente no RIP. Exige os algoritmos e as estruturas de dados novos atuais no IGRP.

O RIP utiliza uma métrica simples de "contagem de nós" para descrever a rede. Ao contrário do IGRP, onde cada trajeto é descrito por um atraso, por uma largura de banda, etc., no RASGO é descrito por um número de 1 a 15. Este número é usado normalmente para representar quantos gateways o trajeto vai completamente antes de obter ao destino. Isso significa que não há nenhuma distinção entre uma linha serial lenta e uma Ethernet. Em algumas aplicações do RASGO, é possível para o administrador de sistema especificar que um salto dado deve ser contado mais de uma vez. As redes lentas podem ser representadas por uma grande contagem de salto. Mas desde que o máximo é 15, isto não pode ser feito muito. Por exemplo se um Ethernet é representado por 1 e por uma linha 56Kb por 3, pode haver no máximo umas linhas 5 56Kb em um trajeto, ou o máximo de 15 é excedido. A fim representar a gama completa de velocidades de rede disponíveis, e permiti-la uma rede grande, os estudos feitos por Cisco sugerem que uma métrica 24-bit esteja precisada. Se a métrica máxima for pequena demais, o administrador do sistema terá duas opções desagradáveis: ou ele não pode distinguir entre rotas rápidas e lentas, ou ele não consegue encaixar sua rede completa no limite. De fato um número de redes nacional são agora grandes bastante que o RASGO não pode as segurar mesmo se cada salto é contado somente uma vez. O RIP simplesmente não pode ser utilizado para estas redes.

A resposta óbvia seria modificar o RIP para permitir uma métrica maior. Infelizmente, isso não vai funcionar. Como todos os protocolos de vetor de distância, o RASGO tem o problema da “contagem à infinidade”. Isto é descrito com maiores detalhes no RFC 1058 . Quando as alterações de topologia, rotas artificiais serão introduzidas. O medidor associou com estas rotas artificiais aumenta lentamente até que alcancem 15, que no ponto as rotas estão removidas. 15 são uns máximos pequeno bastante que este processo convirja razoavelmente rapidamente, supondo que as atualizações disparada estão usadas. Se o RASGO foi alterado para permitir uma métrica 24-bit, os laços persistiriam o suficiente para que a métrica seja contada até 2**24.

Isto não é tolerável. O IGRP tem recursos projetados para impedir que rotas artificiais sejam introduzidas. Estes são discutidos abaixo na seção 5.2. Não é prática segurar redes complexo sem introduzir tais características ou mudá-las a um protocolo tal como o SPF.

O IGRP faz bem mais do que simplesmente aumentar o intervalo de métricas permitidas. Reestrutura a métrica para descrever o retardo, a largura de banda, a confiabilidade e a carga. É possível representar essas considerações em uma única métrica, por exemplo, RIPs. No entanto, a abordagem aplicada pelo IGRP é potencialmente mais precisa. Por exemplo, com uma única métrica, diversos links rápidos sucessivos parecerão ser equivalentes a um único retardam um. Esta pode ser a caixa para o tráfego interativo, onde o atraso é o interesse principal. No entanto, para transferências de dados em grande escala, a preocupação principal é a largura de banda e a adição de métricas em conjunto não é o método certo aqui. O IGRP processa o atraso e a largura de banda separadamente, acumulando atrasos, mas utilizando o mínimo das larguras de banda. Não é fácil saber como incorporar os efeitos de confiabilidade e carga em uma métrica de componente único.

Na minha opinião, uma das vantagens grandes do IGRP é facilidade da configuração. Pode diretamente representar as quantidades que têm o significado físico. Isto significa que pode se estabelecer automaticamente, com base no tipo de interface, velocidade de linha, etc. Com uma métrica do componente único, a métrica é mais provável ter que “ser cozinhado” para incorporar efeitos de diversas coisas diferentes.

Outras inovações se referem mais a algoritmos e estruturas de dados do que ao Routing Protocol. Por exemplo, o IGRP especifica algoritmos e estruturas de dados que suportam divisão de tráfego entre várias rotas. É certamente possível projetar uma aplicação do RASGO que faz este. Entretanto, uma vez o roteamento tendo sido reimplementado, não há motivo para manter o RIP.

Eu tenho descrito até agora “o IGRP genérico”, uma tecnologia que poderia apoiar o roteamento para todo o protocolo de rede. Entretanto, nesta seção é válido falar um pouco mais sobre a implementação específica de TCP/IP. Essa é a implementação que será comparada ao RIP.

As mensagens de atualização de RIP contêm apenas instantâneos da tabela de roteamento. Ou seja, elas têm vários destinos e valores métricos. A implementação IP do IGRP tem a estrutura adicional. Primeiramente, o mensagem de atualização é identificado por um “número de sistema autônomo.” Essa terminologia provém da tradição Arpanet e tem aqui um significado específico. Entretanto, em muitas redes isto significa que é possível executar vários sistemas de roteamento diferentes na mesma rede. Isto é útil para os lugares onde as redes de diversas organizações convirgem. Cada organização pode manter seu próprio roteamento. Como cada atualização é rotulada, os gateways podem ser configurados para observar apenas a correta. Certos gateways são configurados para receber atualizações de diversos sistemas autônomos. Eles passam informações entre os sistemas de maneira controlada. Observe que esta não é uma solução completa para os problemas de segurança do roteamento. Todo o gateway pode ser configurado para escutar atualizações de qualquer sistema autônomo. No entanto, essa continua sendo uma ferramenta muito útil na implementação de políticas de roteamento nas quais há um grau razoável de confiança entre os administradores de rede.

O segundo recurso estrutural sobre mensagens de atualização de IGRP afeta a maneira como as rotas padrão são tratadas pelo IGRP. A maioria dos protocolos de roteamento possui um conceito de rota padrão. Não é frequentemente prática para que as atualizações de roteamento alistem cada rede no mundo. Geralmente, um conjunto de gateways precisa de informações detalhadas de roteamento para as redes da organização. Todo o tráfego para destinos fora de sua organização pode ser enviado a um de alguns gateways limite. É possível que esses gateways limite tenham informações mais completas. A rota ao melhor gateway limite é uma “rota padrão”.

É um padrão no sentido que é usado para obter a todo o destino que não for alistado especificamente nas atualizações de roteamento internas. O RASGO, e alguns outros protocolos de roteamento, circulam a informação sobre a rota padrão como se era uma rede real. O IGRP usa um método diferente. Em vez de uma única entrada falsa para a rota padrão, o IGRP permite que redes reais sejam marcadas como candidatas para ser um padrão. Isto é implementado pelo posicionamento de informações sobre essas redes em uma seção externa especial da mensagem de atualização. Contudo, pôde-se também pensar como de girar sobre um bit associado com aquelas redes. Periodicamente, o IGRP faz a varredura de todas as rotas padrão candidatas e escolhe aquela com a menor métrica para ser a rota padrão atual.

Potencialmente, essa aproximação dos padrões é um tanto mais flexível que a aproximação usada pela maioria das implementações de RIP. A maioria dos gateways tipicamente RIP pode ser definida para gerar uma rota padrão com uma certa métrica especificada. A intenção é fazer isso nos gateways de limite.

Descrição detalhada

Esta seção fornece uma descrição detalhada do IGRP.

