Introduction à IGRP

Contenu

Introduction

Ce document présente le protocole Interior Gateway Routing Protocol (IGRP). Il a deux buts. Le premier est d'offrir une introduction à la technologie IGRP à ceux qui sont intéressés par son utilisation, son évaluation et sa possible implémentation. Le deuxième est de donner une exposition plus large à quelques idées et concepts intéressants incarnés par le protocole IGRP. Veuillez vous reporter à Configuration du protocole IGRP, Implémentation Cisco du protocole IGRP et Commandes IGRP pour en savoir plus sur comment configurer le protocole IGRP.

Buts pour l'IGRP

Le protocole IGRP permet à un certain nombre de passerelles pour coordonner leur routage. Ses buts sont les suivants :

- Routage stable même dans les réseaux très grands ou complexes. Aucune boucle de routage ne devrait se produire, même pendant que des coupures.
- Réponse rapide aux changements de la topologie du réseau.

- Bas temps système. C'est-à-dire, IGRP lui-même ne devrait pas utiliser plus de bande passante que ce qui est réellement nécessaire pour sa tâche.
- Partage du trafic parmi plusieurs artères de parallèle quand ils sont de l'avantage rudement égal.
- Prendre en considération les taux d'erreur et le niveau du trafic sur des différents chemins.

L'implémentation d'IGRP en cours manipule le routage pour le TCP/IP. Cependant, la conception de base est destinée pour pouvoir manipuler un grand choix de protocoles.

Aucun outil ne va résoudre tous les problèmes de routage. Par convention le problème de routage est divisé en plusieurs parties. Des protocoles tels que l'IGRP s'appellent les « protocoles de passerelle interne » (des IGP). Ils sont destinés pour l'usage dans une série unique de réseaux, sous une Gestion simple ou des Gestions étroitement coordonnées. De tels ensembles de réseaux sont connectés par des « protocoles de passerelle externe » (des EGPs). Un IGP est conçu pour maintenir beaucoup de détail au sujet de topologie du réseau. La priorité en concevant un IGP est placée sur produire des routes optimales et répondre rapidement aux modifications. Une EGP est destinée pour protéger un système des réseaux contre des erreurs ou la fausse déclaration intentionnelle par d'autres systèmes, BGP est un tel Exterior Gateway Protocol. La priorité en concevant une EGP est sur la stabilité et les contrôles administratifs. Souvent il est suffisant qu'une EGP produise une artère raisonnable, plutôt que la route optimale.

L'IGRP a quelques similitudes à des protocoles plus anciens tels que le RIP du Protocole d'Information de Routage, du Berkeley de Xerox, et les moulins de Dave bonjour. Il diffère de ces protocoles principalement en étant conçu pour de plus grands et plus complexes réseaux. Voyez la comparaison avec la section de RIP pour une comparaison plus détaillée avec le RIP, qui est le plus très utilisé de la génération plus ancienne des protocoles.

Comme ces protocoles plus anciens, l'IGRP est un protocole de vecteur de distance. Dans un tel protocole, les passerelles permutent les informations de routage seulement avec des passerelles contiguës. Ces informations de routage contiennent un résumé des informations sur le reste du réseau. Il peut afficher mathématiquement que toutes les passerelles prises ensemble résolvent un problème d'optimisation par quelles quantités à un algorithme distribué. Chaque passerelle doit seulement résoudre une partie du problème, et elle seulement doit recevoir une partie de toutes les données.

La principale alternative à l'IGRP est l'Enhanced IGRP (EIGRP) et une classe des algorithmes désignés sous le nom de la SPF (Shortest-Path d'abord). L'OSPF utilise ce concept. Pour se renseigner plus sur l'OSPF référez-vous au guide de conception OSPF. L'OSPF que ceux-ci sont est basé sur une technique d'inondation, où chaque passerelle est tenue à jour au sujet du statut de chaque interface sur chaque autre passerelle. Chaque passerelle résout indépendamment le problème d'optimisation de son point de vue utilisant des données pour le tout le réseau. Il y a des avantages à chaque approche. Dans certaines circonstances la SPF peut pouvoir répondre à change plus rapidement. Afin d'empêcher des boucles de routage, l'IGRP doit ignorer de nouvelles données pendant quelques minutes après certains genres de modifications. Puisque la SPF a les informations directement de chaque passerelle, il peut éviter ces boucles de routage. Ainsi il peut agir sur les nouvelles informations immédiatement. Cependant, la SPF doit traiter essentiellement plus de données que l'IGRP, en structures de données internes et dans les messages entre les passerelles.

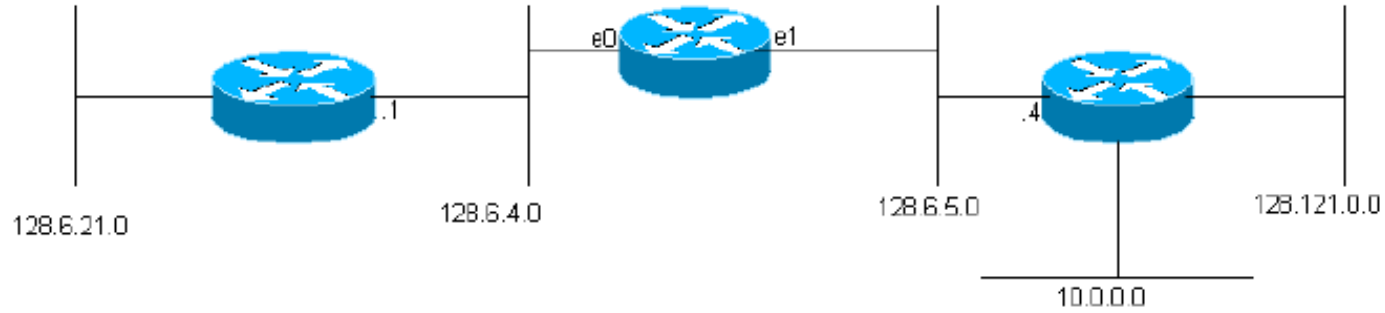
Le problème de routage

L'IGRP est destiné pour l'usage dans des passerelles connectant plusieurs réseaux. Nous

supposons que les réseaux utilisent la technologie paquet paquet. En effet les passerelles agissent en tant que commutateurs de paquets. Quand un système connecté à un réseau veut envoyer un paquet à un système sur un réseau différent, il adresse le paquet à une passerelle. Si la destination est sur un des réseaux connectés à la passerelle, la passerelle expédiera le paquet à la destination. Si la destination est plus éloignée, la passerelle expédiera le paquet à une autre passerelle qui est plus près de la destination. Tables de routage d'utilisation de passerelles pour les aider à décider quoi faire avec des paquets. Voici une table de routage d'exemple simple. (Les adresses utilisées dans les exemples sont des adresses IP prises de l'université de Rutgers. Notez que le problème de base de routage est semblable pour d'autres protocoles aussi bien, mais cette description supposera que l'IGRP est utilisé pour l'IP de routage.)

