Introduction à IGRP

Contenu

[Introduction](#)
[Objectifs d'IGRP](#)
[Le problème du routage](#)
[Résumé d'IGRP](#)
[Comparaison avec RIP](#)
[Description détaillée](#)
[Description générale](#)
[Fonctionnalités de stabilité](#)
[Désactiver les mises en attente](#)
[Détails du processus de mise à jour](#)
[Routage des paquets](#)
[Réception des mises à jour de routage](#)
[Traitement périodique](#)
[Génération des messages de mise à jour](#)
[Calcul des informations de la métrique](#)
[Détails de la mise en œuvre IP](#)
[Requêtes](#)
[Mises à jour](#)
[Calculs de la métrique](#)
[Informations connexes](#)

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.

Objectifs d'IGRP

Le protocole IGRP permet à plusieurs passerelles de coordonner leur routage. Ses objectifs sont les suivants :

- Un routage stable même dans des réseaux très grands ou complexes. Aucune boucle de routage, même transitoire.
- Une réaction rapide aux changements topologiques du réseau.

- Peu d'utilisation de bande passante. C'est-à-dire qu'IGRP ne devrait utiliser que la bande passante nécessaire à ses activités.
- Une distribution du trafic vers des routes parallèles quand leur désidérabilité est à peu près égale.
- Prise en compte des taux d'erreurs et du trafic des différentes routes.

La mise en œuvre actuelle d'IGRP gère le routage de TCP/IP. Toutefois, la conception de base d'IGRP doit pouvoir gérer des protocoles variés.

Aucun outil ne peut résoudre tous les problèmes de routage. Les problèmes de routage sont par convention classés en plusieurs catégories. Des protocoles comme IGRP sont appelés des « protocoles de passerelle interne » (IGP). Ils sont conçus pour être utilisés à l'intérieur d'un ensemble de réseaux gérés par une seule entité ou par plusieurs entités étroitement coordonnées. Ces ensembles de réseaux sont connectés par des « protocoles de passerelle externe » (EGP). Un IGP est conçu pour effectuer le suivi d'un grand nombre d'informations à propos de la topologie du réseau. Les priorités lors de la conception d'un IGP sont de pouvoir établir des routes optimales et réagir rapidement aux changements. Un EGP est conçu afin de protéger un ensemble de réseaux des erreurs ou de fausses déclarations intentionnelles par d'autres systèmes. BGP est un de ces protocoles de passerelle externe. Les priorités lors de la conception d'un EGP sont la stabilité et le contrôle administratif. Il est souvent suffisant pour l'EGP d'établir une route acceptable et non la route optimale.

IGRP a certaines similarités avec des protocoles plus anciens, comme le protocole d'information de routage (Routing Information Protocol ou RIP) de Xerox ou de Berkeley et le protocole Hello de David Mills. Il diffère de ces protocoles principalement parce qu'il est conçu pour des réseaux plus grands et plus complexes. Consultez la section Comparaison avec RIP pour une comparaison plus détaillée avec RIP, le protocole le plus largement utilisé parmi les plus anciens protocoles.

Comme les protocoles plus anciens, IGRP est un protocole à vecteur de distance. Dans ce type de protocole, les passerelles ne partagent des informations de routage qu'avec celles qui leur sont contiguës. Ces informations de routage sont un résumé des informations à propos du reste du réseau. Il peut être mathématiquement démontré que l'ensemble des passerelles résout un problème d'optimisation en utilisant ce qui équivaut à un algorithme distribué. Chaque passerelle n'a qu'une partie du problème à résoudre en n'utilisant qu'une partie de l'ensemble des données.

La principale solution similaire à IGRP est l'IGRP amélioré (EIGRP) et une classe d'algorithmes dite du plus court chemin d'abord (SPF pour Shortest Path First). OSPF utilise ce concept. Pour en savoir plus sur OSPF, consultez le Guide de conception OSPF. OSPF utilise une technique de propagation grâce à laquelle chaque passerelle est tenue à jour sur l'état de toutes les interfaces de toutes les autres passerelles. Chaque passerelle résout indépendamment le problème d'optimisation à partir de son point de vue en utilisant les données de l'ensemble du réseau. Chaque approche a ses avantages. Dans certains cas, SPF peut être en mesure de réagir plus rapidement aux changements. Afin de prévenir les boucles de routage, IGRP doit ignorer les nouvelles données pendant quelques minutes après certains types de changements. Comme SPF dispose d'informations provenant directement de chaque passerelle, il est en mesure d'éviter les boucles de routage. Il peut donc réagir immédiatement aux nouvelles informations. Cependant, SPF doit traiter beaucoup plus de données qu'IGRP, tant dans les structures de données internes que dans les messages entre les passerelles.