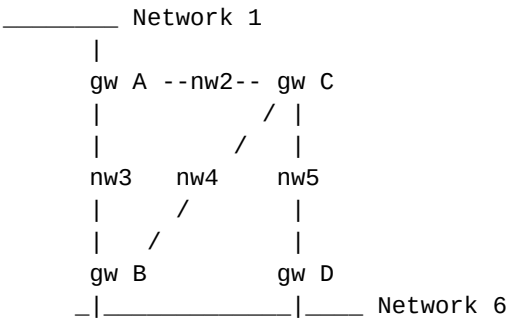
Descrição geral

Quando um gateway é ligado pela primeira vez, a tabela de roteamento respectiva é inicializada. Isso pode ser feito por um operador a partir do terminal do console ou lendo as informações nos arquivos de configuração. Uma descrição de cada rede conectada ao gateway é fornecida, incluindo o atraso topológico junto ao link (por exemplo, quanto tempo demora para um único bit atravessar o link) e a largura de banda do link.

Figura 2

Por exemplo, no diagrama acima, o gateway S seria informado de que está conectado às redes 2 e 3 por meio das interfaces correspondentes. Assim, inicialmente, o gateway 2 sabe somente que pode alcançar todo o computador de destino nas redes 2 e 3. Todos os gateways são programados para transmitir periodicamente a seus gateways vizinhos a informação que estiveram inicializados com, assim como a informação recolhida de outros gateways. Assim, o gateway S receberia atualizações dos gateways R e T e aprenderia que pode alcançar computadores no gateway direto R da rede 1 e computadores na rede 4 através do gateway T. Desde que o gateway S envia sua tabela de roteamento inteira, no gateway seguinte do ciclo T aprenderá que pode obter à rede 1 através do gateway S. É fácil perceber que as informações sobre todas as redes no sistema acabarão alcançando todos os gateways no sistema, desde que a rede esteja completamente conectada.

Figura 3



Cada gateway calcula uma métrica composta para determinar a conveniência dos caminhos de dados para computadores de destino. Por exemplo, no diagrama acima de, para um destino na rede 6, gateway A (o gw A) computaria funções métricas para dois trajetos, através dos gateways B e do C. Note que os trajetos estão definidos simplesmente pelo salto seguinte. Há realmente três rotas possíveis de A à rede 6:

- Dirija a B
- Ao C e então a B
- Para C e, em seguida, para D

Contudo, o gateway A não precisa de escolher entre as duas rotas que envolvem o C. A tabela de roteamento em A tem uma única entrada que representa o trajeto ao C. Sua métrica representa a melhor maneira de obtenção do C ao destino final. Se A envia um pacote para C, fica a critério de C decidir utilizar B ou D.

Equação 1

A função métrica composta calculada para cada caminho de dados é mostrada abaixo:

```
[(K1 / Be) + (K2 * Dc)] r
```

Onde r = a confiabilidade fracional (% das transmissões que são recebidas com sucesso no salto seguinte), C.C. = retardo composto, sejam = largura de banda efetiva: largura de banda descarregada x (1 - ocupação de canal), e K1 e K2 = constantes.

Equação 2

Em princípio, o atraso composto, Dc, poderia ter sido determinado como mostrado abaixo:

```
Dc = Ds + Dcir + Dt
```

Onde Ds = retardo de switching, Dcir = retardo do circuito (retardo da propagação de 1 bit) e DT = retardo da transmissão (nenhum retardo de carregamento para uma mensagem de 1500 bits)

Contudo, um dígito de retardo padrão é usado na prática para cada tecnologia do tipo de rede. Por exemplo, haverá uma figura de atraso padrão para Ethernet e para linhas seriais em qualquer taxa de bits específica.

Eis um exemplo de como pode ser a tabela de roteamento do gateway A no caso do diagrama de rede 6 acima. (Observe que componentes isolados do vetor de métrica não são mostrados, para efeito de simplicidade.)

Exemplo da tabela de roteamento:

Rede	Interface	Gateway seguinte	Métrico
1	NW 1	Nenhum	Conectado diretamente
2	NW 2	Nenhum	Conectado diretamente
3	NW3	Nenhum	Conectado diretamente
4	NW 2	C	1270
	NW3	B	1180

5	NW 2	C	1270
	NW3	B	2130
6	NW 2	C	2040
	NW3	B	1180

O processo básico de criação de uma tabela de roteamento trocando informações com os vizinhos é descrito pelo algoritmo Bellman-Ford. O algoritmo foi usado em uns protocolos mais adiantados tais como o RASGO (RFC 1058). Para lidar com redes mais complexas, o IGRP adiciona três recursos ao algoritmo básico de Bellman-Ford:

1. No lugar de uma métrica simples, um vetor de métrica é usado para caracterizar os caminhos. Uma única métrica composta pode ser calculada com base nesse vetor, de acordo com a Equação 1, acima. O uso de um vetor permite que o gateway acomode tipos de serviço diferentes, usando diversos coeficientes diferentes na equação 1. Também permite uma representação mais precisa das características da rede do que uma métrica única.
2. Em vez de escolher um caminho simples com a menor métrica, ele divide o tráfego em vários caminhos cujas métricas se encontram em um intervalo especificado. Isto permite que diversas rotas sejam usadas paralelamente, fornecendo uma largura de banda efetiva maior do que toda a rota única. Uma variação V é especificada pelo administrador da rede. Todos os caminhos com métrica composta mínima M são mantidos. Além disso, todos os caminhos cuja métrica for inferior a V x M são mantidos. O tráfego é distribuído entre caminhos múltiplos na proporção inversa ao medidor composto.
3. Há alguns problemas com esse conceito de variância. É difícil vir acima com estratégias que utilizam os valores da variação maiores de 1, e igualmente não conduz aos pacotes dar laços. No Cisco versão 8.2, o recurso de variância não está implementado. (Eu não sou certo em que liberação a característica foi removida.) O efeito deste é ajustar permanentemente a variação a 1.
4. Diversos recursos são introduzidos para oferecer estabilidade em situações nas quais a topologia está se modificando. Estas características são pretendidas impedir os loop de roteamento e a “contagem à infinidade,” que caracterizaram tentativas precedentes de usar o Ford-tipo algoritmos para este tipo de aplicativo. Os recursos de estabilidade primária são “holddowns”, “triggered updates” (atualizações disparadas), “split horizon” e “poisoning”. Estes serão discutidos com maiores detalhes abaixo.

A divisão do tráfego (ponto 2) aumenta um perigo sutil. A variação V é designada para permitir que os gateways utilizem caminhos paralelos de velocidades diferentes. Por exemplo, é possível que haja uma linha de 9600 BPS sendo executada em paralelo com uma linha de 19200 BPS, para redundância. Se a variação V é 1, simplesmente o melhor caminho estará usado. A linha de 9600 BPS não será usada assim se a linha de 19200 BPS tem uma confiabilidade razoável. (Contudo, se diversos trajetos são os mesmos, a carga será compartilhada entre eles.) Levantando a variação, nós podemos permitir que o tráfego seja rachado entre a melhor ruta e outras rotas que são quase como bons. Com uma grande variação, o tráfego será dividido entre as duas linhas. O perigo é que com uma variação de tamanho suficiente, os caminhos que se tornem alocados não sejam exatamente os mais lentos, mas que estejam realmente, na direção errada. Portanto, deveria haver uma regra adicional para evitar que o tráfego fosse enviado upstream: Nenhum tráfego é enviado aos caminhos cuja métrica composta remota (a métrica composta calculada no próximo salto) é superior à métrica composta calculada no gateway. Em geral, os administradores do sistema são encorajados a não definir a variação acima de 1, exceto em situações específicas em que os caminhos paralelos precisem ser usados. Nesse caso, a

variação é cuidadosamente configurada para fornecer os resultados certos.