Figure 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
```



(Les tables de routage réelles IGRP ont les informations complémentaires pour chaque passerelle, car nous verrons.) Cette passerelle est connectée à deux Ethernet, appelés 0 et 1. Ils ont été donnés à des network number IP (réellement numéros de sous-réseau) 128.6.4 et 128.6.5. Ainsi des paquets adressés pour ces réseaux spécifiques peuvent être envoyés directement à la destination, simplement à l'aide de l'interface Ethernet appropriée. Il y a deux passerelles, 128.6.4.1 et 128.6.5.4 voisins. Des paquets pour des réseaux autres que 128.6.4 et 128.6.5 seront expédiés à une ou à l'autre de ces passerelles. La table de routage indique quelle passerelle devrait être utilisée pour laquelle réseau. Par exemple, des paquets adressés à un hôte sur le réseau 10 devraient être expédiés à la passerelle 128.6.5.4. On espère que cette passerelle est plus près du réseau 10, c.-à-d. que le meilleur chemin au réseau 10 passe par cette passerelle. L'objectif principal de l'IGRP est permettent aux passerelles pour construire et mettre à jour des tables de routage comme ceci.

Résumé d'IGRP

Comme mentionné ci-dessus, l'IGRP est un protocole qui permet à des passerelles pour accumuler leur table de routage en permutant les informations avec d'autres passerelles. Une passerelle commence avec des entrées pour tous les réseaux qui sont directement connectés à elle. Il obtient des informations sur d'autres réseaux en permutant des mises à jour de routage avec des passerelles contiguës. Dans le cas le plus simple, la passerelle trouvera un chemin qui représente la meilleure manière d'obtenir à chaque réseau. Un chemin est caractérisé par la prochaine passerelle à laquelle des paquets devraient être envoyés, l'interface réseau qui devrait

être utilisée, et les informations métriques. Les informations métriques sont un ensemble de nombres qui caractérisent combien bon le chemin est. Ceci permet à la passerelle pour comparer les chemins qu'elle a entendus de diverses passerelles et pour décider lesquels pour utiliser. Il y a souvent des cas où il semble raisonnable de séparer le trafic entre deux chemins ou plus. L'IGRP fera ceci toutes les fois que deux chemins ou plus sont également bons. L'utilisateur peut également le configurer pour séparer le trafic quand les chemins sont presque également bons. Dans ce cas plus de trafic sera envoyé le long du chemin avec la mesure meilleure. L'intention est que le trafic peut être séparé entre des 9600 bps rayent et des 19200 bps rayent, et la ligne 19200 obtiendra rudement deux fois autant le trafic que les 9600 bps rayent.

Les mesures utilisées par IGRP incluent ce qui suit :

- Temps de retard topologique
- Bande passante du segment de bande passante le plus étroit du chemin
- Occupation de la Manche du chemin
- Fiabilité du chemin

Le temps de retard topologique est la durée qu'il prendrait pour obtenir à la destination le long de ce chemin, assumant un réseau déchargé. Naturellement il y a retard supplémentaire quand le réseau est chargé. Cependant, le chargement est expliqué à l'aide du chiffre d'occupation de canal, pas en tentant pour mesurer des retards d'effectif. La bande passante de chemin est simplement la bande passante dans des bits par seconde du lien le plus lent dans le chemin. L'occupation de la Manche indique quelle quantité de cette bande passante est actuellement en service. Il est mesuré, et changera avec le chargement. La fiabilité indique le taux d'erreur en cours. C'est la fraction des paquets qui arrivent à la destination intacte. Il est mesuré.

Bien qu'ils ne soient pas utilisés en tant qu'élément de la mesure, deux informations d'ajout sont passées avec elle : compte et MTU de saut. Le compte de saut est simplement le nombre de passerelles qu'un paquet devra intervenir pour obtenir à la destination. Le MTU est la taille de paquet maximale qui peut être envoyée le long du chemin entier sans fragmentation. (C'est-à-dire, c'est le minimum des mtu de tous les réseaux impliqués dans le chemin.)

Basé sur les informations métriques, « une mesure composée » simple est calculée pour le chemin. La mesure composée combine l'effet des divers composants métriques dans un numéro unique représentant la « qualité » de ce chemin. C'est la mesure composée qui est utilisée réellement pour décider du meilleur chemin.

Périodiquement chaque passerelle annonce sa table de routage entière (avec certains censurant en raison de la règle fendue d'horizon) à toutes les passerelles contiguës. Quand une passerelle obtient cette émission d'une autre passerelle, elle compare la table à sa table existante. Tous les nouveaux destinations et chemins sont ajoutés à la table de routage de la passerelle. Des chemins dans l'émission sont comparés aux chemins existants. Si un nouveau chemin est meilleur, il peut remplacer existant. Les informations dans l'émission sont également utilisées pour mettre à jour l'occupation de canal et d'autres informations sur les chemins existants. Cette procédure générale est semblable à cela utilisée par tous les protocoles de vecteur de distance. Il désigné dans la littérature mathématique sous le nom de l'algorithme Bellman-Ford. Référez-vous à RFC 1058 pour un développement détaillé de la procédure de base, qui décrit le RIP, un protocole plus ancien de vecteur de distance.

Dans l'IGRP, l'algorithme Bellman-Ford général est modifié dans trois aspects essentiels. D'abord, au lieu d'une mesure simple, un vecteur des mesures est utilisé pour caractériser des chemins. En second lieu, au lieu de sélectionner un chemin unique avec la plus petite mesure, le trafic est séparé parmi plusieurs chemins, dont les mesures tombent dans une plage spécifiée.

Troisièmement, plusieurs caractéristiques sont introduites pour fournir la stabilité dans les situations où la topologie change.

Le meilleur chemin est sélectionné a basé sur une mesure composée :

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

Là où K1, K2 = constantes, soyez = bande passante de chemin déchargée X (1 - occupation de canal), C.C = retard topologique, et r = fiabilité.

Le chemin ayant la plus petite mesure composée sera le meilleur chemin. Là où il y a des plusieurs chemins à la même destination, la passerelle peut conduire les paquets au-dessus de plus d'un chemin. Ceci est fait selon la mesure composée pour chaque chemin de données. Par exemple, si un chemin a une mesure composée de 1 et un autre chemin a une mesure composée de 3, trois fois autant de paquets seront envoyés au-dessus du chemin de données ayant la mesure composée de 1.

Il y a deux avantages à utiliser un vecteur des informations métriques. Le premier est qu'il fournit la capacité de prendre en charge des plusieurs types de service du même ensemble de données. Le deuxième avantage est précision améliorée. Quand une mesure simple est utilisée, elle est normalement traitée comme si c'étaient un retard. Chaque lien dans le chemin est ajouté à la métrique totale. S'il y a un lien avec une faible bande passante, elle est normalement représentée par un grand retard. Cependant, les limites de bande passante ne cumulent pas vraiment la manière que les retards font. En traitant la bande passante comme composant distinct, il peut être manipulé correctement. De même, le chargement peut être manipulé par un nombre distinct d'occupation de canal.

L'IGRP fournit un système pour l'interconnexion des réseaux informatiques qui peuvent stablement manipuler une topologie générale de graphique comprenant des boucles. Le système met à jour les informations métriques de chemin d'accès complet, c.-à-d., il connaît les paramètres de chemin à tous autres réseaux auxquels n'importe quelle passerelle est connectée. Le trafic peut être réparti sur des chemins parallèles et des paramètres de plusieurs chemins peuvent être simultanément calculés au-dessus du tout le réseau.

Comparaison avec le RIP

Cette section compare l'IGRP au RIP. Cette comparaison est utile parce que le RIP est utilisé largement pour des buts semblables à l'IGRP. Cependant, faire ceci n'est pas entièrement équitable. Le RIP n'a pas été destiné pour atteindre tous les mêmes buts que l'IGRP. Le RIP a été destiné pour l'usage dans de petits réseaux avec la technologie raisonnablement uniforme. Dans de telles applications il est généralement adéquat.

La différence la plus fondamentale entre l'IGRP et le RIP est la structure de leurs mesures. Malheureusement ce n'est pas une modification qui peut simplement être rattrapée POUR DÉCHIRER. Il exige les nouvelles structures d'algorithmes et de données actuelles dans l'IGRP.

Le RIP emploie une mesure simple « de compte de saut » pour décrire le réseau. À la différence de l'IGRP, où chaque chemin est décrit par un retard, une bande passante, etc., dans le RIP il est décrit par un nombre de 1 à 15. Normalement ce nombre est utilisé pour représenter combien de passerelles le chemin intervient avant d'obtenir à la destination. Ceci signifie qu'aucune distinction n'est faite entre une ligne série lente et un Ethernet. Dans quelques réalisations de RIP, il est possible que l'administrateur système spécifie qu'un saut donné devrait être compté plus d'une

fois. Des réseaux lents peuvent être représentés par un grand compte de saut. Mais puisque le maximum est 15, ceci ne peut pas être fait beaucoup. Par exemple si un Ethernet est représenté par 1 et une ligne 56Kb par 3, il peut y avoir tout au plus 5 lignes 56Kb dans un chemin, ou le maximum de 15 est dépassé. Afin de représenter la gamme complète de vitesses du réseau disponibles, et tenir compte d'un grand réseau, les études faites par Cisco suggèrent qu'une mesure 24-bit soit nécessaire. Si la mesure maximum est trop petite, l'administrateur système est présenté avec un choix désagréable : ou il ne peut pas distinguer les artères rapides et lentes, ou il ne peut pas s'insérer son réseau entier dans la limite. En fait un certain nombre de réseaux nationaux sont maintenant assez grands que le RIP ne peut pas les manipuler même si chaque saut est compté seulement une fois. Le RIP simplement ne peut pas être utilisé pour de tels réseaux.

La réponse évidente serait de modifier le RIP pour permettre une plus grande mesure. Malheureusement, ceci ne fonctionnera pas. Comme tous les protocoles de vecteur de distance, le RIP a le problème du « compte à l'infini ». Ceci est décrit plus en détail dans RFC 1058 . Quand la topologie change, de fausses artères seront introduites. Les mesures associées avec ces fausses artères augmentent lentement jusqu'à ce qu'elles atteignent 15, lesquels au point les artères sont retirées. 15 est un assez petit maximum que ce processus convergera assez rapidement, supposant que des mises à jour déclenchées sont utilisées. Si le RIP étaient modifiés pour permettre une mesure 24-bit, les boucles persisteraient assez longtemps pour que la mesure soit comptée jusqu'à 2**24. Ce n'est pas tolérable. L'IGRP a des caractéristiques conçues pour empêcher de fausses artères d'être introduit. Ceux-ci sont discutés ci-dessous dans la section 5.2. Il n'est pas pratique pour manipuler les réseaux complexes sans introduire de telles caractéristiques ou changer à un protocole tel que la SPF.