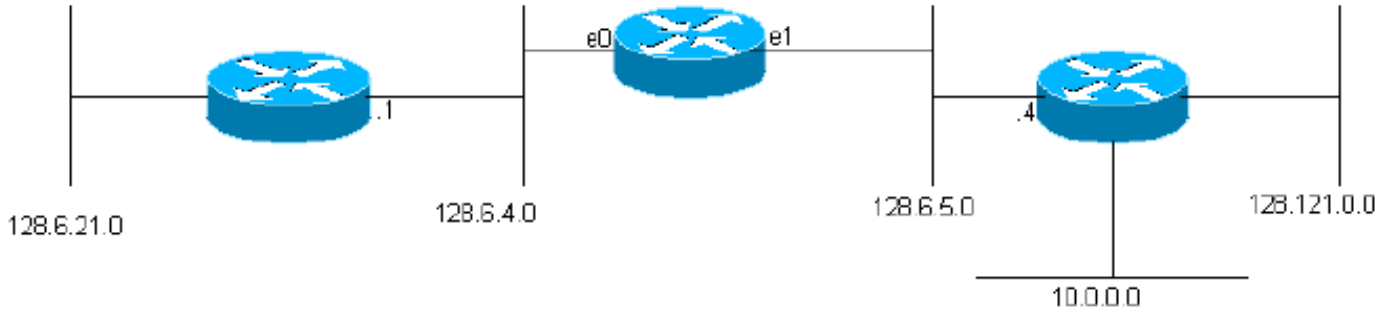
Le problème du routage

IGRP est conçu pour être utilisé dans des passerelles qui connectent plusieurs réseaux. Nous

supposons que les réseaux utilisent des paquets. En fait, les passerelles agissent comme des commutateurs de paquets. Lorsqu'un système connecté à un réseau veut envoyer un paquet à un système d'un autre réseau, il l'envoie à une passerelle. Si la destination est sur un des réseaux connectés à la passerelle, la passerelle y acheminera le paquet. Si la destination est plus éloignée, la passerelle acheminera le paquet à une passerelle qui est plus près de la destination. Les passerelles se servent de tables de routage pour savoir où acheminer les paquets. Voici un exemple de table de routage simple. (Les adresses utilisées dans les exemples sont des adresses IP issues de l'Université Rutgers. Remarquez que le problème de base du routage est similaire à ceux des autres protocoles, mais cette description suppose que c'est IGRP qui est utilisé pour le routage IP.)

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 IGRP réelles contiennent plus d'informations sur chaque passerelle, comme nous le verrons plus loin.) Cette passerelle est connectée à deux réseaux Ethernets désignés 0 et 1. Ils ont reçu les adresses de réseau IP (en fait, les adresses de sous-réseau) 128.6.4 et 128.6.5. Les paquets destinés à ces réseaux peuvent alors être acheminés directement à leur destination, en utilisant tout simplement l'interface Ethernet appropriée. Il n'y a que deux passerelles contiguës, 128.6.4.1 et 128.6.5.4. Les paquets destinés à des réseaux autres que 128.6.4 et 128.6.5 seront acheminés vers l'une ou l'autre de ces passerelles. La table de routage indique quelle passerelle doit être utilisée pour quel réseau. Par exemple, les paquets destinés à un hôte sur le réseau 10 doivent être acheminés vers la passerelle 128.6.5.4. On espère que cette passerelle est plus près du réseau 10, c'est-à-dire que le meilleur chemin vers le réseau 10 passe par cette passerelle. L'objectif principal d'IGRP est de permettre aux passerelles de créer et de gérer des tables de routage comme celle-ci.

Résumé d'IGRP

Comme mentionné plus haut, IGRP est un protocole qui permet aux passerelles de créer des tables de routage en partageant des informations avec les autres passerelles. Une passerelle a d'abord des entrées sur tous les réseaux avec qui elle est directement connectée. Elle obtient des informations sur les autres réseaux en échangeant des mises à jour de routage avec les passerelles contiguës. Dans le cas le plus simple, la passerelle détermine le meilleur chemin pour accéder à chaque réseau. Les caractéristiques d'un chemin sont la passerelle vers laquelle les paquets doivent être acheminés, l'interface réseau à utiliser et les informations de la métrique. Les

informations de la métrique sont un ensemble de nombres qui caractérisent la qualité du chemin. Cela permet à la passerelle de comparer les chemins reçus des différentes passerelles et de décider lequel utiliser. Il arrive souvent qu'il soit logique d'acheminer le trafic par plus d'un chemin. IGRP le fera dès lors que plusieurs chemins s'équivalent. L'utilisateur peut également le configurer pour acheminer le trafic par plusieurs chemins qui sont presque équivalents. Dans ce cas, plus de trafic sera acheminé par le chemin ayant la meilleure métrique. L'objectif est de pouvoir acheminer le trafic par une ligne de 9600 b/s et une ligne de 19 200 b/s, par exemple, et qu'environ deux fois plus de trafic passe par cette dernière.

Les métriques utilisées par IGRP comprennent les éléments suivants :

- La latence topologique
- La bande passante du segment du chemin le plus étroit
- L'occupation de canal du chemin
- La fiabilité du chemin

La latence topologique est la durée nécessaire pour atteindre la destination en empruntant ce chemin, en supposant un réseau non chargé. Évidemment, cette durée est plus grande quand le réseau est chargé. Cependant, la charge du réseau est calculée à l'aide de la valeur de l'occupation de canal, non pas en tentant de mesurer les latences réelles. La bande passante du chemin est tout simplement la bande passante en bits par seconde du segment le plus étroit du chemin. L'occupation de canal indique la quantité de cette bande passante actuellement utilisée. Elle est mesurée et se modifie en fonction de la charge. La fiabilité indique le taux d'erreur actuel. Il s'agit de la proportion de paquets qui arrivent à destination sans erreurs. Elle est mesurée.

Bien qu'elles ne fassent pas partie de la métrique, deux informations supplémentaires sont aussi transmises : le nombre de sauts et l'unité de transmission maximale (MTU). Le nombre de sauts est simplement le nombre de passerelles par lesquelles un paquet doit être acheminé pour se rendre à destination. La MTU est la taille maximale des paquets qui peuvent être envoyés sans devoir être fragmentés tout le long du chemin. (Autrement dit, c'est la plus petite valeur de MTU de tous les réseaux du chemin.)