O IGRP foi planejado para cuidar de vários tipos de serviço e vários protocolos. O tipo de serviço é uma especificação em um pacote de dados que altere a maneira que os trajetos devem ser avaliada. Por exemplo, o protocolo TCP/IP permite que o pacote especifique a importância relativa da alta largura de banda, do fraco atraso ou da alta confiabilidade. Geralmente, as aplicações interativas especificarão um retardo baixo, enquanto as aplicações de transferência de grande escala especificarão uma alta largura de banda. Esses requisitos determinam os valores relativos de K1 e K2 que são apropriados para uso em Eq. 1. Cada combinação de especificações no pacote que deve ser suportado é mencionada como um tipo de serviço. Para cada tipo de serviço deve ser escolhido um conjunto de parâmetros K1 e K2. Uma tabela de roteamento é mantida para cada tipo de serviço. Isso é feito porque os caminhos são selecionados e ordenados de acordo com a métrica composta definida por Eq. 1. Isso é diferente para cada tipo de serviço. As informações de todas essas tabelas de roteamento são combinadas para produzir mensagens atualizadas de roteamento intercambiadas pelos gateways, como descrito na Figura 7.

Recursos de estabilidade

Esta seção descreve holddowns, atualizações disparadas, split horizon e envenenamento. Esses recursos são projetados para impedir que os gateways selecionam rotas erradas. Como descrito no RFC 1058 , isto pode acontecer quando uma rota se torna inusável, devido à falha de um gateway ou de uma rede. A princípio, os gateways adjacentes detectam falhas. Então, eles enviam atualizações de roteamento que exibem a rota antiga como não-utilizável. Contudo, é possível para atualizações não alcançar algumas partes da rede de todo, ou ser atrasado em alcançar determinados gateways. Um gateway que ainda considera a rota antiga como adequada pode continuar a disseminar essas informações, reinserindo assim a rota defeituosa no sistema. Eventualmente esta informação propagará através da rede e virá para trás ao gateway que a injetar novamente. O resultado é uma rota circular.

De fato há alguma Redundância entre as contramedidas. Em princípio, holddowns e atualizações disparadas devem ser suficientes para evitar rotas errôneas no primeiro lugar. Na prática, entretanto, falhas de comunicação de diversos tipos pode fazer com que sejam insuficientes. O horizonte e o corrompimento de rota rachados são pretendidos impedir loop de roteamento em todo caso.

Normalmente, as tabelas de roteamento novas são enviadas aos gateways vizinhos numa base regular (cada 90 segundos à revelia, embora isto possa ser ajustado pelo administrador de sistema). Uma atualização iniciada é uma nova tabela de roteamento que é enviada imediatamente, em resposta a alguma mudança. A mudança a mais importante é remoção de uma rota. Isto pode acontecer porque um intervalo expirou (provavelmente um gateway vizinho ou uma linha foram para baixo), ou porque um mensagem de atualização do gateway seguinte no trajeto mostra que o trajeto é já não útil. Quando um gateway G detecta que uma rota não é mais aproveitável, ele dispara uma atualização imediatamente. Essa atualização mostrará que a rota não é utilizável. Considere o que acontece quando essa atualização atinge os gateways vizinhos. Se a rota do vizinho apontar de volta para G, o vizinho deve remover a rota. Isto faz com que o vizinho provoque uma atualização, etc. Assim uma falha provocará uma onda dos mensagens de atualização. Esta onda propagará durante todo essa parcela da rede em que as rotas atravessaram o gateway ou a rede falhada.

Atualizações disparadas seriam insuficientes se pudéssemos garantir que a onda de atualizações atingiria cada gateway apropriado imediatamente. No entanto, há dois problemas. Primeiramente,

os pacotes que contêm o mensagem de atualização podem ser deixados cair ou corrompido por algum link na rede. Em segundo lugar, as atualizações acionadas não acontecem instantaneamente. É possível que um gateway que ainda não tenha recebido a atualização disparada emita uma atualização normal exatamente no momento errado, fazendo com que a rota errada seja reinserida no vizinho que já recebeu a atualização disparada. Holddowns são projetados para solucionar esses problemas. A regra de holddown afirma que, quando uma rota é removida, nenhuma nova rota será aceita para o mesmo destino pelo mesmo período. Isso oferece às atualizações acionadas tempo para obter todos os outros gateways, para que possamos nos certificar de que as rotas que obtemos não são apenas algum gateway reinserindo o antigo. O período de holddown deve ser por muito tempo bastante permitir a onda das atualizações disparada ir durante todo a rede. Além disso, deve incluir alguns ciclos de transmissão comuns, para manejar pacotes perdidos. Considere o que acontece se uma das atualizações disparada é deixado cair ou corrompido. O gateway que emitiu essa atualização emitirá outra na próxima atualização regular. Isso reiniciará a onda de atualizações disparadas em vizinhos que perderam a onda inicial.

A combinação de atualizações disparada e de holddowns deve ser suficiente para obter livrada das rotas expiradas e para impedir que estejam reintroduzidas. Contudo, algumas precauções adicionais valem a pena fazer de qualquer maneira. Permitem muito redes com perdas, e redes que se tornaram divididas. As precauções adicionais para IGRP são split horizon e route poisoning. O Split horizon surge da observação de que nunca faz sentido enviar uma rota de volta na direção da qual veio. Considere a seguinte situação:

```
network 1        network 2
  -------------X-----------------X
           gateway A           gateway B
```

O gateway A dirá a B que tem uma rota à rede 1. Quando B envia atualizações a A, há nunca toda a razão para que mencione a rede 1. Desde que A é mais perto de 1, não há nenhuma razão para que considere ir através do B. A regra split horizon diz que um mensagem de atualização separado deve ser gerado para cada vizinho (realmente cada rede de vizinhança). A atualização de um determinado vizinho deve omitir as rotas que apontam para esse vizinho. Esta regra impede laços entre gateways contiguos. Por exemplo, suponha que a interface de A para a rede 1 falhe. Sem a regra split horizon, B seria dizendo a A que pode obter a 1. Desde que já não tem uma rota real, A pôde pegarar essa rota. Neste caso, A e B ambos teriam rotas a 1. Mas A apontaria a B e a B apontaria às atualizações disparada A. naturalmente e os holddowns devem impedir que este aconteça. Mas, como não há motivo para retornar informações ao local de origem, o horizonte de divisão vale a pena mesmo assim. Além de sua função de impedir loops, o horizonte dividido controla o tamanho das mensagens de atualização.