L'IGRP fait augmentent un peu plus que simplement la plage des mesures permises. Il restructure la mesure pour décrire le retard, la bande passante, la fiabilité, et le chargement. Il est possible de représenter de telles considérations dans une mesure simple telle que des déchirures cependant, l'approche adoptée par IGRP est potentiellement plus précis. Par exemple, avec une mesure simple, plusieurs liens rapides successifs sembleront être équivalents à un simple ralentissent un. Ceci peut être la caisse pour le trafic interactif, où le retard est la principale préoccupation. Cependant, pour le transfert des données en vrac, la principale préoccupation est bande passante, et ajouter des mesures n'est pas ensemble la bonne approche là. Les traitements IGRP retardent et bande passante séparément, cumulant des retards, mais prenant le minimum des bandes passantes. Il n'est pas facile de voir comment incorporer les effets de la fiabilité et du chargement à une métrique de composante unique.

Àmon avis, un des grands avantages de l'IGRP est facilité de configuration. Il peut directement représenter les quantités qui ont la signification physique. Ceci signifie qu'il peut être installé automatiquement, basé sur le type d'interface, vitesse linéaire, etc. Avec une métrique de composante unique, la mesure est pour devoir « être faite cuire » pour incorporer des effets de plusieurs différentes choses.

D'autres innovations sont plus une question des structures d'algorithmes et de données que du protocole de routage. Par exemple, l'IGRP spécifie les structures d'algorithmes et de données qui prennent en charge le partage du trafic parmi plusieurs artères. Il est certainement possible de concevoir une implémentation du RIP qui fait ceci. Cependant, une fois que l'acheminement re-est mis en application, il n'y a aucune raison de coller avec le RIP.

Jusqu'ici j'ai décrit « l'IGRP générique », une technologie qui pourrait prendre en charge le routage pour n'importe quel protocole réseau. Cependant, dans cette section il vaut de mentionner un peu plus au sujet de l'implémentation TCP/IP de particularité. C'est l'implémentation qui va être comparée au RIP.

Les messages de mise à jour de RIP contiennent simplement des instantanés de la table de routage. C'est-à-dire, ils ont un certain nombre de destinations et de valeurs métriques, et peu autrement. L'implémentation d'IP de l'IGRP a la structure supplémentaire. D'abord, le message de mise à jour est identifié par un « numéro de système autonome. » Cette terminologie sort de la tradition d'ARPANet, et a la signification spécifique là. Cependant, pour la plupart des réseaux ce que signifie il est que vous pouvez exploiter plusieurs différents systèmes de routage sur le même réseau. C'est utile pour des endroits où les réseaux de plusieurs organismes convergent. Chaque organisation peut mettre à jour son propre routage. Puisque chaque mise à jour est étiquetée, des passerelles peuvent être configurées pour prêter l'attention seulement à la droite. Certaines passerelles sont configurées pour recevoir des mises à jour de plusieurs Autonomous System. Ils passent les informations entre les systèmes d'une façon contrôlée. Notez que ce n'est pas une solution complète aux problèmes de la Sécurité de routage. N'importe quelle passerelle peut être configurée pour écouter des mises à jour de n'importe quel Autonomous System. Cependant, c'est toujours un outil très utile en mettant en application des stratégies de routage où est un degré raisonnable de confiance entre les administrateurs réseau.

La deuxième caractéristique structurelle au sujet des messages de mise à jour IGRP affecte la manière que des default route sont manipulés par IGRP. La plupart des protocoles de routage ont un concept de default route. Il n'est souvent pas pratique pour conduire des mises à jour pour répertorier chaque réseau dans le monde. Typiquement un ensemble du besoin de passerelles a détaillé les informations de routage pour des réseaux dans leur organisation. Tout le trafic pour des destinations en dehors de leur organisation peut être envoyé à une de quelques passerelles de périphérie. Ces passerelles de périphérie peuvent avoir plus d'informations complètes. L'artère à la meilleure passerelle de périphérie est un « default route ». C'est un par défaut dans le sens qu'il est utilisé pour obtenir à n'importe quelle destination qui n'est pas répertoriée spécifiquement dans les mises à jour internes de routage. Le RIP, et quelques autres protocoles de routage, distribuent des informations sur le default route comme si c'étaient un réseau réel. L'IGRP adopte une approche différente. Plutôt qu'une fausse entrée simple pour le default route, l'IGRP permet des réseaux réels à signaler comme candidats pour être un par défaut. Ceci est mis en application en plaçant des informations sur ces réseaux dans une section extérieure spéciale du message de mise à jour. Cependant, il pourrait considérer aussi bien en tant qu'activer un bit associé avec ces réseaux. Périodiquement l'IGRP balaye tous les default route de candidat et choisit celui avec la plus basse mesure comme default route réel.

Potentiellement cette approche aux par défaut est en quelque sorte plus souple que l'approche adoptée par la plupart des réalisations de RIP. Le plus typique des passerelles de RIP peuvent être placées pour générer un default route avec une certaine mesure spécifiée. L'intention est que ceci serait fait aux passerelles de périphérie.

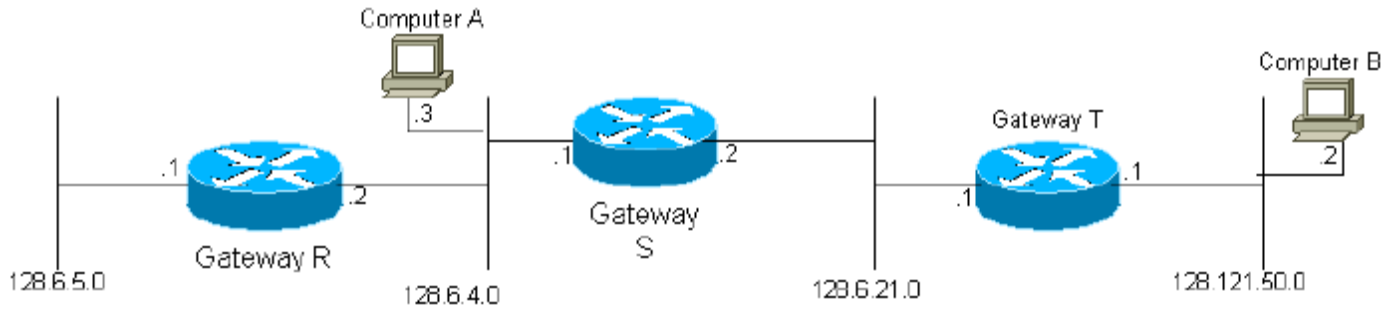
Description détaillée

Cette section fournit une description détaillée d'IGRP.

Description globale

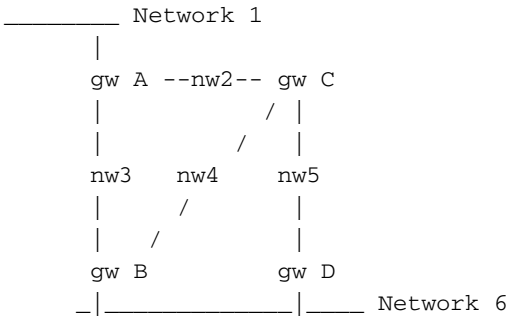
Quand une passerelle est d'abord activée, sa table de routage est initialisée. Ceci peut être fait par un opérateur d'une console, ou par les informations de lecture à partir des fichiers de configuration. Une description de chaque réseau connecté à la passerelle est fournie, y compris le retard topologique le long du lien (par exemple, combien de temps il faut à un à bit unique à transversal le lien) et de la bande passante du lien.

Figure 2



Par exemple, dans le diagramme ci-dessus, on dirait la passerelle S qu'elle est connectée aux réseaux 2 et 3 par l'intermédiaire des interfaces correspondantes. Ainsi, au commencement, la passerelle 2 sait seulement qu'elle peut atteindre n'importe quel ordinateur de destination dans les réseaux 2 et 3. Toutes les passerelles sont programmées pour transmettre périodiquement à leurs passerelles voisines les informations qu'elles ont été initialisées avec, aussi bien que des informations recueillies d'autres passerelles. Ainsi, la passerelle S recevrait des mises à jour des passerelles R et T et apprendrait qu'elle peut accéder des ordinateurs dans la passerelle traversante R du réseau 1 et des ordinateurs dans le réseau 4 par la passerelle T. Puisque la passerelle S envoie sa table de routage entière, dans la prochaine passerelle de cycle T apprendra qu'il peut obtenir au réseau 1 par la passerelle S. Il est facile de voir que les informations sur chaque réseau dans le système atteindront par la suite chaque passerelle dans le système, fournissant seulement que le réseau est entièrement connecté.

Figure 3



Chaque passerelle calcule une mesure composée pour déterminer l'avantage des chemins de données aux ordinateurs de destination. Par exemple, dans le diagramme au-dessus de, pour un réseau de destination in 6, passerelle A (le gw A) calculerait des fonctions métriques pour deux chemins, par l'intermédiaire des passerelles B et du C. Notez que des chemins sont définis simplement par le prochain saut. Il y a réellement trois artères possibles d'A au réseau 6 :

- Dirigez vers B
- Au C et puis à B
- Au C et puis à D

Cependant, la passerelle A n'a pas besoin de choisir entre les deux artères impliquant le C. La table de routage dans A a une seule entrée représentant le chemin au C. Sa mesure représente la meilleure manière d'obtenir du C à la destination définitive. Si A envoie un paquet au C, il appartient au C pour décider si utiliser B ou D.

Équation 1

La fonction métrique composée calculée pour chaque chemin de données est comme affichée ci-dessous :

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

Là où r = la fiabilité fractionnaire (% de transmissions qui sont avec succès reçues au prochain saut), C.C = délai composite, soit = bande passante réelle : bande passante déchargée X (1 - occupation de canal), et K1 et K2 = constantes.

Équation 2

En principe le délai composite, C.C, a pu être déterminé comme affiché ci-dessous :

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

Là où Ds = retard de commutation, Dcir = retard de circuit (délai de propagation de 1 bit), et décollement = retard de transmission (retard à vide pour un message de 1500 bits).

Cependant, dans la pratique une valeur de délai standard est utilisée pour chaque type de technologie de réseau. Par exemple, il y aura une valeur de délai standard pour des Ethernets, et pour des lignes série à n'importe quel débit binaire particulier.

Voici un exemple de la façon dont la table de routage de la passerelle A pourrait regarder dans le cas du diagramme du réseau 6 ci-dessus. (Note que des composants individuels du vecteur métrique ne sont pas affichés, pour la simplicité.)

Exemple de Tableau de routage :

Réseau	Interface	Prochaine passerelle	Mesure
1	Nanowatt 1	Aucun	Directement connecté
2	Nanowatt 2	Aucun	Directement connecté
3	Nanowatt 3	Aucun	Directement connecté
4	Nanowatt 2	C	1270
	Nanowatt 3	B	1180
5	Nanowatt 2	C	1270
	Nanowatt 3	B	2130
6	Nanowatt 2	C	2040
	Nanowatt 3	B	1180

L'opération de base d'accumuler une table de routage en permutant les informations avec des voisins est décrite par l'algorithme Bellman-Ford. L'algorithme a été utilisé dans des protocoles plus tôt tels que le RIP (RFC 1058). Afin de traiter des réseaux plus complexes, l'IGRP ajoute trois caractéristiques à l'algorithme Bellman-Ford de base :

1. Au lieu d'une mesure simple, un vecteur des mesures est utilisé pour caractériser des chemins. Une mesure composée simple peut être calculée de ce vecteur selon l'équation 1,

en haut. L'utilisation d'un vecteur permet à la passerelle pour faciliter différents types de service, à l'aide de plusieurs différents coefficients dans l'équation 1. Il permet également une représentation plus précise des caractéristiques du réseau qu'une mesure simple.
2. Au lieu de sélectionner un chemin unique avec la plus petite mesure, le trafic est séparé parmi plusieurs chemins avec des mesures tombant dans une plage spécifiée. Ceci permet plusieurs artères à utiliser en parallèle, fournissant une plus grande bande passante réelle que n'importe quelle artère simple. Une variance V est spécifiée par l'administrateur réseau. Tous les chemins avec la mesure composée minimale M sont gardés. En outre, tous les chemins dont la mesure est moins que V x M sont gardés. Le trafic est distribué parmi des plusieurs chemins dans la proportion inverse avec les mesures composées.
3. Il y a quelques problèmes avec ce concept de variance. Il est difficile de proposer les stratégies qui se servent des valeurs de variance plus grandes que 1, et ne mène pas également aux paquets le bouclage. Dans la version 8.2 de Cisco, la caractéristique de variance n'est pas mise en application. (Je ne suis pas sûr dans quelle release la caractéristique a été retirée.) L'effet de ceci est de placer la variance de manière permanente à 1.
4. Plusieurs caractéristiques sont introduites pour fournir la stabilité dans les situations où la topologie change. Ces caractéristiques sont destinées pour empêcher les boucles de routage et le « compte à l'infini, » qui ont caractérisé des précédentes tentatives d'utiliser des algorithmes de Ford-type pour ce type d'application. Les fonctions de stabilité primaires sont des « holddowns », « les mises à jour déclenchées », le « horizon de fractionnement, » et « empoisonnant ». Ceux-ci seront discutés plus en détail ci-dessous.