En fonction des informations de la métrique, une « métrique composite » est calculée pour le chemin. La métrique composite combine les effets des diverses métriques dans un seul nombre qui représente la qualité de ce chemin. C'est la métrique composite qui sert à déterminer le meilleur chemin.

Périodiquement, chaque passerelle diffuse l'intégralité de sa table de routage (avec certaines omissions en raison de la règle de l'horizon partagé) à toutes les passerelles contiguës. Quand une passerelle reçoit une table de routage d'une autre passerelle, il la compare avec la sienne. Toutes les nouvelles destinations et tous les nouveaux chemins s'ajoutent alors à la table de routage de la passerelle. Les chemins inclus dans la diffusion sont comparés aux chemins existants. Si un nouveau chemin est meilleur, il pourra remplacer le chemin existant. Les informations contenues dans la diffusion serviront également à mettre à jour l'occupation de canal et les autres informations sur les chemins existants. Cette procédure générale est semblable à celle utilisée par tous les protocoles à vecteur de distance. Elle est connue dans la littérature mathématique comme l'algorithme de Bellman-Ford. Référez-vous à RFC 1058 pour un développement détaillé de la procédure de base, qui décrit RIP, un protocole à vecteur de distance plus ancien.

Dans IGRP, trois aspects importants de l'algorithme général de Bellman-Ford sont modifiés. Tout d'abord, plutôt qu'une métrique simple, un vecteur de métriques est utilisé pour caractériser les chemins. Ensuite, plutôt que d'acheminer le trafic sur le chemin qui a la meilleure métrique, on

utilise plusieurs chemins dont les métriques sont dans une plage de valeurs spécifiées. Finalement, plusieurs fonctionnalités sont introduites afin d'assurer la stabilité en cas de changements topologiques.

Le meilleur chemin est sélectionné en fonction d'une métrique composite :

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

Où K1 et K2 sont des constantes, Be = la bande passante non chargée x (1 – l'occupation de canal), Dc = la latence topologique et r = la fiabilité.

Le chemin qui a la métrique composite la plus basse sera considéré comme le meilleur chemin. Quand il y a plusieurs chemins vers la destination, la passerelle peut acheminer les paquets sur plus d'un chemin. La division est effectuée en fonction de la métrique composite de chaque chemin des données. Par exemple, si un chemin a une métrique composite de 1 et qu'un autre chemin a une métrique composite de 3, trois fois plus de paquets seront acheminés par le chemin des données dont la métrique composite est de 1.

Il y a deux avantages à utiliser un vecteur d'informations de la métrique. Le premier est qu'il est possible de prendre en charge plusieurs types de service avec le même ensemble de données. Le second consiste en une amélioration de la précision. Quand une seule métrique est utilisée, elle est normalement traitée comme une latence. Chaque segment du chemin est alors ajouté au total de la métrique. Si un segment a une bande passante étroite, il sera normalement représenté par une latence importante. Cependant, les limites de bande passante ne s'accumulent pas vraiment de la même manière que celles des latences. En considérant la bande passante comme une composante distincte, elle peut être gérée correctement. De même, la charge peut être gérée à l'aide d'une valeur distincte pour l'occupation de canal.

IGRP propose un système d'interconnexions de réseaux informatiques qui peut gérer avec stabilité une topologie en graphe générale, y compris des boucles. Le système conserve les informations de la métrique du chemin complet, c'est-à-dire qu'il connaît les paramètres des chemins vers tous les autres réseaux auxquels n'importe quelle passerelle est connectée. Le trafic peut être acheminé vers des chemins parallèles et plusieurs paramètres de chemin peuvent être simultanément calculés sur l'ensemble du réseau.

Comparaison avec RIP

Cette section compare IGRP et RIP. Cette comparaison est utile, car RIP est largement utilisé à des fins similaires à celles d'IGRP. Cette comparaison n'est toutefois pas tout à fait juste. RIP n'a pas été conçu pour répondre exactement aux mêmes exigences qu'IGRP. RIP a été conçu pour n'être utilisé que dans de petits réseaux dont la technologie est relativement uniforme. Il est généralement adéquat dans ce genre de situations.

La différence la plus importante entre IGRP et RIP est la structure des métriques. Malheureusement, RIP ne peut pas facilement être mis à niveau avec cette modification. Celle-ci nécessite de nouveaux algorithmes et de nouvelles structures de données qui sont présentes dans IGRP.

RIP n'utilise qu'une métrique simple de « nombre de sauts » pour décrire le réseau. Contrairement à IGRP, où chaque chemin est décrit par un ensemble de métriques (latence, bande passante, etc.), RIP décrit chaque chemin à l'aide d'un nombre de 1 à 15. Normalement, cette métrique représente le nombre de passerelles empruntées par le chemin pour atteindre sa destination. Cela

signifie qu'il n'y a aucune distinction entre une ligne série lente et une ligne Ethernet. Dans certaines mises en œuvre de RIP, l'administrateur système peut indiquer qu'un saut donné doit être compté plusieurs fois. Les réseaux lents peuvent alors être représentés par un grand nombre de sauts. Mais comme le maximum est de 15, les limites sont rapidement atteintes. Par exemple, si une ligne Ethernet est représentée par un 1 et une ligne de 56 kb/s par un 3, il ne peut pas y avoir plus de 5 lignes de 56 kb/s dans un chemin ou le nombre maximal de sauts de 15 sera dépassé. Les études réalisées par Cisco suggèrent qu'afin de représenter la gamme complète de vitesses de réseaux disponibles et de grands réseaux, une métrique de 24 bits est nécessaire. Si la métrique maximale est trop basse, l'administrateur du système fait face à un dilemme : soit il ne peut distinguer les routes rapides des lentes, soit son réseau dépasse la limite. D'ailleurs, un certain nombre de réseaux nationaux sont maintenant trop grands pour que RIP puisse les gérer, même en ne comptant tous les sauts qu'une seule fois. RIP ne peut tout simplement pas être utilisé pour des réseaux aussi grands.