O horizonte dividido deve evitar loops entre os gateways adjacentes. O corrompimento de rota é pretendido quebrar laços maiores. A regra é que, quando uma atualização mostra que a métrica de uma rota existente aumentou o suficiente, existe um loop. A rota deverá ser removida e colocada em holddown. Atualmente a regra é que uma rota está removida se o métrica composta aumenta mais do que um fator de 1.1. Não é seguro para apenas nenhum aumento em métrica composta provocar a remoção da rota, desde que as mudanças métricas pequenas podem ocorrer devido às mudanças na ocupação de canal ou na confiança. Portanto, o fator de 1.1 é somente um heurístico. O valor exato não é obrigatório. Nós esperamos esta regra ser precisados somente de quebrar laços muito grandes, desde que os pequenos serão impedidos por atualizações disparada e por holddowns.

Desativar holddowns

A partir da versão 8.2, o código da Cisco fornece uma opção para desabilitar holddowns. A

desvantagem dos holddowns é que eles atrasam a adoção de uma nova rota, quando uma rota antiga falha. Com os parâmetros padrão, pode levar muitos minutos para um roteador adotar uma nova rota após uma alteração. Entretanto, pelos motivos explicados acima, não é seguro simplesmente remover holddowns. O resultado seria contagem até o infinito, como descrito no RFC 1058. Nós conjeturamos, mas não podemos provar, que com uma versão mais forte do corrompimento de rota, os holddowns estão precisados já não de parar o contagem até o infinito. Desta maneira, desabilitar holddowns habilita essa forma mais forte de corrupção de rota. Observe que o split horizon e atualizações disparadas ainda estão vigorando.

A forma mais forte de envenenamento de rota se baseia em uma contagem de nó. Se a contagem de saltos para um caminho aumentar, a rota será removida. Isto removerá obviamente as rotas que são ainda válidas. Se um elemento em algum outro lugar da rede sofrer alteração fazendo com que o caminho passe por mais um gateway, a contagem de saltos aumentará. Nesse caso, a rota ainda é válida. Entretanto, não há um meio totalmente seguro de distinguir este caso dos loops de roteamento (contagem até o infinito). Dessa maneira, a abordagem mais segura é remover a rota sempre que a contagem de saltos aumentar. Se a rota é legítima, ela será reinstalada pela próxima atualização, e isso causará uma atualização que reinstalará a rota em qualquer outro lugar do sistema.

Geralmente, o vetor de distância algorithms1 adota rotas novas facilmente. O problema é limpar completamente os antigos do sistema. Assim, uma regra excessivamente agressiva sobre como remover rotas suspeitas deve ser segura.

Detalhes do processo de atualização

O conjunto de processos descrito nas Figuras 4 a 8 visa a manipular um protocolo de rede simples, por exemplo, o protocolo TCP/IP, DECnet ou ISSO/OSI. No entanto, os detalhes do protocolo serão dados apenas para TCP/IP. Um único gateway pode processar dados que seguem mais de um protocolo. Porque cada protocolo tem estruturas de endereçamento e formatos de pacote de informação diferentes, o código de computador usado para executar figuras 4 8 será geralmente diferente para cada protocolo. O processo descrito em figura 4 variará o a maioria, como descrito nas notas detalhadas para figura 4. Os processos descritos na figura 5 a 8 terão a mesma estrutura geral. A principal diferença de protocolo para protocolo será o formato do pacote de atualização do roteamento, que deve ser definido como sendo compatível com um protocolo específico.

Observe que a definição de um destino pode variar de protocolo para protocolo. O método descrito aqui pode ser usado para o roteamento para hosts individuais, para redes ou para esquemas mais complexos de endereço hierárquico. O tipo de roteamento usado dependerá da estrutura de endereçamento do protocolo. A implementação atual de TCP/IP suporta apenas roteamento para redes IP. Assim o “destino” significa realmente a rede IP ou o subnet number. As informações de sub-rede são mantidas somente para redes conectadas.

As figuras 4 a 7 mostram pseudocódigos para várias partes do processo de roteamento usados pelos gateways. No início do programa, protocolos e parâmetros aceitáveis descrevendo cada interface são inseridos.

O gateway segurará somente determinados protocolos que estão listados. Qualquer comunicação de um sistema usando um protocolo que não esteja na lista será ignorada. As entradas de dados são as seguintes:

- Redes às quais o gateway está conectado.

- Largura de banda não carregada de cada rede.
- Atraso topológico de cada rede.
- Confiança de cada rede.
- Ocupação de canal de cada rede.
- MTU de cada rede.

A função métrica para cada trajeto de dados é computada então de acordo com a equação 1. Note que os primeiros três artigos são razoavelmente permanentes. Eles são uma função da tecnologia de rede subjacente e não dependem da carga. Eles podem ser definidos a partir de um arquivo de configuração ou por uma entrada direta do operador. Observe que o IGRP não utiliza atraso medido. Tanto a teoria quanto a experiência sugerem que é muito difícil para protocolos que utilizam o retardo medido manter o roteamento estável. Há dois parâmetros medidos: confiança e ocupação de canal. A confiabilidade se baseia nas taxas de erros reportadas pelo hardware ou firmware da interface de rede.

Além dessas entradas, o algoritmo de roteamento requer um valor para diversos parâmetros de roteamento. Isto inclui valores de temporizador, variação, e se os holddowns estão permitidos. Isso normalmente seria especificado por um arquivo de configuração ou entrada de operador. (Desde o lançamento do Cisco 8.2, a variação está permanentemente definida como 1).

Uma vez que a informação inicial é incorporada, as operações no gateway estão provocadas por eventos — a chegada de um pacote de dados em uma das interfaces de rede, ou por expiração de um temporizador. Os processos descritos nas Figuras 4 a 7 são acionados da seguinte forma:

- Quando um pacote chega, está processado de acordo com figura 4. Isso faz com que o pacote seja enviado para outra interface, descartado ou aceito para processamento posterior.
- Quando um pacote é aceitado pelo gateway para o processamento adicional, está analisado em uma forma do específico de protocolo não descrita nesta especificação. Se o pacote é uma atualização de roteamento, ele é processado de acordo com a Figura 5.
- A figura 6 mostra os eventos provocados por um temporizador. O cronômetro é definido de forma a gerar uma interrupção uma vez por segundo. Quando a interrupção ocorre, o processo mostrado na Figura 6 é executado.
- A figura 7 mostra uma sub-rotina da atualização de roteamento. As chamadas para esta sub-rotina são mostradas nas Figuras 5 e 6.
- Além disso, a figura 8 mostra detalhes de computação métrica mencionados nas figuras 5 e 7.