Séparer du trafic (le point 2) soulève un danger plutôt subtil. La variance V est conçue pour permettre à des passerelles pour utiliser des chemins parallèles de différentes vitesses. Par exemple, il pourrait y a des 9600 bps que la ligne exécution parallèlement à des 19200 bps rayent, pour la Redondance. Si la variance V est 1, seulement le meilleur chemin sera utilisé. Ainsi les 9600 bps de ligne ne seront pas utilisées si les 19200 bps de ligne a une fiabilité raisonnable. (Cependant, si plusieurs chemins sont identiques, le chargement sera partagé parmi eux.) En soulevant la variance, nous pouvons permettre le trafic à séparer entre la meilleure route et d'autres artères qui sont presque comme bons. Avec une assez grande variance, le trafic sera séparé entre les deux lignes. Le danger est celui avec une assez grande variance, les chemins deviennent laissé qui ne sont pas simplement plus lents, mais sont réellement « dans la mauvaise direction ». Ainsi il devrait y a une règle supplémentaire d'empêcher le trafic d'être envoyé à « en amont » : Aucun trafic n'est envoyé le long des chemins dont la mesure composée distante (la mesure composée calculée au prochain saut) est plus grande que la mesure composée calculée à la passerelle. En général des administrateurs système sont encouragés à ne pas placer la variance au-dessus de 1 excepté dans des situations spécifiques où des chemins parallèles doivent être utilisés. Dans ce cas, la variance est soigneusement placée pour fournir les « bons » résultats.

L'IGRP est destiné pour manipuler de plusieurs « types de service, » et plusieurs protocoles. Le type de service est une spécification dans un paquet de données qui modifie la manière que des chemins doivent pour être évaluée. Par exemple, le protocole TCP/IP permet au paquet pour spécifier l'importance relative de la bande passante élevée, du bas retard, ou de la grande fiabilité. Généralement, les applications interactives spécifieront le bas retard, tandis que les applications de transfert en masse spécifieront la bande passante élevée. Ces conditions requises déterminent les valeurs relatives de K1 et de K2 qui sont appropriés pour l'usage dans l'eq. 1. Chaque combinaison des caractéristiques dans le paquet qui doit être pris en charge est mentionnée pendant qu'un « type de service ». Pour chaque type de service, un ensemble de paramètres K1 et K2 doivent être choisis. Une table de routage est gardée pour chaque type de service. Ceci est

fait parce que des chemins sont sélectionnés et commandés selon la mesure composée définie par eq. 1. C'est différent pour chaque type de service. Les informations de toutes ces tables de routage sont combinées pour produire les messages de mise à jour de routage permutés par les passerelles, comme décrit dans la figure 7.

Fonctions de stabilité

Cette section décrit des holddowns, des mises à jour déclenchées, l'horizon fendu, et l'empoisonnement. Ces caractéristiques sont conçues pour empêcher des passerelles de sélectionner des routes incorrectes. Comme décrit dans RFC 1058 , ceci peut se produire quand une artère devient inutilisable, due à la panne d'une passerelle ou d'un réseau. En principe, les passerelles contiguës détectent des pannes. Ils envoient alors les mises à jour de routage qui affichent la vieille artère comme inutilisable. Cependant, il est possible que des mises à jour de ne pas atteindre quelques parties du réseau du tout, ou soient retardées en atteignant certaines passerelles. Une passerelle qui croit toujours que la vieille artère est bonne peut continuer de se propager ces informations, de ce fait ressaisissant la route défaillante dans le système. Par la suite ces informations propageront par le réseau et seront livré de retour à la passerelle qui l'a réinjecté. Le résultat est une artère circulaire.

En fait il y a une certaine Redondance parmi les contre-mesures. En principe, les holddowns et les mises à jour déclenchées devraient être suffisants pour empêcher des routes incorrectes en premier lieu. Cependant, dans la pratique, les pannes de communications de diverses sortes peuvent les faire être soient insuffisantes. L'empoisonnement fendu d'horizon et d'artère sont destinés pour empêcher des boucles de routage en tous cas.

Normalement, de nouvelles tables de routage sont envoyées aux passerelles voisines de façon régulière (toutes les 90 secondes par défaut, bien que ceci puisse être ajusté par l'administrateur système). Une mise à jour déclenchée est une nouvelle table de routage qui est envoyée immédiatement, en réponse à une certaine modification. La modification la plus importante est suppression d'une artère. Ceci peut se produire parce qu'un délai d'attente a expiré (probablement une passerelle ou une ligne voisine est descendue), ou parce qu'un message de mise à jour de la prochaine passerelle dans le chemin prouve que le chemin n'est plus utilisable. Quand une passerelle G la détecte qu'une artère n'est plus utilisable, elle déclenche une mise à jour immédiatement. Cette mise à jour affichera cette artère comme inutilisable. Considérez ce qui se produit quand cette mise à jour atteint les passerelles voisines. Si l'artère du voisin redésignait G, le voisin doit retirer l'artère. Ceci fait déclencher le voisin une mise à jour, etc. Ainsi une panne déclenchera une vague de messages de mise à jour. Cette onde propagera dans toute cette partie du réseau dans lequel les artères sont passées par la passerelle ou le réseau défectueuse.

Les mises à jour déclenchées seraient suffisantes si nous pourrions garantir que l'onde des mises à jour a atteint chaque passerelle appropriée immédiatement. Cependant, il y a deux problèmes. D'abord, des paquets contenant le message de mise à jour peuvent être lâchés ou corrompus par un certain lien dans le réseau. En second lieu, les mises à jour déclenchées ne se produisent pas instantanément. Il est possible qu'une passerelle qui n'a pas encore la mise à jour déclenchée émettra une mise à jour régulière juste au mauvais moment, causant la mauvaise artère d'être réinsérée dans un voisin qui a déjà eu la mise à jour déclenchée. Des holddowns sont conçus pour venir à bout ces problèmes. La règle de holddown indique que quand une artère est retirée, aucune nouvelle route ne sera reçue pour la même destination pour une certaine période. Ceci donne aux mises à jour déclenchées l'heure d'obtenir à toutes autres passerelles, de sorte que nous puissions être sûrs qu'aucune nouvelle route que nous obtenons ne sont pas simplement une certaine passerelle réinsérant le vieil. La période de holddown doit être assez longue pour tenir compte de l'onde des mises à jour déclenchées pour aller dans tout le réseau. En outre, il

devrait inclure quelques cycles réguliers d'émission, pour manipuler les paquets relâchés. Considérez ce qui se produit si une des mises à jour déclenchées est relâchée ou corrompue. La passerelle qui a émis cette mise à jour émettra une autre mise à jour à la prochaine mise à jour régulière. Ceci redémarrera l'onde des mises à jour déclenchées aux voisins qui ont manqué l'onde initiale.

La combinaison des mises à jour et des holddowns déclenchés devrait être suffisante pour se débarasser des artères expirées et pour les empêcher d'être réinséré. Cependant, quelques précautions supplémentaires valent de faire de toute façon. Ils tiennent compte très des réseaux lossy, et des réseaux qui sont devenus divisés. Les précautions supplémentaires nécessitées par l'IGRP sont empoisonnement fendu d'horizon et d'artère. L'horizon fendu résulte de l'observation qu'il ne se comprend jamais de renvoyer une artère dans la direction de laquelle il a été livré. Considérez la situation suivante :

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

La passerelle A indiquera à B qu'elle a une artère au réseau 1. Quand B envoie des mises à jour à A, il n'y a jamais n'importe quelle raison pour qu'elle mentionne le réseau 1. Puisqu'A est plus près de 1, il n'y a aucune raison pour qu'elle envisage d'aller par l'intermédiaire du B. La règle fendue d'horizon indique qu'un message distinct de mise à jour devrait être généré pour chaque voisin (réellement chaque réseau voisin). La mise à jour pour un voisin donné devrait omettre les artères qui indiquent ce voisin. Cette règle empêche des boucles entre les passerelles contiguës. Par exemple supposez que l'interface d'A au réseau 1 échoue. Sans règle fendue d'horizon, B serait disant à A qu'il peut obtenir à 1. Puisqu'il n'a plus une vraie artère, A pourrait prendre cette artère. Dans ce cas, A et B chacun des deux auraient des artères à 1. Mais A indiquerait B et B indiquerait les mises à jour déclenchées A. naturellement et les holddowns devraient empêcher ceci de se produire. Mais puisqu'il n'y a aucune raison d'envoyer les informations de nouveau à l'endroit qu'elles sont provenu, l'horizon fendu vaut de faire de toute façon. En plus de son rôle en empêchant des boucles, l'horizon fendu réduit la taille des messages de mise à jour.

L'horizon fendu devrait empêcher des boucles entre les passerelles contiguës. L'empoisonnement d'artère est destiné pour casser de plus grandes boucles. La règle est que quand une mise à jour affiche que la mesure pour une route existante augmentait suffisamment, il y a une boucle. L'artère devrait être retirée et mise dans le holddown. Actuellement la règle est qu'une artère est retirée si la mesure composée augmente plus qu'un facteur de 1.1. Il n'est pas sûr que juste aucune augmentation de la mesure composée ne déclenche la suppression de l'artère, puisque les petites modifications métriques peuvent se produire en raison des changements d'occupation ou de fiabilité de canal. Ainsi le facteur de 1.1 est juste un heuristique. La valeur précise n'est pas essentielle. Nous nous attendons à cette règle d'être nécessaire seulement pour casser les boucles très grandes, puisque les petites seront empêchées par les mises à jour et les holddowns déclenchés.

Holddowns de débronchement

En date de la version 8.2, le code de Cisco fournit une option de désactiver des holddowns. L'inconvénient des holddowns est qu'ils retardent l'adoption d'une nouvelle route quand une vieille artère échoue. Avec des paramètres par défaut, il peut prendre plusieurs minutes avant qu'un routeur adopte une nouvelle route après une modification. Cependant, parce que les raisons expliquées ci-dessus, il n'est pas sûr simplement de retirer des holddowns. Le résultat serait comptage à l'infini, comme décrit dans RFC 1058. Nous conjecturons, mais ne pouvons pas s'avérer, cela avec une version plus forte de l'empoisonnement d'artère, des holddowns ne

sommes nécessaires plus pour arrêter le comptage à l'infini. De ce fait désactiver des holddowns active cette forme plus forte de l'empoisonnement d'artère. Notez cet horizon fendu et les mises à jour déclenchées sont toujours en effet.

La forme plus forte de l'empoisonnement d'artère est basée sur un compte de saut. Si le compte de saut pour un chemin augmente, l'artère est retirée. Ceci retirera évidemment les artères qui sont encore valides. Si quelque chose ailleurs dans le réseau change de sorte que le chemin passe maintenant par une plus de passerelle, le compte de saut augmentera. Dans ce cas, l'artère est encore valide. Cependant, il n'y a aucune manière complètement sûre de distinguer ce cas des boucles de routage (comptage à l'infini). Ainsi l'approche la plus sûre est de retirer l'artère toutes les fois que le compte de saut augmente. Si l'artère est encore légitime, elle sera réinstallée par la prochaine mise à jour, et cela entraînera une mise à jour déclenchée qui réinstallera l'artère ailleurs dans le système.