La solution évidente serait de modifier RIP pour permettre une métrique plus grande. Malheureusement, cela ne fonctionnera pas. Comme tout protocole à vecteur de distance, le « comptage à l'infini » est un problème pour RIP. Ceci est décrit plus en détail dans RFC 1058 . Lorsque la topologie est modifiée, des chemins erronés apparaissent. Les métriques associées à ces chemins augmentent lentement jusqu'à atteindre 15, puis les chemins sont supprimés. Une limite maximale de 15 est assez basse pour que la convergence se produise rapidement, en supposant que les mises à jour déclenchées sont utilisées. Si RIP était modifié pour permettre une métrique de 24 bits, les boucles persisteraient jusqu'à ce que la métrique atteigne 2**24. Ce n'est pas acceptable. IGRP est doté de fonctionnalités conçues pour empêcher l'apparition de routes erronées. Elles sont abordées dans une section plus bas. Il n'est pas pratique de gérer des réseaux complexes sans introduire ces fonctionnalités ou sans passer à un protocole comme SPF.

IGRP fait plus que de simplement étendre la plage des métriques permises. Il restructure la métrique pour inclure la latence, la bande passante, la fiabilité et la charge. Il est possible de les représenter par une métrique simple comme le fait RIP. Cependant, l'approche utilisée par IGRP est potentiellement plus précise. Par exemple, avec une métrique simple, une suite de liens rapides sera équivalente à un seul lien lent. Ce sera peut-être le cas pour le trafic interactif où la latence est la métrique la plus importante. Toutefois, pour le transfert massif de données, la métrique la plus importante est la bande passante, et l'addition des métriques n'est pas la bonne approche. IGRP gère séparément la latence et la bande passante, en cumulant les latences, mais en prenant en compte la bande passante la plus faible. Il n'est pas facile d'incorporer la fiabilité et la charge à une métrique à une composante.

Selon moi, un des plus grands avantages d'IGRP est qu'il est facile à configurer. Il peut représenter directement des quantités ayant une dimension physique. Cela signifie qu'il peut être configuré automatiquement, en fonction du type d'interface, de la vitesse de ligne, etc. Avec une métrique à un seul composant, la métrique est plus susceptible d'avoir à être « cuite » pour incorporer les effets de plusieurs choses différentes.

Les autres innovations sont davantage du domaine des algorithmes et des structures de données que du protocole de routage. Par exemple, IGRP utilise des algorithmes et des structures de données qui prennent en charge l'acheminement du trafic par plusieurs routes. Il est certainement possible de concevoir une mise en œuvre de RIP qui le ferait aussi. Cependant, une fois que le routage est remis en œuvre, il n'y a aucune raison de continuer à utiliser RIP.

Jusqu'à maintenant, je n'ai décrit que l'« IGRP générique », une technologie qui peut prendre en charge le routage de n'importe quel protocole réseau. Il vaut cependant la peine de mentionner dans cette section la mise en œuvre particulière à TCP/IP. Il s'agit de la mise en œuvre qui sera

comparée à RIP.

Les messages de mise à jour de RIP contiennent simplement des copies instantanées de la table de routage. Autrement dit, ils contiennent un certain nombre de destinations et de valeurs de métrique et pas vraiment plus. La mise en œuvre IP d'IGRP a une structure plus poussée. D'abord, le message de mise à jour est identifié par un « numéro de système autonome ». Cette terminologie provient de la tradition Arpanet dans laquelle elle a un sens particulier. Toutefois, pour la plupart réseaux, cela signifie que plusieurs systèmes de routage différents peuvent être utilisés sur le même réseau. Cela est utile là où les réseaux de plusieurs organisations convergent. Chaque organisation peut conserver son propre routage. Comme chaque mise à jour est étiquetée, les passerelles peuvent être configurées pour ne porter attention qu'à celles qui sont pertinentes. Certaines passerelles sont configurées pour recevoir les mises à jour de plusieurs systèmes autonomes. Elles transmettent les informations entre les systèmes de façon contrôlée. Remarquez que ce n'est pas une solution complète aux problèmes de sécurité de routage. Toutes les passerelles peuvent être configurées pour écouter les mises à jour de tout système autonome. Toutefois, il reste un outil très pratique pour la mise en œuvre des politiques de routage quand il y a une certaine confiance entre les administrateurs des réseaux.