Há quatro constantes de horário crítico que propagação e expiração da rota do controle. Estes períodos constantes podem ser ajustados pelo administrador de sistema. Contudo, há uns valores padrão. Estas constantes de tempo são:

- Tempo de transmissão — As atualizações são transmissão por todos os gateways em todas as interfaces conectadas isto frequentemente. O padrão é a cada 90 segundos.
- Tempo inválido — Se nenhuma atualização foi recebida para um trajeto dado dentro desta quantidade de tempo, considera-se ter cronometrado para fora. Deve ser diversas vezes o tempo de transmissão, a fim permitir a possibilidade que os pacotes que contêm uma atualização poderiam ser deixados cair pela rede. O padrão é 3 vezes o tempo de transmissão.
- Tempo de contenção — Quando um destino se transformar inacessível (ou a métrica aumentou bastante para causar o envenenamento), o destino entra no “holddown”. Durante este estado, nenhum trajeto novo será aceitado para o mesmo destino para esta quantidade

de tempo. O tempo de espera indica a duração desse estado. O tempo de espera deve ser várias vezes o tempo de difusão. O valor padrão é 3 vezes o tempo de broadcast mais 10 segundos. (Conforme descrito na seção Desabilitar Holddowns, é possível desabilitar holddowns.)
- Tempo de descarga — Se nenhuma atualização foi recebida para um destino fornecido dentro desta quantidade de tempo, a entrada para ela está removida da tabela de roteamento. Observe a diferença entre o tempo inválido e o tempo de limpeza: Depois do tempo inválido, um caminho tem o tempo esgotado e é removido. Se não houver mais caminhos para um destino, ele agora será inalcançável. No entanto, a entrada do banco de dados para o destino permanece. Ela deve permanecer para reforçar o holddown. Após o tempo de descarga, a entrada do banco de dados é removida da tabela. Ele deve ser um pouco mais longo do que o tempo de holddown. O padrão é 7 vezes o tempo de transmissão.

Estas figuras pressupõem as seguintes estruturas de dados principais. Um conjunto separado dessas estruturas de dados é mantido para cada protocolo suportado pelo gateway. Dentro de cada protocolo, é mantido um conjunto separado de estruturas de dados para cada tipo de serviço a ser suportado.

Para cada destino conhecido no sistema, há uma lista (nula possivelmente) de caminhos para o destino, um tempo de expiração de holddown e um tempo recente de atualização. A hora da última atualização indica a última hora em que qualquer caminho para este destino foi incluído em uma atualização de outro gateway. Observe que também há tempos de atualização para cada caminho. Quando o último caminho para um destino for removido, o destino é colocado em holddown, a menos que os holddowns estejam desativados (Consulte a seção Desativar holddowns para obter mais informações). A hora de validade do holddown indica a hora na qual o holddown expira. O fato de que é diferente de zero indica que o destino está no holddown. Para economizar o tempo de cálculo, é bom manter uma métrica recomendada para cada destino. Isso é simplesmente o mínimo das métricas compostas para todos os caminhos até o destino.

Para cada caminho para um destino, há o endereço do próximo salto no caminho, a interface a ser usada, um vetor de métrica que caracteriza o caminho, incluindo retardo topológico, largura de banda, confiabilidade e ocupação do canal. A outra informação é associada igualmente com cada trajeto, incluindo o contagem de saltos, o MTU, o origem de informação, o métrica composta remoto, e um métrica composta calculado destes números de acordo com a equação 1. Há igualmente um último update time. A fonte de informações indica de onde provém a mais recente atualização para esse caminho. Na prática este é o mesmo que o endereço do salto seguinte. O horário da última atualização é simplesmente a hora em que a atualização mais recente chegou nesse caminho. Ele é utilizado para caminhos com o intervalo de tempo esgotado.

Observe que a mensagem de atualização do IGRP tem três partes: interior, sistema (significando "este sistema autônomo" mas não interior) e exterior. A seção interna é para as rotas para sub-redes. Não toda a informação de sub-rede é incluída. Somente as sub-redes de uma rede são incluídas. É a rede associada ao endereço para o qual a atualização está sendo enviada. Normalmente, as atualizações são difunidas em cada interface, portanto, essa rede é a rede a partir da qual a difusão está sendo enviada. (Outros casos elevaram para respostas a uma requisição IGRP e a um IGRP ponto a ponto.) As redes principal (por exemplo, NON-sub-redes) estão postas na parcela do sistema do mensagem de atualização a menos que forem embandeiradas especificamente como o exterior.

Uma rede será embandeirada como o exterior se era instruída de um outro gateway e a informação chegou na parcela exterior do mensagem de atualização. A implementação da Cisco também permite que o administrador do sistema declare redes específicas como exteriores.

Rotas externas também são conhecidas como padrão candidato. São as rotas a que atravesse ou os gateways que são considerados ser apropriados como padrões, a ser usados quando não há nenhuma rota explícita a um destino. Por exemplo, na Rutgers, configuramos o gateway que conecta a Rutgers à nossa rede regional, de modo que ela sinalize como externa a rota para o backbone NSFnet. A implementação do Cisco escolhe uma rota padrão selecionando a rota exterior com a menor métrica.

As seguintes seções são pretendidas esclarecer determinadas porções de figuras 4 8.

Roteamento de Pacotes

A Figura 4 descreve o processamento total de pacotes de entrada. Seu uso tem por fim explicar a terminologia. Obviamente, esta não é uma descrição completa do que faz um gateway IP.

Esse processo utilize a lista de protocolos suportados e informações sobre as interfaces inseridas quando o gateway foi inicializado. Os detalhes do processamento do pacote dependem do protocolo usado pelo pacote. Isso é determinado na Etapa A. A Etapa A é a única parte da Figura 4 que é compartilhada por todos os protocolos. Uma vez que o tipo de protocolo é sabido, a aplicação de figura 4 apropriada ao tipo de protocolo está usada. Os detalhes do conteúdo do pacote são descritos pelas especificações do protocolo. As especificações de um protocolo incluem um procedimento para determinar o destino de um pacote, um procedimento para comparar o destino com os próprios endereços do gateway para determinar se o próprio gateway é o destino, um procedimento para determinar se um pacote é uma transmissão e um procedimento para determinar se o destino é parte de uma rede especificada. Estes procedimentos são usados nas etapas B e no C de figura 4. O teste na etapa D exige uma busca dos destinos alistados na tabela de roteamento. O teste é satisfeito se há uma entrada na tabela de roteamento para o destino, e esse destino associou com ele pelo menos um trajeto útil. Note que os dados do destino e do trajeto usados neste e na próxima etapa estão mantidos separadamente para cada tipo de serviço apoiado. Portanto, essa etapa começa com a determinação do tipo de serviço especificado pelo pacote e com a seleção do conjunto correspondente de estruturas de dados a ser usado para essa e para a próxima etapa.

Um trajeto é útil para fins das etapas D e E se seu métrica composta remoto é menos do que seu métrica composta. Um caminho cuja métrica composta remota seja maior que a sua métrica composta, é um caminho cujo próximo salto é “mais distante” do destino, conforme medido pela métrica. Isso é conhecido como "caminho de upstream". Normalmente, era de se esperar que o uso de métricas evitasse que caminhos de upstream fossem escolhidos. É fácil perceber que um caminho de upstream nunca será o mais conveniente. Contudo, se uma grande variação é permitida, os trajetos diferentes do melhor podem ser usados. Alguma daquelas podia ser ascendente.

O passo E computa o caminho a ser utilizado. Os caminhos cuja métrica composta remota não é menor que suas métricas compostas não são considerados. Se mais de um trajeto é aceitável, tais trajetos estão usados em um formulário tornado mais pesado da alternação do arredondamento robin. A freqüência com que um caminho é utilizado é inversamente proporcional à sua métrica composta.

Recebimento de Atualizações de Roteamento

A figura 5 descreve o processamento de uma atualização de roteamento recebida de um gateway vizinho. Tais atualizações consistem em uma lista de entradas, cada qual dê a informação para um destino único. Pode haver mais de uma entrada para o mesmo destino em uma única

atualização de roteamento, para acomodar vários tipos de serviços. Cada um destas entradas é processada individualmente, como descrito na figura 5. Se uma entrada estiver na seção externa da atualização, o flag externo será definido para o destino se for adicionado como resultado do processo.