Généralement le vecteur de distance algorithms1 adoptent des nouvelles routes facilement. Le problème purge complètement les vieux du système. Ainsi une règle qui est terminée agressive au sujet de retirer les artères méfiantes devrait être sûre.

Détails du processus de mise à jour

L'ensemble de processus décrits dans les figures 4 à 8 sont destinés pour manipuler un protocole de réseau simple, par exemple, le TCP/IP, le DECNet, ou le protocole ISO/OSI. Cependant, des détails de protocole seront fournis seulement pour le TCP/IP. Une passerelle simple peut traiter les données qui suivent plus d'un protocole. Puisque chaque protocole a différents structures d'adressage et formats de paquet, le code machine utilisé pour mettre en application des figures 4 à 8 sera généralement différent pour chaque protocole. Le processus décrit dans la figure 4 variera les la plupart, comme décrit dans les notes détaillées pour la figure 4. Les processus décrits dans la figure 5 à 8 auront la même structure générale. La différence principale du protocole au protocole sera le format du paquet de mise à jour de routage, qui doit être conçu pour être compatible avec un protocole spécifique.

Notez que la définition d'une destination peut varier du protocole au protocole. La méthode décrite ici peut être utilisée pour conduire à différents hôtes, aux réseaux, ou pour des schémas hiérarchiques plus complexes d'adresse. Quel type de routage est utilisé dépendra de la structure d'adressage du protocole. L'implémentation TCP/IP de courant prend en charge seulement l'acheminement aux réseaux IP. Ainsi la « destination » signifie vraiment le réseau IP ou le numéro de sous-réseau. L'information de sous-réseau est seulement gardée pour des réseaux connectés.

Figures 4 au pseudo-code de 7 expositions pour différentes parties du processus de routage utilisé par les passerelles. Au début du programme, des protocoles acceptables et les paramètres décrivant chaque interface sont entrés.

La passerelle manipulera seulement certains protocoles qui sont répertoriés. N'importe quelle transmission d'un système utilisant un protocole pas relatif à la liste sera ignorée. Les entrées de données sont les suivantes :

- Réseaux auxquels la passerelle est connectée.
- Bande passante déchargée de chaque réseau.
- Retard topologique de chaque réseau.
- Fiabilité de chaque réseau.
- Occupation de la Manche de chaque réseau.

- MTU de chaque réseau.

La fonction métrique pour chaque chemin de données est alors calculée selon l'équation 1. Notez que les trois premiers éléments sont raisonnablement permanents. Ils sont une fonction de la technologie de réseau sous-jacente, et ne dépendent pas du chargement. Ils ont pu être placés à partir d'un fichier de configuration ou par la saisie par un opérateur directe. Notez que l'IGRP n'utilise pas le retard mesuré. La théorie et l'expérience suggèrent qu'il soit très difficile pour les protocoles qui emploient le retard mesuré pour mettre à jour le routage stable. Il y a deux paramètres mesurés : occupation de fiabilité et de canal. La fiabilité est basée sur des taux d'erreur signalés par le matériel ou le micrologiciel d'interface réseau.

En outre ces entrées, l'algorithme de routage exige une valeur pour plusieurs paramètres de routage. Ceci inclut des valeurs de temporisateur, variance, et si des holddowns sont activés. Ceci serait normalement spécifié par un fichier de configuration ou une saisie par un opérateur. (En date de la version 8.2 de Cisco, la variance est de manière permanente placée à 1.)

Les informations une fois initiales sont écrites, des exécutions dans la passerelle sont déclenchées par des événements — l'arrivée d'un paquet de données à une des interfaces réseau, ou expiration d'un temporisateur. Les processus décrits dans les figures 4 à 7 sont déclenchés comme suit :

- Quand un paquet arrive, il est traité selon la figure 4. Ceci a comme conséquence le paquet étant envoyé une autre interface, jeté, ou reçu pour une transformation plus ultérieure.
- Quand un paquet est reçu par la passerelle pour une transformation plus ultérieure, il est analysé d'une mode de Protocol-particularité non décrite dans cette spécification. Si le paquet est une mise à jour de routage, il est traité selon la figure 5.
- La figure 6 affiche des événements déclenchés par un temporisateur. Le temporisateur est placé pour générer une interruption une fois par seconde. Quand l'interruption se produit, on exécute le processus affiché dans la figure 6.
- La figure 7 affiche une sous-routine de mise à jour de routage. Des appels à cette sous-routine sont affichés dans les figures 5 et 6.
- En outre, la figure 8 affiche des détails des calculs métriques visés dans les figures 5 et 7.

Il y a quatre constantes de temps essentielles qui propagation et expiration d'artère de contrôle. Ces constantes de temps peuvent être placées par l'administrateur système. Cependant, il y a des valeurs par défaut. Ces constantes de temps sont :

- Durée de diffusion — Les mises à jour sont émission par toutes les passerelles sur le tout connecté relie ceci souvent. Le par défaut est une fois toutes les 90 secondes.
- Heure non valide — Si aucune mise à jour n'a été reçue pour un chemin donné dans cette durée, elle est considérée comme pour avoir chronométré. Il devrait être plusieurs temps la durée de diffusion, afin de tenir compte de la possibilité que des paquets contenant une mise à jour pourraient être lâchés par le réseau. Le par défaut est 3 fois la durée de diffusion.
- Durée d'attente — Quand une destination est devenue inaccessible (ou la mesure a augmenté assez pour entraîner l'empoisonnement), la destination entre dans le « holddown ». Pendant cet état, aucun nouveau chemin ne sera reçu pour la même destination pour cette durée. La durée d'attente indique combien de temps cet état durer. Il devrait être plusieurs temps la durée de diffusion. La valeur par défaut est 3 fois la durée de diffusion plus 10 secondes. (Comme décrit dans la section de holddowns de débronchement, il est possible de désactiver des holddowns.)
- Temps affleurant — Si aucune mise à jour n'a été reçue pour une destination donnée dans cette durée, l'entrée pour elle est retirée de la table de routage. Notez la différence entre

l'heure non valide et le moment affleurant : Après l'heure non valide un chemin est chronométré et retiré. S'il n'y a aucun chemin restant à une destination, la destination est maintenant inaccessible. Cependant, l'entrée de base de données pour la destination demeure. Il doit rester pour imposer le holddown. Après le temps affleurant, l'entrée de base de données est retirée de la table. Il devrait être en quelque sorte plus long que l'heure non valide plus le temps de gel. Le par défaut est 7 fois la durée de diffusion.

Ces figures présupposent les principales structures de données suivantes. Un ensemble distinct de ces structures de données est gardé pour chaque protocole pris en charge par la passerelle. Dans chaque protocole, des ensembles de structures de données distincts est gardés pour chaque type de service à prendre en charge.

Pour chaque destination connue du système, il y a liste a (probablement nul) de chemins à la destination, à un temps d'expiration de holddown, et à un temps de dernière modification. La périodicité de dernière modification indique que la dernière fois n'importe quel chemin pour cette destination a été inclus dans une mise à jour d'une autre passerelle. Notez qu'il y a également des minuteurs de mise à jour gardés pour chaque chemin. Quand le dernier chemin à une destination est retiré, la destination est mise dans le holddown, à moins que des holddowns soient désactivés (voyez le pour en savoir plus de section de holddowns de débronchement). Le temps d'expiration de holddown indique le temps à l'où le holddown expire. Le fait qu'il est différent de zéro indique que la destination est dans le holddown. Afin d'épargner le temps de calcul, c'est également une bonne idée de garder une « meilleure mesure » pour chaque destination. C'est simplement le minimum des mesures composées pour tous les chemins à la destination.

Pour chaque chemin à une destination, il y a l'adresse du prochain saut dans le chemin, l'interface à utiliser, un vecteur des mesures caractérisant le chemin, y compris le retard, la bande passante, la fiabilité, et l'occupation de canal topologiques. D'autres informations sont également associées avec chaque chemin, y compris le compte de saut, le MTU, la source d'informations, la mesure composée distante, et une mesure composée calculée à partir de ces nombres selon l'équation 1. Il y a également un temps de dernière modification. La source d'informations indique où la mise à jour la plus récente pour ce chemin est provenue. Dans la pratique c'est identique que l'adresse du prochain saut. La périodicité de dernière modification est simplement le temps à l'où la mise à jour la plus récente est arrivée pour ce chemin. Il est utilisé pour expirer les chemins synchronisés-.

Notez qu'un message de mise à jour IGRP a trois parties : interne, système (signification « ces Autonomous System » mais non intérieur), et extérieur. La section intérieure est pour des artères aux sous-réseaux. Non toute l'information de sous-réseau est incluse. Seulement des sous-réseaux d'un réseau sont inclus. C'est le réseau associé avec l'adresse à laquelle la mise à jour est envoyée. Normalement les mises à jour sont émission sur chaque interface, ainsi c'est simplement le réseau sur lequel l'émission est envoyée. (D'autres cas se présentent pour des réponses à une demande IGRP et à un IGRP point par point.) Des réseaux importants (par exemple, des non-sous-réseaux) sont mis dans la partie de système du message de mise à jour à moins qu'ils soient spécifiquement signalés en tant qu'extérieur.

Un réseau sera signalé comme extérieur si on l'apprenait d'une autre passerelle et les informations arrivaient dans la partie extérieure du message de mise à jour. L'implémentation de Cisco permet également à l'administrateur système pour déclarer les réseaux spécifiques en tant qu'extérieur. Des routes extérieures désigné également sous le nom du « candidat par défaut ». Ils sont des artères aux lesquelles passez ou par les passerelles qui sont considérées appropriées comme par défaut, à utiliser quand il n'y a aucune route explicite à une destination. Par exemple chez Rutgers nous configurons la passerelle qui connecte Rutgers à notre réseau régional de sorte qu'il signale l'artère au circuit principal de NSFnet en tant qu'extérieur. L'implémentation de

Cisco choisit un default route en sélectionnant cette route extérieure avec la plus petite mesure.

Les sections suivantes sont destinées pour clarifier des certaine parties de figures 4 à 8.

Acheminement par paquets

La figure 4 décrit le traitement de combinaison des paquets en entrée. Ceci est utilisé simplement pour clarifier la terminologie. Évidemment ce n'est pas une description complète de quelle passerelle IP fait.