La seconde fonctionnalité structurelle des messages de mise à jour d'IGRP influence la manière dont IGRP gère les routes par défaut. La plupart des protocoles de routage ont un concept de route par défaut. Il n'est souvent pas utile que les mises à jour du routage mentionnent tous les réseaux du monde. Un ensemble de passerelles n'a généralement besoin que des informations de routage détaillées sur les réseaux de son organisation. Tout le trafic vers des destinations à l'extérieur de son organisation peut être acheminé vers l'une des quelques passerelles frontière. Ces passerelles frontière pourraient avoir des informations plus complètes. La route vers la meilleure passerelle frontière est une « route par défaut ». Elle est dite route par défaut, car elle sert à atteindre toute destination qui n'apparaît pas dans les mises à jour de routage internes. RIP, ainsi que certains autres protocoles de routage, propage les informations sur la route par défaut comme s'il s'agissait d'un vrai réseau. IGRP adopte une approche différente. Plutôt que de programmer une seule fausse entrée pour le routage par défaut, IGRP permet de marquer de vrais réseaux comme candidat pour le routage par défaut. Ceci est mis en œuvre en plaçant les informations à propos de ces réseaux dans une section extérieure spéciale du message de mise à jour. On peut toutefois simplement s'imaginer qu'on modifie un bit associé à ces réseaux. IGRP analyse périodiquement tous les candidats et choisit comme route par défaut celui dont la métrique est la plus basse.

Cette approche relative aux routes par défaut est potentiellement plus flexible que celle de la plupart des mises en œuvre de RIP. Typiquement, la plupart des passerelles RIP peuvent être configurées pour générer une route par défaut ayant une certaine métrique. L'intention est que cela soit fait par les passerelles frontière.

Description détaillée

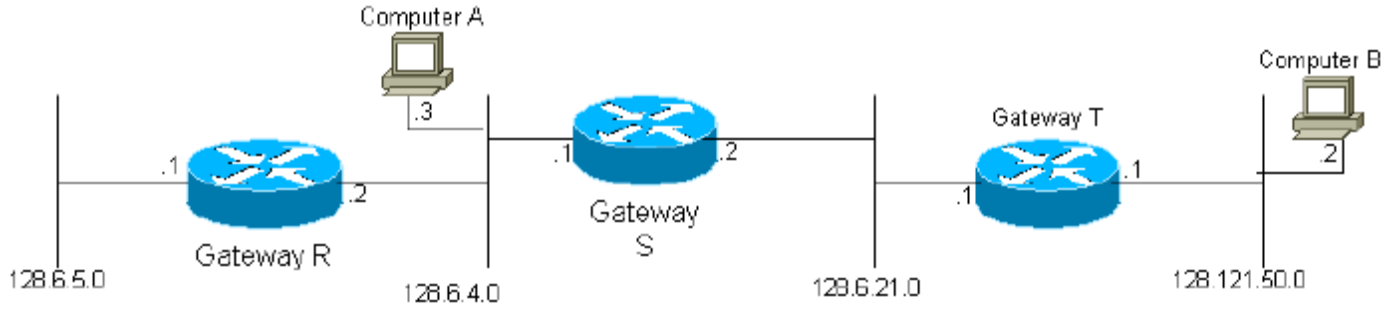
Cette section contient une description détaillée d'IGRP.

Description générale

Quand une passerelle est mise en service pour la première fois, sa table de routage est initialisée. Un opérateur peut le faire à partir de la console d'un terminal ou les informations peuvent être lues à partir de fichiers de configuration. Une description de chaque réseau connecté à la passerelle est fournie, y compris la latence topologique tout le long du lien (par exemple, le temps nécessaire

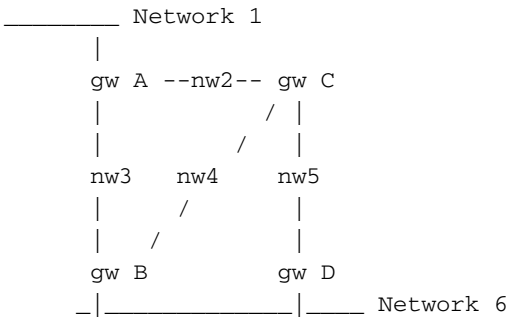
à un bit pour parcourir le lien) et la bande passante du lien.

Figure 2



Par exemple, dans le schéma ci-dessus, la passerelle S recevrait comme informations qu'elle est connectée aux réseaux 2 et 3 par l'intermédiaire des interfaces correspondantes. Ainsi, la passerelle S sait dès le départ qu'elle peut atteindre n'importe quel ordinateur des réseaux 2 et 3. Toutes les passerelles sont programmées pour transmettre périodiquement aux passerelles voisines les informations reçues lors de leur initialisation, ainsi que celles reçues des autres passerelles. Ainsi, la passerelle S recevrait des mises à jour des passerelles R et T et apprendrait qu'elle peut atteindre les ordinateurs du réseau 1 par l'intermédiaire de la passerelle R et les ordinateurs du réseau 4 par l'intermédiaire de la passerelle T. Comme la passerelle S envoie l'intégralité de sa table de routage, lors du prochain cycle, la passerelle T saura qu'elle peut atteindre le réseau 1 par l'intermédiaire de la passerelle S. On peut facilement comprendre que les informations à propos de chaque réseau finiront par atteindre chaque passerelle du système, si bien sûr l'ensemble du réseau est connecté.

Figure 3



Chaque passerelle calcule une métrique composite pour déterminer la désidérabilité des chemins de données vers les ordinateurs de destination. Par exemple, dans le schéma ci-dessus, pour une destination dans le réseau 6, la passerelle A (gw A) calculerait les fonctions de métrique pour deux chemins, via les passerelles B et C. Notez que les chemins sont définis simplement par le saut suivant. Il y a en fait trois routes possibles à partir de la passerelle A jusqu'au réseau 6 :

- Directement vers B
- Vers C, puis vers B
- Vers C, puis vers D

Cependant, la passerelle A n'a pas besoin de choisir entre les deux routes impliquant C. La table de routage de A a une entrée unique représentant le chemin vers C. Sa métrique représente le meilleur moyen de passer de C à la destination finale. Si A achemine un paquet vers C, c'est à C de décider s'il l'acheminera vers B ou vers D.