Todo o processo descrito na Figura 5 deve ser repetido uma vez para cada tipo de serviço suportado pelo gateway, usando o conjunto de informações de destino/caminho associadas a esse tipo de serviço. Isto é mostrado no loop mais distante na figura 5. A atualização de roteamento inteira deve ser processada uma vez para cada tipo de serviço. Observe que a implementação atual de IGRP não suporta vários tipos de serviço, portanto o circuito mais externo não é de fato implementado.

No passo A, os testes básicos de aceitabilidade são feitos no caminho. Isso deve incluir testes de racionalidade para o destino. Os números de rede impossíveis ("marcianos") devem ser rejeitados. (Refira o RFC 1009 e o RFC 1122 para mais informação.) As atualizações estão rejeitadas igualmente se o destino que referem está no holddown, isto é o tempo de expiração de holddown é diferente de zero e mais tarde do que as horas atual.

No Passo B, a tabela de roteamento é procurada para ver se esta entrada descreve um caminho que já é conhecido. Um trajeto na tabela de roteamento é definido pelo destino com que é associada, pelo salto seguinte alistado como parte do trajeto, pela interface de saída a ser usados para o trajeto, e pelo origem de informação (o endereço de que a atualização veio — na prática normalmente o mesmo que o salto seguinte). A entrada do pacote de atualização descreve um caminho cujo destino está listado na entrada, cuja interface de saída é que originou a atualização e cujo salto seguinte e a fonte de informações são o endereço do gateway que enviou a atualização (a "origem" S).

Nas Etapas H e T, o processo de atualização descrito na Figura 7 é agendado. Na verdade, este processo será executado após a conclusão completa do processo descrito na figura 5. Isto é, o processo de atualização descrito na figura 7 acontecerá somente uma vez, mesmo se é provocado diversas vezes durante o processamento descrito na figura 5. Além disso, são necessárias precauções para evitar a emissão de atualizações muito freqüentes quando a rede é alterada rapidamente.

A etapa K é executada se o destino descrito pela entrada atual no pacote de atualização já existe na tabela de roteamento. K compara a nova medição composta calculada a partir dos dados no pacote de atualização com a melhor medição composta do destino. Observe que a melhor métrica composta não é recalculada nesse momento, portanto, se o caminho considerado já estiver na tabela de roteamento, esse teste poderá comparar métricas novas e antigas para o mesmo caminho.

A etapa L é executada para os trajetos que são mais ruins do que melhor métrica composta existente. Isto inclui ambos os trajetos novos que são mais ruins do que os existências e os trajetos existentes cujo métrica composta aumentou. A Etapa L testa se o novo caminho é aceitável. Note que este teste executa ambos o teste para se um trajeto novo é bom bastante de se manter, e corrompimento de rota. Para ser aceitável, o valor do retardo não deve indicar destino inalcançável (para a implementação de IP atual, todos aqueles em um campo de 24 bits) e a métrica composta (calculada conforme especificado na figura 8) deve ser admissível. Para determinar se o métrica composta é aceitável, compare-o com o medidor composto de todos trajetos restantes ao destino. Deixe M ser o mínimo destes. O novo caminho será aceitável se for < V X M, ONDE V É A VARIANTE DEFINIDA QUANDO O GATEWAY FOI INCIALIZADO. SE V = 1 (O QUE SEMPRE É VERDADEIRO A PARTIR DO CISCO VERSÃO 8.2), ENTÃO QUALQUER UMA MÉTRICA PIOR QUE A EXISTENTE NÃO É ACEITÁVEL. HÁ UMA EXCEÇÃO PARA

ISSO: SE O CAMINHO JÁ EXISTIR E FOR O ÚNICO CAMINHO PARA O DESTINO, O CAMINHO SERÁ MANTIDO SE A MÉTRICA NÃO PRECISAR SER AUMENTADA EM MAIS DE 10% (OU ONDE OS HOLDDOWNS ESTIVEREM DESATIVADOS, SE A CONTAGEM DE SALTOS NÃO TIVER AUMENTADO).

A etapa V está concluída quando as novas informações de um caminho indicam que a medição composta será reduzida. O medidor composto de todos os trajetos ao destino D é comparado. Nesta comparação, a nova métrica composta para P é usada, em vez da que aparece na tabela de roteamento. A métrica composta mínima M é calculada. Em seguida, todos os caminhos para D são examinados novamente. Se a métrica composta para algum caminho for maior que M x V, o caminho é removido. V é a variação, inserida quando o gateway foi inicializado. (Desde o lançamento do Cisco 8.2, a variação está permanentemente definida como 1).

Processamento periódico

O processo descrito na figura 6 é provocado uma vez ao segundo. Ele examina vários temporizadores na tabela de roteamento para ver se algum deles expirou. Esses cronômetros são descritos acima.

Na Etapa U, o processo descrito na Figura 7 é ativado.

As Etapas R e S são necessárias porque as métricas compostas armazenadas na tabela de roteamento dependem da ocupação do canal que muda com o tempo, com base nas medições. A ocupação do canal é periodicamente recalculada, usando-se uma média móvel do tráfego medido através da interface. Se o valor recém-calculado diferir do valor existente, todas as métricas compostas envolvendo essa interface deverão ser ajustadas. Cada caminho mostrado na tabela de roteamento é examinado. Qualquer caminho cujo salto seguinte utilize a interface I possui sua métrica composta recalculada. Isso é feito de acordo com a Equação 1, utilizando como ocupação do canal o máximo do valor armazenado na tabela de roteamenteo como parte da métrica de caminhos e a ocupação do canal recém calculada da interface.

Gerar mensagens de atualização

A Figura 7 descreve como o gateway gera mensagens de atualização para serem enviadas a outros gateways. Uma mensagem separada é gerada para cada interface de rede anexada ao gateway. Essa mensagem é enviada para todos os demais gateways que podem ser atingidos por meio da interface (Passo J). Em geral, isso é feito através do envio da mensagem como broadcast. Entretanto, se a tecnologia de rede ou o protocolo não permitir broadcasts, talvez seja necessário enviar a mensagem individualmente para cada gateway.

Geralmente, a mensagem é acumulada adicionando uma entrada para cada destino na tabela de roteamento, na etapa G. Note que os dados do destino/trajeto associados com cada tipo de serviço devem ser usados. Em último caso, uma nova entrada é adicionada à atualização de cada destino para cada tipo de serviço. Entretanto, antes de adicionar uma entrada na mensagem de atualização na Etapa G, as entradas já adicionadas são varridas. Se a entrada nova está já atual no mensagem de atualização, não está adicionada outra vez. Uma entrada nova duplica existente quando os destinos e os gateways do salto seguinte são os mesmos.

Para a simplicidade, o pseudocode omite uma coisa — as mensagens da atualização de IGRP têm três porções: o interior, o sistema, e o exterior, assim que significam que há realmente três laços sobre destinos. O primeiro inclui somente sub-redes da rede a que a atualização está sendo enviada. O segundo inclui todas as redes principal (por exemplo, NON-sub-redes) que não são

embandeiradas como o exterior. O terço inclui todas as redes principal que são embandeiradas como o exterior.