Ce processus utilise la liste de protocoles pris en charge et les informations sur les interfaces sont entrées quand la passerelle est initialisée. Les détails du traitement de paquets dépendent du protocole utilisé par le paquet. Ceci est déterminé dans l'étape A. Step A est la seule partie de la figure 4 qui est partagée par tous les protocoles. Une fois que le type de protocole est connu, l'implémentation de la figure 4 appropriée au type de protocole est utilisée. Des détails du contenu de paquet sont décrits par les caractéristiques du protocole. Les caractéristiques d'un protocole incluent une procédure pour déterminer la destination d'un paquet, une procédure pour comparer la destination aux propres adresses de la passerelle pour déterminer si la passerelle elle-même est la destination, une procédure pour déterminer si un paquet est une émission, et une procédure pour déterminer si la destination fait partie d'un réseau spécifié. Ces procédures sont utilisées dans les étapes B et le C de la figure 4. Le test dans l'étape D exige une recherche des destinations répertoriées dans la table de routage. Le test est satisfait s'il y a une entrée dans la table de routage pour la destination, et cette destination a associé avec elle au moins un chemin utilisable. Notez que la destination et les données de chemin utilisées en cela et l'étape suivante sont mises à jour séparément pour chaque type de service pris en charge. Ainsi cette étape commence en déterminant le type de service spécifié par le paquet, et en sélectionnant les ensembles de structures de données correspondants pour utiliser pour ceci et l'étape suivante.

Un chemin est utilisable aux fins des étapes D et E si sa mesure composée distante est inférieure sa mesure composée. Un chemin dont la mesure composée distante est plus grande que sa mesure composée est un chemin dont le prochain saut est « plus loin parti » de la destination, comme mesuré par la mesure. Ceci désigné sous le nom d'un « chemin ascendant. » Normalement un prévoirait que l'utilisation des mesures empêcherait des chemins ascendants d'être choisi. Il est facile de voir qu'un chemin ascendant peut ne jamais être le meilleur. Cependant, si on permet une grande variance, des chemins autres que les meilleurs peuvent être utilisés. Certaines de ceux ont pu être en amont.

L'étape E calcule le chemin pour l'utiliser. Des chemins dont la mesure composée distante n'est pas moins que leurs mesures composées ne sont pas considérés. Si plus d'un chemin est acceptable, de tels chemins sont utilisés sous une forme pesée de l'alternance circulaire. La fréquence avec laquelle un chemin est utilisé est inversement proportionnelle à sa mesure composée.

Réception des mises à jour de routage

La figure 5 décrit le traitement d'une mise à jour reçue de routage d'une passerelle voisine. De telles mises à jour se composent d'une liste d'entrées, qui fournit les informations pour une destination simple. Plus d'une entrée pour la même destination peut se produire dans une mise à jour simple de routage, pour faciliter des plusieurs types de service. Chacune de ces entrées est traitée individuellement, comme décrit dans la figure 5. Si une entrée est dans la section extérieure de la mise à jour, l'indicateur extérieur sera placé pour la destination si on l'ajoute en raison de ce processus.

Le processus entier décrit dans la figure 5 doit être répété une fois pour chaque type de service pris en charge par la passerelle, utilisant l'ensemble d'informations de destination/chemin associées avec ce type de service. Ceci est affiché dans la boucle extérieure dans la figure 5. La mise à jour entière de routage doit être traitée une fois pour chaque type de service. (La note que l'implémentation d'IGRP en cours ne prend en charge pas les plusieurs types de service ainsi la boucle extérieure n'est pas mise en application réellement.)

Dans l'étape A, des tests de base d'acceptabilité sont faits sur le chemin. Ceci devrait inclure des tests de caractère raisonnable pour la destination. (« Martien ») des network number impossibles devraient être rejetés. (Référez-vous au pour en savoir plus RFC 1009 et RFC 1122.) Des mises à jour sont également rejetées si la destination qu'ils se réfèrent est dans le holddown, c.-à-d. le temps d'expiration de holddown est différent de zéro et plus tard que le temps en cours.

Dans l'étape B la table de routage est recherchée pour voir si cette entrée décrit un chemin qui est déjà connu. Un chemin dans la table de routage est défini par la destination avec laquelle elle est associée, le prochain saut répertorié en tant qu'élément du chemin, l'interface de sortie à utiliser pour le chemin, et la source d'informations (l'adresse de laquelle la mise à jour a été livré — dans la pratique normalement la même que le prochain saut). L'entrée du paquet de mise à jour décrit un chemin dont la destination est répertoriée dans l'entrée, dont l'interface de sortie est l'interface que la mise à jour est entrée, et dont prochains saut et source d'informations sont l'adresse de la passerelle qui a envoyé la mise à jour (la « source » S).

Dans l'étape H et l'étape T, le processus de mise à jour décrit dans la figure 7 est programmé. Ce processus fonctionnera réellement après le processus entier décrit dans la figure 5 est de finition. C'est-à-dire, le processus de mise à jour décrit dans la figure 7 se produira seulement une fois, même si il est déclenché plusieurs fois pendant le traitement décrit dans la figure 5. En outre, des précautions doivent être prises pour garder des mises à jour d'être émis trop souvent, si le réseau change rapidement.

L'étape K est faite si la destination décrite par l'entrée en cours dans le paquet de mise à jour existe déjà dans la table de routage. K compare la nouvelle mesure composée calculée des données dans le paquet de mise à jour à la meilleure mesure composée pour la destination. Notez que la meilleure mesure composée re-n'est pas calculée à ce moment, ainsi, si le chemin étant considéré est déjà dans la table de routage, ce test peut comparer de nouvelles et vieilles mesures pour le même chemin.

L'étape L est exécutée pour les chemins qui sont plus mauvais que la meilleure mesure composée existante. Ceci inclut les nouveaux chemins qui sont plus mauvais que celles existantes et les chemins existants dont la mesure composée a augmenté. L'étape L teste si le nouveau chemin est acceptable. Notez que ceci introduit de façon expérimentale chacun des deux le test pour s'il est assez bon garder un nouveau chemin, et conduit l'empoisonnement. Afin d'être acceptable, la valeur de retard ne doit pas être la valeur spéciale qui indique une destination inaccessible (pour l'implémentation d'IP en cours, toute la dans des 24 domaines de bit), et la mesure composée (calculée comme spécifiée sur le schéma 8) doit être acceptable. Pour déterminer si la mesure composée est acceptable, comparez-la aux mesures composées de tous autres chemins à la destination. Permettez M d'être le minimum de ces derniers. Le nouveau chemin est acceptable s'il est < V x M, OÙ V EST LA VARIANCE RÉGLÉE QUAND LA PASSERELLE A ÉTÉ INITIALISÉE. SI V = 1 (QUI EST TOUJOURS VRAI EN DATE DE LA VERSION 8.2 DE CISCO), ALORS UNE MESURE PLUS MAUVAISE QU'EXISTANTE N'EST PAS ACCEPTABLE. IL Y A UNE EXCEPTION À CECI : SI LE CHEMIN DÉJÀ EXISTE ET EST LE SEUL CHEMIN À LA DESTINATION, LE CHEMIN SERA RETENU SI LA MESURE N'A PAS AUGMENTÉ PAR PLUS DE 10% (OU OÙ DES HOLDDOWNS SONT DÉSACTIVÉS, SI LE COMPTE DE SAUT N'A PAS AUGMENTÉ).

Étape V est faite quand les nouvelles informations pour un chemin indiquent que la mesure composée sera diminuée. Les mesures composées de tous les chemins à la destination D sont comparées. Dans cette comparaison, la nouvelle mesure composée pour P est utilisée, plutôt que celui apparaissant dans la table de routage. La mesure composée minimum M est calculée. Alors tous les chemins à D sont examinés de nouveau. Si la mesure composée pour n'importe quels chemin > M x V, ce chemin est retirée. V est la variance, écrite quand la passerelle a été initialisée. (En date de la version 8.2 de Cisco, la variance est de manière permanente placée à 1.)

Traitement périodique

Le processus décrit dans la figure 6 est déclenché une fois une seconde. Il examine de divers temporisateurs dans la table de routage, pour voir si en a expiré. Ces temporisateurs sont décrits ci-dessus.

Dans l'étape U, le processus décrit dans la figure 7 est lancé.

L'étape R et l'étape S sont nécessaires parce que les mesures composées enregistrées dans la table de routage dépendent de l'occupation de canal, qui des modifications au fil du temps, basée sur des mesures. Périodiquement l'occupation de canal est recalculée, utilisant une moyenne mobile du trafic mesuré par l'interface. Si la valeur nouveau-calculée diffère de existante, toutes les mesures composées impliquant cette interface doivent être ajustées. Chaque chemin affiché dans la table de routage est examiné. N'importe quel chemin dont le prochain saut utilise l'interface « je » a sa mesure composée recalculée. Ceci est fait selon l'équation 1, utilisant comme occupation de canal le maximum de la valeur entreposé dans la table de routage en tant qu'élément de la mesure du chemin, et l'occupation de canal nouvellement calculée de l'interface.

Générez les messages de mise à jour

La figure 7 décrit comment la passerelle génère des messages de mise à jour à envoyer à d'autres passerelles. Un message indépendant est généré pour chaque interface réseau reliée à la passerelle. Ce message est alors envoyé à toutes autres passerelles qui sont accessibles par l'interface (étape J). Généralement ceci est fait en envoyant le message comme émission. Cependant, si la technologie de réseau ou le protocole ne permet pas des émissions, il peut être nécessaire d'envoyer le message individuellement à chaque passerelle.

Généralement le message est accumulé en ajoutant une entrée pour chaque destination in la table de routage, dans l'étape G. Notez que la destination/données de chemin associées avec chaque type de service doit être utilisée. Dans le pire des cas, une nouvelle entrée est ajoutée à la mise à jour pour chaque destination pour chaque type de service. Cependant, avant d'ajouter une entrée au message de mise à jour dans l'étape G, les entrées déjà ajoutées sont balayées. Si la nouvelle entrée est déjà présente dans le message de mise à jour, on ne l'ajoute pas de nouveau. Une nouvelle entrée reproduit existant quand les destinations et les prochaines passerelles de saut sont identiques.

Dans l'intérêt de la simplicité, le pseudo-code omet une chose — les messages de mise à jour IGRP ont trois parts : l'interne, le système, et l'extérieur, ainsi lui veut dire qu'il y a réellement trois boucles au-dessus des destinations. Le premier inclut seulement des sous-réseaux du réseau auquel la mise à jour est envoyée. Le deuxième inclut tous les réseaux importants (par exemple, des non-sous-réseaux) qui ne sont pas signalés en tant qu'extérieur. Le tiers inclut tous les réseaux importants qui sont signalés en tant qu'extérieur.

L'étape E implémente le test fendu d'horizon. Dans le cas normal, ce test échoue pour les artères dont le meilleur chemin sort la même interface que la mise à jour est envoyée. Cependant, si la mise à jour est envoyée à une destination spécifique (par exemple, en réponse à une demande IGRP d'une autre passerelle, ou en tant qu'élément « d'IGRP point par point »), l'horizon fendu échoue seulement si le meilleur chemin provenait initialement que la destination (sa « source d'informations » est identique que la destination) et son interface de sortie est identique dont celle la demande est entrée.

Les informations métriques de calcul

La figure 8 décrit comment les informations métriques sont traitées des messages de mise à jour reçus par la passerelle, et comment elles sont générées pour des messages de mise à jour envoyé par la passerelle. Notez que l'entrée est basée sur un chemin particulier à la destination. S'il y a plus d'un chemin à la destination, un chemin dont la mesure composée est minimum est choisi. Si plus d'un chemin a la mesure composée minimum, une règle à égalité arbitraire est utilisée. (Pour la plupart des protocoles, ceci est basé sur l'adresse de la prochaine passerelle de saut.)

Figure 4 — Traitement des paquets entrant