Équation 1

La fonction de métrique composite utilisée pour calculer chaque chemin des données se trouve ci-dessous :

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

où r = la fiabilité fractionnaire (le pourcentage des transmissions qui sont reçues avec succès par la passerelle suivante), Dc = la latence composite, Be= la bande passante réelle : bande passante non chargée x (1 – l'occupation de canal), et K1 et K2 sont des constantes.

Équation 2

En principe, la latence composite (Dc) peut être calculée à l'aide de l'équation ci-dessous :

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

Où Ds = la latence de commutation, Dcir = la latence de circuit (la latence de propagation de 1 bit) et DT = la latence de transmission (la latence d'un message de 1500 bits sur un réseau non chargé).

Cependant, en pratique, une latence type est utilisée pour chaque type de technologie de réseau. Par exemple, il y a une latence type pour Ethernet et pour les lignes séries de n'importe quel débit binaire.

Voici un exemple de la manière dont la table de routage de la passerelle A pourrait gérer le routage vers le réseau 6 dans le diagramme ci-dessus. (Remarquez qu'à des fins de simplicité, les composantes individuelles du vecteur de la métrique ne sont pas affichées)

Exemple de table de routage :

Réseau	Interface	Prochaine passerelle	Métrique
1	NW 1	Aucune	Connexion directe
2	NW 2	Aucune	Connexion directe
3	NW 3	Aucune	Connexion directe
4	NW 2	C	1270
	NW 3	B	1180
5	NW 2	C	1270
	NW 3	B	2130
6	NW 2	C	2040
	NW 3	B	1180

Le processus de base de la construction d'une table de routage par l'échange d'informations avec les voisins est décrit par l'algorithme de Bellman-Ford. Cet algorithme a été utilisé dans des protocoles antérieurs comme RIP (RFC 1058). Afin de gérer des réseaux plus complexes, IGRP ajoute trois fonctionnalités à l'algorithme Bellman-Ford de base :

1. Plutôt qu'une métrique simple, un vecteur de métriques est utilisé afin de caractériser les chemins. Une métrique composite simple peut être calculée à partir de ce vecteur à l'aide de l'équation 1 ci-dessus. L'utilisation d'un vecteur permet à la passerelle d'accommoder différents types de service en utilisant différents coefficients dans l'équation 1. Elle permet également une représentation plus précise des caractéristiques d'un réseau qu'une métrique unique.
2. Plutôt que de choisir le chemin qui a la meilleure métrique, le trafic est acheminé par plusieurs chemins dont les métriques sont dans une plage de valeurs spécifiées. Cela permet de faire l'acheminement par plusieurs chemins en parallèle afin de mieux tirer parti de la bande passante que le ferait une route unique. Une variance V est définie par l'administrateur réseau. Tous les chemins avec une métrique composite minimale de M sont conservés. De plus, tous les chemins dont la métrique est plus basse que V x M sont conservés. Le trafic est acheminé par plusieurs chemins de façon inversement proportionnelle à leur métrique composite.
3. Ce concept de variance pose toutefois certains problèmes. Il est difficile d'élaborer des stratégies qui se servent de valeurs de variance supérieures à 1 sans créer de boucles de paquets. La version 8.2 de Cisco ne met pas en œuvre la fonctionnalité de variance. (Je ne sais pas exactement dans quelle version la fonctionnalité a été retirée.) Cela a eu pour effet de régler définitivement la variance à 1.
4. Plusieurs fonctionnalités ont été ajoutées afin d'assurer la stabilité lors des changements topologiques. Ces fonctionnalités sont conçues pour empêcher les boucles de routage et le « comptage à l'infini » qui ont caractérisé les tentatives précédentes d'utilisation des algorithmes de type Ford pour ce genre d'application. Les fonctionnalités principales de stabilité sont les mises en attente, les mises à jour déclenchées, l'horizon partagé et l'empoisonnement. Elles seront abordées plus en détail ci-dessous.

La division du trafic (le point 2) pose des risques plutôt subtils. La variance V est conçue pour permettre aux passerelles d'utiliser des chemins parallèles ayant des vitesses différentes. Par exemple, une ligne de 9600 b/s pourrait être parallèle à une ligne de 19 200 b/s pour assurer la redondance. Si la variance V est de 1, seul le meilleur chemin sera utilisé. Donc, la ligne de 9600 b/s ne servira pas si la ligne de 19 200 b/s a une fiabilité raisonnable. (Cependant, si plusieurs chemins sont identiques, le trafic sera partagé entre ceux-ci.) En augmentant la variance, le trafic peut être partagé entre la meilleure route et d'autres routes presque aussi bonnes. Si la variance est suffisamment élevée, le trafic sera partagé entre les deux lignes. Le risque d'une variance très élevée est qu'en plus de chemins plus lents, des chemins allant « dans la mauvaise direction » soient utilisés. Il doit donc y avoir une règle supplémentaire pour empêcher le trafic d'être envoyé « en amont » : Aucun trafic ne doit être envoyé vers les chemins dont la métrique composite distante (la métrique composite du saut suivant) est supérieure à la métrique composite de la passerelle. En général, il est conseillé aux administrateurs système de ne pas définir une variance supérieure à 1, sauf dans des cas particuliers où des chemins parallèles doivent être utilisés. Dans ce cas, la variance est minutieusement réglée afin de fournir les « bons » résultats.