O Passo E implementa o teste de horizonte dividido. No caso normal, esse teste falhará para rotas cujo melhor caminho passa pela mesma interface pela qual a interface está sendo enviada. No entanto, se a atualização estiver sendo enviada para um destino específico (por exemplo, em resposta a uma solicitação de IGRP, a partir de outro gateway ou como parte do IGRP ponto-a-ponto), o horizonte dividido falha somente se o melhor caminho, originalmente vindo daquele destino (sua origem de informação é a mesma do destino), e sua interface de saída forem iguais àquela de onde a solicitação veio.

Calcular informações sobre métrica

A figura 8 descreve como as informações de métricas são processadas a partir das mensagens atualizadas recebidas pelo gateway e como elas são geradas para que as mensagens atualizadas sejam enviadas pelo gateway. Observe que a entrada é baseada em um caminho em particular para o destino. Se há mais de um trajeto ao destino, um trajeto cujo métrica composta seja mínimo está escolhido. Se mais de um caminho tiver a métrica de composição mínima, uma regra arbitrária de quebra de vínculo será usada. (Para a maioria dos protocolos, isso se baseia no endereço do gateway de próximo salto).

Figura 4 — Processando pacotes recebidos

```
Data packet arrives using interface I

A   Determine protocol used by packet

    If protocol is not supported
      then discard packet

B   If destination address matches any of gateway's addresses
    or the broadcast address
      then process packet in protocol-specific way

C   If destination is on a directly-connected network
      then send packet direct to the destination, using
      the encapsulation appropriate to the protocol and link type

D   If there are no paths to the destination in the routing
    table, or all paths are upstream
      then send protocol-specific error message and discard the packet

E   Choose the next path to use. If there are more than
    one, alternate round-robin with frequency proportional
    to inverse of composite metric.

    Get next hop from path chosen in previous step.

    Send packet to next hop, using encapsulation appropriate
    to protocol and data link type.
```

Figura 5 — Processando atualizações de roteamento entrante

```
Routing update arrives from source S

    For each type of service supported by gateway
      Use routing data associated with this type of service

      For each destination D shown in update
```

```
A       If D is unacceptable or in holddown
          then ignore this entry and continue loop with next destination D

B       Compute metrics for path P to D via S (see Fig 8)

        If destination D is not already in the routing table
        then Begin

          Add path P to the routing table, setting last
          update times for P and D to current time.

H         Trigger an update

          Set composite metric for D and P to new composite
          metric computed in step B.

          End

        Else begin (dest. D is already in routing table)

K         Compare the new composite metric for P with best
          existing metric for D.

           New > old:

L            If D is shown as unreachable in the update,
             or holddowns are enabled and
              the new composite metric >
                (the existing metric for D) * V
                [use 1.1 instead of V if V = 1,
                as it is as of Cisco release 8.2]
O            or holddowns are disabled and
             P has a new hop count > old hop count
             then Begin

              Remove P from routing table if present

              If P was the last route to D
                then Unless holddowns are disabled
                    Set holddown time for D to
                     current time + holddown time
T                  and Trigger an update

              End

             else Begin

              Compute new best composite metric for D

              Put the new metric information into the
              entry for P in the routing table

              Add path P to the routing table if it
              was not present.

              Set last update times for P and D to
              current time.

              End

           New <= OLD:

V            Set composite metric for D and P to new
```

```
            composite metric computed in step B.

            If any other paths to D are now outside the
            variance, remove them.

            Put the new metric information into the
            entry for P in the routing table

            Set last update times for P and D to
            current time.

          End

        End of for

      End of for
```

Figura 6 — Processamento periódico

```
Process is activated by regular clock, e.g. once per second

    For each path P in the routing table (except directly
    connected interfaces)

      If current time < P'S LAST UPDATE TIME + INVALID TIME
        THEN CONTINUE WITH THE NEXT PATH P

      Remove P from routing table

      If P was the last route to D
        then Set metric for D to inaccessible
          Unless holddowns are disabled,
            Start holddown timer for D and
          Trigger an update

        else Recompute the best metric for D

      End of for

    For each destination D in the routing table

      If D's metric is inaccessible
        then Begin

        Clear all paths to D

        If current time >= D's last update time + flush time
          then Remove entry for D

        End

      End of for

    For each network interface I attached to the gateway

R     Recompute channel occupancy and error rate

S     If channel occupancy or error rate has changed,
        then recompute metrics

      End of for

    At intervals of broadcast time
```

```
U     Trigger update
```

Figura 7 — Gerencia a atualização

```
Process is caused by "trigger update"

    For each network interface I attached to the gateway

      Create empty update message

      For each type of service S supported

        Use path/destination data for S

        For each destination D

E         If any paths to D have a next hop reached through I
            then continue with the next destination

          If any paths to D with minimal composite metric are
          already in the update message
            then continue with the next destination

G         Create an entry for D in the update message, using
          metric information from a path with minimal
          composite metric (see Fig. 8)

          End of for

        End of for

J     If there are any entries in the update message
       then send it out interface I

      End of for
```

Figura 8 — Detalhes de computações métricas

Esta seção descreve o procedimento para métricos de computação e contagens de saltos de uma atualização de roteamento de chegada. A entrada a esta função é a entrada para um destino específico em um pacote de atualização de roteamento. A saída é um vetor do medidor que possa ser usado para computar o métrica composta, e de um contagem de saltos. Se este caminho for adicionado à tabela de roteamento, o vetor de métrica inteiro é inserido na tabela. Os parâmetros de interface usados nas seguintes definições são os definidos quando o gateway foi inicializado, para a interface em que a atualização de roteamento foi introduzida, com exceção de que a ocupação de canais e a confiabilidade têm como base uma média transitória de tráfego medido por meio da interface.

- Atraso = atraso do retardo topológico do pacote + da relação
- Bandwidth = max (largura de banda do pacote, largura de banda do pacote)
- Reliability = min (confiabilidade a partir do pacote, confiabilidade da interface)
- Ocupação de canal = max (ocupação de canal do pacote, ocupação do canal de interface)(Máximo é usado para a largura de banda porque a métrica da largura de banda é armazenada no formulário inverso. Conceptualmente, nós queremos a largura de banda mínima.) Note que a ocupação de canal original do pacote deve ser salvar, desde que será recalcular necessário a ocupação de canal eficaz sempre que o manutenção de canal de interface muda.

Os elementos descritos a seguir não fazem parte do vetor métrico, mas também são mantidos na tabela de roteamento como características do caminho:

- Contagem de saltos = contagem de saltos do pacote.
- MTU = min (MTU a partir de pacote, MTU de interface).
- Métrica composta remoto = calculado da equação 1 usando os valores de métrica do pacote. Isto é, os componentes de métrica são aqueles do pacote e não são atualizados como mostrado acima. Obviamente isto deve ser calculado antes que os ajustes mostrados acima estejam feitos.
- Métrica composta = calculada a partir da equação 1, utilizando valores métricos calculados como descrito nesta seção.

O resto desta seção descreve o procedimento de métricas de computação e contagem de nó das atualizações de roteamentos a serem enviadas.