```
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.
```

Figure 5 — Traitement des mises à jour entrantes de routage

```
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
```

Figure 6 — Traitement périodique

```
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
```

Figure 7 — Générez la mise à jour

```
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
```

Figure 8 — Détails des calculs métriques

Cette section décrit la procédure pour calculer des mesures et le saut compte d'une mise à jour de arrivée de routage. L'entrée à cette fonction est l'entrée pour un destination in spécifique par paquet de mise à jour de routage. La sortie est un vecteur des mesures qui peuvent être utilisées pour calculer la mesure composée, et d'un compte de saut. Si ce chemin est ajouté à la table de routage, le vecteur entier des mesures est écrit dans la table. Les paramètres d'interface utilisés dans les définitions suivantes sont positionnement quand la passerelle a été initialisée, pour l'interface sur laquelle la mise à jour de routage sont arrivés, sauf que l'occupation et la fiabilité de canal sont basées sur une moyenne mobile du trafic mesuré par l'interface.

- Retard = retard de retard topologique de paquet + d'interface
- Bande passante = maximum (bande passante de paquet, de bande passante d'interface)
- Fiabilité = minute (fiabilité de paquet, de fiabilité d'interface)
- Occupation de la Manche = maximum (occupation de canal de paquet, d'occupation d'interface channel)(Maximum est utilisé pour la bande passante parce que la mesure de bande passante est enregistrée en forme inverse. Conceptuellement, nous voulons la bande passante minimale.) Notez que l'occupation de canal d'origine du paquet doit être enregistrée, puisqu'elle sera nécessaire pour recompute l'occupation de canal efficace toutes les fois que l'occupation d'interface channel change.

Ce qui suit n'est pas une partie du vecteur métrique, mais est également maintenu dans la table de routage comme caractéristiques du chemin :

- Compte de saut = compte de saut de paquet.
- MTU = minute (MTU de paquet, d'interface MTU).
- La mesure composée distante = a calculé à partir de l'équation 1 utilisant les valeurs métriques du paquet. C'est-à-dire, les composants métriques sont ceux du paquet, et ne sont pas mis à jour comme affiché ci-dessus. Évidemment ceci doit être calculé avant que les réglages affichés ci-dessus soient faits.
- Mesure composée = calculé à partir de l'équation 1 utilisant les valeurs métriques calculées comme décrit dans cette section.

Ce reste de cette section décrit la procédure pour calculer des mesures et le compte de saut pour conduire des mises à jour à envoyer.

Cette fonction détermine les informations métriques et le compte de saut à mettre dans un paquet sortant de mise à jour. Il est basé sur un chemin spécifique à une destination, s'il y a des chemins utilisables. S'il n'y a aucun chemin, ou les chemins sont tout l'en amont, la destination s'appelle « inaccessible ».