IGRP est conçu pour gérer des « types de service » et des protocoles variés. Le type de service est une caractéristique contenue dans un paquet de données qui modifie la façon dont les chemins sont évalués. Par exemple, le protocole TCP/IP permet de définir pour le paquet l'importance relative d'une bande passante élevée, d'une latence basse ou d'une fiabilité élevée. Généralement, les applications interactives favoriseront une latence basse, tandis que les applications de transfert de masse favoriseront une bande passante élevée. Ces exigences déterminent les valeurs relatives de K1 et K2 qui sont appropriées dans l'équation 1. Chaque combinaison des spécifications du paquet qui doit être pris en charge est désignée comme un

« type de service ». Pour chaque type de service, une paire de paramètres K1 et K2 doit être sélectionnée. Une table de routage est conservée pour chaque type de service. C'est parce que les chemins sont sélectionnés et ordonnés en fonction de la métrique composite calculée par l'équation 1. Elle est différente pour chaque type de service. Les informations de toutes ces tables de routage sont combinées pour produire le message de mise à jour de routage qui est envoyé aux autres passerelles, tel que décrit dans la figure 7.

Fonctionnalités de stabilité

Cette section décrit les mises en attente, les mises à jour déclenchées, l'horizon partagé et l'empoisonnement. Ces fonctionnalités sont conçues pour empêcher les passerelles de choisir des routes erronées. Comme décrit dans la RFC 1058 , cela peut se produire lorsqu'une route devient inutilisable en raison d'une défaillance d'une passerelle ou d'un réseau. En principe, les passerelles contiguës détectent les défaillances. Elles envoient ensuite des mises à jour du routage pour indiquer que l'ancienne route est inutilisable. Il est toutefois possible que les mises à jour n'atteignent pas du tout certaines parties du réseau ou qu'elles tardent à atteindre certaines passerelles. Une passerelle qui croit que l'ancienne route fonctionne toujours correctement peut continuer à diffuser cette information, ce qui réintroduit la route défaillante dans le système. Cette information finira par se propager à travers le réseau pour revenir à la passerelle qui l'a réinjectée. Il en résulte une route circulaire.

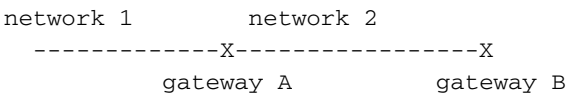
En fait, il existe certaines redondances parmi les contre-mesures. En principe, les mises en attente et les mises à jour déclenchées devraient suffire à empêcher les routes erronées en premier lieu. Cependant, en pratique, elles sont parfois insuffisantes en raison de divers types de pannes de communications. L'horizon partagé et l'empoisonnement de route sont conçus pour empêcher toutes les boucles de routage.

Normalement, les nouvelles tables de routage sont régulièrement envoyées aux passerelles voisines (toutes les 90 secondes par défaut, mais cette valeur peut être modifiée par l'administrateur système). Une mise à jour déclenchée est une nouvelle table de routage qui est envoyée immédiatement en réaction à certains changements. Le changement le plus important est le retrait d'une route. Cela peut arriver quand un délai d'inactivité expire (possiblement à cause de la défaillance d'une passerelle ou d'une ligne voisine) ou quand un message de mise à jour de la prochaine passerelle du chemin indique que celui-ci n'est plus utilisable. Quand une passerelle G détecte qu'une route n'est plus utilisable, une mise à jour est immédiatement déclenchée. Cette mise à jour indique que la route est inutilisable. Pensez à ce qui se passe quand cette mise à jour atteint les passerelles voisines. Si la route de la passerelle voisine pointe vers G, cette passerelle devra retirer cette route. Cela entraîne le déclenchement d'une mise à jour par le voisin, etc. Ainsi, un échec déclenchera une vague de messages de mise à jour. Cette vague se propagera dans la partie du réseau dont les routes passent par la passerelle ou le réseau défaillant.

Les mises à jour déclenchées seraient suffisantes s'il était possible de garantir que la vague de mises à jour atteigne immédiatement toutes les passerelles touchées. Toutefois, il y a deux problèmes. D'abord, les paquets contenant le message de mise à jour peuvent être perdus ou corrompus par un lien du réseau. Ensuite, les mises à jour déclenchées ne sont pas instantanées. Il est possible qu'une passerelle n'ayant pas encore reçu la mise à jour déclenchée envoie au mauvais moment une mise à jour régulière qui réintroduira la route erronée dans la table de routage d'un voisin ayant déjà reçu la mise à jour déclenchée. Les mises en attente sont conçues pour résoudre ces problèmes. La règle de mise en attente dicte que, quand une route est supprimée, aucune nouvelle route vers la même destination ne sera acceptée pendant une certaine période. Cela permet aux mises à jour déclenchées de se propager à toutes les autres

passerelles pour s'assurer que toute nouvelle route ne sera pas la réintroduction de l'ancienne par une autre passerelle. La période de mise en attente doit être suffisamment longue pour permettre à la vague de mises à jour déclenchées de rejoindre l'ensemble du réseau. De plus, elle doit aussi inclure quelques cycles de diffusion réguliers afin de gérer les paquets perdus. Pensez à ce qui arrive si une des mises à jour déclenchées est perdue ou corrompue. La passerelle qui a émis cette mise à jour enverra une autre mise à jour lors du prochain cycle de mise à jour régulier. Ceci va relancer la vague de mises à jour déclenchées chez ses voisins qui n'ont pas été atteints par la vague initiale.