Essa função determina as informações de métricas e a contagem de nós a serem colocadas em um pacote de atualização de saída. Está baseada em um trajeto específico a um destino, se há algum trajeto útil. Caso não haja caminhos ou os caminhos sejam todos de upstream, o destino é chamado de inacessível.

```
If destination is inaccessible, this is indicated by using a specific
        value in the delay field. This value is chosen to be larger
        than the largest valid delay. For the IP implementation this is
        all ones in a 24-bit field.

   If destination is directly reachable through one of the interfaces, use
        the delay, bandwidth, reliability, and channel occupancy of the
        interface. Set hop count to 0.

   Otherwise, use the vector of metrics associated with the path in the
        routing table. Add one to the hop count from the path in the
        routing table.
```

Detalhes da implementação de IP

Este resumo da seção descreve os formatos de pacote usados pelo Cisco IGRP. O IGRP é enviado usando datagramas IP com protocolo IP 9 (IGP). O pacote é iniciado com um cabeçalho. Começa imediatamente depois do cabeçalho IP.

```
unsigned version: 4;  /* protocol version number */
    unsigned opcode: 4;   /* opcode */
    uchar edition;        /* edition number */
    ushort asystem;       /* autonomous system number */
    ushort ninterior;     /* number of subnets in local net */
    ushort nsystem;       /* number of networks in AS */
    ushort nexterior;     /* number of networks outside AS */
    ushort checksum;      /* checksum of IGRP header and data */
```

Em mensagens de atualização, as informações de roteamento seguem imediatamente após o cabeçalho.

O número de versão é os pacotes 1. que têm outros números de versão é ignorado atualmente.

Opcode pode ser 1 = atualização ou 2 = requisição.

Isto indica o tipo de mensagem. O formato dos dois tipos de mensagem será mostrado abaixo.

Edição é um número de série que é incrementado sempre que há uma alteração na tabela de roteamento. (Isto é feito naquelas circunstâncias em que o pseudocode acima diz provocar uma atualização de roteamento.) O número de edição permite que os gateways evitem processar as

atualizações que contêm a informação que têm considerado já. (Isto não é executado atualmente. Isto é, o número de edição é gerado corretamente, mas é ignorado na entrada. Como é possível que pacotes sejam descartados, não está claro se o número da edição é suficiente para evitar o processo de duplicação. Seria necessário verificar se todos os pacotes associados à edição foram processados.

Asystem é o número de sistema autônomo. Na implementação Cisco, um gateway pode participar em mais de um sistema autônomo. Cada um desses sistemas executa seu próprio protocolo IGRP. Conceitualmente, existem tabelas de roteamento completamente separadas para cada sistema autônomo. As rotas que chegam de um sistema autônomo via IGRP são enviadas apenas em atualizações para esse AS. Este campo permite que o gateway selecione qual conjunto de tabelas de roteamento usar para processamento da mensagem. Se o gateway receber uma mensagem de IGRP para um AS não-configurado, a mensagem será ignorada. Na verdade, a implementação Cisco permite o "vazamento" de informações de um AS para outro. No entanto, eu considero isso uma ferramenta administrativa e não parte do protocolo.

Ninterior, nsystem e nexterior indicam o número de entradas em cada uma das três seções das mensagens de atualização. Essas seções foram descritas acima. Não há nenhuma outra delimitação entre as seções. As primeiras entradas ninterior são capturadas para serem internas, as próximas entradas nsystem como sistema e as últimas nexterior como externas.

A soma de verificação é de IP, calculada usando o mesmo algoritmo usado em uma soma de verificação de UDP. A soma de verificação é calculada no cabeçalho do IGRP e em todas as informações de roteamento que o seguem. O campo de checksum é ajustado a zero ao computar a soma de verificação. A soma de verificação não inclui o cabeçalho IP, nem há todo o cabeçalho virtual como no UDP e no TCP.

Solicitações

Uma requisição IGRP pede que o receptor envie sua tabela de roteamento. O mensagem request tem somente um encabeçamento. Somente a versão, o opcode, e os campos do asystem são usados. Todos campos restantes são zero. Espera-se que o destinatário envie uma mensagem de atualização de IGRP normal ao requisitante.

Atualizações

Uma mensagem da atualização de IGRP contém um encabeçamento, seguido imediatamente por entradas de roteamento. São incluídas tantas entradas de roteamento quanto caberão em um datagrama de 1500 bytes (incluindo o cabeçalho IP). Com declarações de estrutura atual, isto permite até 104 entradas. Se forem necessárias mais entradas, diversas mensagens de atualização são enviadas. Como mensagens de atualização são simplesmente processadas entrada por entrada, não há nenhuma vantagem em utilizar uma única mensagem fragmentada em vez de várias outras independentes.

Está aqui a estrutura de uma entrada de roteamento:

```
uchar number[3];       /* 3 significant octets of IP address */
    uchar delay[3];        /* delay, in tens of microseconds */
    uchar bandwidth[3];    /* bandwidth, in units of 1 Kbit/sec */
    uchar mtu[2];          /* MTU, in octets */
    uchar reliability;     /* percent packets successfully tx/rx */
    uchar load;            /* percent of channel occupied */
    uchar hopcount;        /* hop count */
```

Os campos definem que uchar[2] e uchar[3] são simplesmente inteiros binários de 16 e 24 bits, na ordem normal da rede de IP.

O número define o destino descrito. Ele é um endereço IP. Para economizar espaço, somente os 3 primeiros bytes do endereço IP são fornecidos, exceto na seção interior. Na seção interior, os últimos 3 bytes são fornecidos. Para rotas de sistema e externas, não são possíveis sub-redes, portanto o byte de ordem baixa é zero. Rotas internas são sempre sub-redes de uma rede conhecida, portanto, o primeiro byte desse número de rede é fornecido.

O retardo é em unidades de 10 microssegundos. Isto dá um intervalo de 10 microssegundos a 168 segundos, que parece suficiente. Um retardo geral indica que a rede não pode ser alcançada.

A largura de banda é a largura de banda inversa, em bits por segundos, em escala pelo fator 1.0e10. O intervalo é de uma linha de 1200 BPS a 10 Gbps. (Ou seja, se a largura de banda for N Kbps, o número usado é 10000000 / N).

O MTU está em bytes.

A confiança é dada como uma fração de 255. Isto é, 255 são 100%.

A carga é determinada como uma fração de 255.

O contagem de saltos é uma contagem simples.

A despeito das unidades um pouco estranhas usadas para largura de banda e retardo, alguns exemplos aparecem ordenados. Estes são os valores padrão usados para diversos meios comuns.

	Delay	Bandwidth
Satellite	200,000 (2 sec)	20 (500 Mbit)
Ethernet	100 (1 ms)	1,000
1.544 Mbit	2000 (20 ms)	6,476
64 Kbit	2000	156,250
56 Kbit	2000	178,571
10 Kbit	2000	1,000,000
1 Kbit	2000	10,000,000

Cálculos métricos

Aqui está uma descrição da forma como a métrica composta é realmente computada na versão do Cisco 8.0(3).

```
metric = [K1*bandwidth + (K2*bandwidth)/(256 - load) + K3*delay] *
                        [K5/(reliability + K4)]

    If K5 == 0, the reliability term is not included.

    The default version of IGRP has K1 == K3 == 1, K2 == K4 == K5 == 0
```

Informações Relacionadas

- Página de Suporte do IP Routing
- Página de suporte de IGRP
- Suporte Técnico - Cisco Systems