```
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.
```

Détails de l'implémentation d'IP

Ce briefle de section décrit les formats de paquet utilisés par Cisco IGRP. L'IGRP est envoyé utilisant des datagrammes IP avec le protocole 9 (IGP) IP. Le paquet commence par une en-tête. Il commence juste après l'en-tête 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 */
```

Pour des messages de mise à jour, les informations de routage suivent juste après l'en-tête.

Le numéro de version est les paquets actuellement 1. ayant d'autres numéros de version sont ignorés.

L'opcode peut être 1 = mise à jour ou 2 = demande.

Ceci indique le type de message. Le format des deux types de message sera donné ci-dessous.

L'édition est un numéro de série qui est incrémenté toutes les fois qu'il y a un changement de la

table de routage. (Ceci est fait en ces conditions en lesquelles le pseudo-code ci-dessus indique pour déclencher une mise à jour de routage.) Le numéro de version permet à des passerelles pour éviter de traiter des mises à jour contenant les informations qu'elles ont déjà vues. (Ceci n'est pas actuellement mis en application. C'est-à-dire, le numéro de version est généré correctement, mais il est ignoré sur l'entrée. Puisqu'il est possible que des paquets soient relâchés, il n'est pas clair que le numéro de version soit suffisant pour éviter le traitement en double. Il serait nécessaire de s'assurer que tous les paquets associés avec l'édition avaient été traités.)

Asystem est le numéro de système autonome. Dans l'implémentation de Cisco, une passerelle peut participer à plus d'un Autonomous System. Chaque un tel système exécute son propre protocole IGRP. Conceptuellement, il y a les tables de routage complètement distinctes pour chaque Autonomous System. Des artères qui arrivent par l'intermédiaire de l'IGRP d'un Autonomous System sont envoyées seulement dans les mises à jour pour cela AS. Ce champ permet à la passerelle pour sélectionner qui a placé des tables de routage pour l'utiliser pour traiter ce message. Si la passerelle reçoit un message IGRP pour COMME ce elle n'est pas configurée pour, elle est ignorée. En fait, l'implémentation de Cisco permet les informations « à couler » d'une quant à des autres. Cependant, je considère qu'en tant qu'un outil d'administration, et pas partie du protocole.

Ninterior, *nsystem*, et *nexterior* indiquent le nombre d'entrées dans chacune des trois sections de messages de mise à jour. Ces sections ont été décrites ci-dessus. Il n'y a aucune autre démarcation entre les sections. Les premières entrées de ninterior sont prises pour être intérieures, les prochaines entrées de nsystem en tant qu'étant système, et le nexterior final en tant qu'extérieur.

La somme de contrôle est une somme de contrôle IP, calculée utilisant le même algorithme de somme de contrôle qu'une somme de contrôle d'UDP. La somme de contrôle est calculée sur l'en-tête IGRP et n'importe quelles informations de routage qui la suivent. Le champ de somme de contrôle est placé à zéro en calculant la somme de contrôle. La somme de contrôle n'inclut pas l'en-tête IP, ni y a il n'importe quelle en-tête virtuelle comme dans l'UDP et le TCP.

Demandes

Une demande IGRP demande au destinataire d'envoyer sa table de routage. Le message de demande a seulement une en-tête. Seulement la version, l'opcode, et les champs d'asystem sont utilisés. Tous autres champs sont zéro. On s'attend à ce que le destinataire envoie un message normal de mise à jour IGRP au demandeur.

Mises à jour

Un message de mise à jour IGRP contient une en-tête, suivie immédiatement en conduisant des entrées. Autant d'entrées de routage sont incluses comme s'insérera dans un datagramme 1500-byte (en-tête IP y compris). Avec des déclarations en cours de structure, ceci permet jusqu'à 104 entrées. Si plus d'entrées sont nécessaires, plusieurs messages de mise à jour sont envoyés. Puisque les messages de mise à jour sont simplement entrée traitée par l'entrée, il n'y a aucun avantage à utiliser un message fragmenté simple plutôt que plusieurs indépendant.

Voici la structure d'une entrée de routage :

```
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 */
```

Les champs ont défini uchar[2] et uchar[3] sont simplement 16 et 24 entiers binaires de bit, dans la commande normale de réseau IP.

Le nombre définit la destination étant décrite. C'est une adresse IP. Pour ménager de l'espace, seulement les 3 premiers octets de l'adresse IP sont indiqués, excepté dans la section intérieure. Dans la section intérieure, les 3 derniers octets sont indiqués. Pour le système et les routes extérieures, aucun sous-réseau n'est possible, ainsi l'octet de poids faible est toujours zéro. Les artères intérieures sont toujours des sous-réseaux d'un réseau connu, ainsi le premier octet de ce network number est fournies.

Le retard est dans les unités de 10 microsecondes. Ceci donne une plage de 10 microsecondes à 168 secondes, qui semble suffisante. Un retard de tout l'indique que le réseau est inaccessible.

La bande passante est bande passante inverse dans les bits par sec mesurés par un facteur de 1.0e10. La plage est des 1200 bps rayent au 10 Gbits/s. (C'est-à-dire, si la bande passante est Kbps N, le nombre utilisé est 10000000/N.)

Le MTU est dans les octets.

La fiabilité est donnée comme fraction de 255. C'est-à-dire, 255 est 100%.

Le chargement est donné comme fraction de 255.

Le compte de saut est un compte simple.

En raison des unités quelque peu étranges utilisées pour la bande passante et le retard, quelques exemples semblent dans la commande. Ce sont les valeurs par défaut utilisées pour plusieurs supports communs.

	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

Calculs métriques

Voici une description de la manière que la mesure composée est calculée réellement dans la version 8.0(3) de Cisco.

```
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
```

Informations connexes

- Page de support pour le routage IP
- Page de support IGRP
- Support technique - Cisco Systems