La combinaison des mises à jour déclenchées et des mises en attente devrait suffire pour retirer les routes expirées et empêcher leur réintroduction. Cependant, il vaut mieux quand même prendre certaines précautions supplémentaires. Elles permettent à des réseaux ayant beaucoup de pertes et à des réseaux qui ont été fractionnés de fonctionner quand même. Ces précautions supplémentaires prévues par IGRP sont l'horizon partagé et l'empoisonnement de route. L'horizon partagé provient de l'idée qu'il est toujours inutile de renvoyer une route vers la passerelle d'où elle provient. Examinons la situation suivante :



La passerelle A informe la passerelle B qu'elle a une route vers le réseau 1. Quand la passerelle B envoie des mises à jour à la passerelle A, elle n'a pas besoin de mentionner le réseau 1. Comme la passerelle A est plus près du réseau 1, elle n'a aucune raison de passer par la passerelle B. La règle d'horizon partagé dicte qu'un message de mise à jour distinct doit être généré pour chaque voisin (en fait, pour chaque réseau voisin). La mise à jour envoyée à un voisin donné doit omettre les routes qui pointent vers ce voisin. Cette règle empêche les boucles entre les passerelles contiguës. Par exemple, supposons une défaillance de l'interface de la passerelle A vers le réseau 1. Sans la règle d'horizon partagé, la passerelle B indiquera à la passerelle A qu'elle peut rejoindre le réseau 1. Comme elle n'a plus de route utilisable, la passerelle A pourrait choisir cette route. Dans ce cas, les passerelles A et B auraient toutes deux des routes vers le réseau 1. Mais A pointe vers B et B pointe vers A. Bien sûr, les mises à jour déclenchées et les mises en attente devraient empêcher cela de se produire. Mais comme il n'y a aucune raison d'envoyer des informations vers la passerelle d'où elles viennent, l'horizon partagé reste utile. En plus d'empêcher les boucles, l'horizon partagé réduit la taille des messages de mise à jour.

L'horizon partagé devrait empêcher les boucles entre les passerelles contiguës. L'empoisonnement de route, quant à lui, s'attaque aux boucles plus grandes. La règle est que si la métrique d'une route augmente dans une certaine proportion lors d'une mise à jour, il y a une boucle. La route doit être retirée et mise en attente. La règle actuelle est qu'une route doit être retirée si la métrique composite augmente d'un facteur supérieur à 1,1. Il n'est pas prudent que toute augmentation de la métrique composite déclenche le retrait de la route, car des changements à l'occupation de canal ou à la fiabilité peuvent entraîner des variations mineures. Le facteur de 1,1 n'est qu'une valeur heuristique. La valeur exacte n'est pas cruciale. Nous nous attendons à ce que cette règle ne serve qu'à briser de très grandes boucles puisque les plus petites auront été empêchées par les mises à jour déclenchées et les mises en attente.

Désactiver les mises en attente

Depuis la version 8.2, le code de Cisco permet de désactiver les mises en attente. Le désavantage des mises en attente est qu'elles retardent l'adoption d'une nouvelle route après la défaillance d'une ancienne route. Avec les paramètres par défaut, plusieurs minutes peuvent

s'écouler avant qu'un routeur adopte une nouvelle route après une modification. Toutefois, pour les raisons expliquées ci-dessus, il n'est pas prudent de simplement retirer les mises en attente. Le résultat serait le comptage à l'infini, comme indiqué dans le RFC 1058. Nous supposons, sans pouvoir le prouver, qu'avec une version plus efficace de l'empoisonnement de route, les mises en attente ne seraient plus nécessaires pour empêcher le comptage à l'infini. La désactivation des mises en attente permet donc cette forme plus efficace d'empoisonnement de route. Remarquez toutefois que l'horizon partagé et les mises à jour déclenchées sont toujours en vigueur.

La forme plus efficace d'empoisonnement de route se base sur le nombre de sauts. Si le nombre de sauts d'un chemin augmente, la route est retirée. Cela retirera évidemment certaines routes qui sont toujours valides. Si un changement ailleurs dans le réseau force le chemin à passer par une passerelle de plus, le nombre de sauts augmentera. Dans ce cas, la route est toujours valide. Il n'y a toutefois aucun moyen absolument sûr de distinguer ce genre de situation des boucles de routage (le comptage à l'infini). L'approche la plus sûre est donc de retirer la route quand le nombre de sauts augmente. Si la route est toujours valide, elle sera réintroduite lors de la prochaine mise à jour, ce qui déclenchera une mise à jour qui réintroduira la route dans tout le système.

En général, les algorithmes de vecteur de distance adoptent facilement de nouvelles routes. Le problème est d'éliminer complètement les anciennes routes du système. Une règle excessivement stricte pour retirer les routes suspectes ne devrait donc pas poser de problèmes.

Détails du processus de mise à jour

Les processus décrits dans les figures 4 à 8 ne sont conçus que pour un seul protocole de réseau, par exemple le protocole TCP/IP, DECnet ou ISO/OSI. Cependant, seuls les détails pour TCP/IP sont fournis. Une passerelle peut traiter les données qui utilisent plusieurs protocoles. Comme chaque protocole a des systèmes d'adressage et des formats de paquet différents, le code utilisé pour mettre en œuvre les figures 4 à 8 variera généralement d'un protocole à l'autre. Le processus décrit dans la figure 4 variera le plus, comme l'indiquent les notes détaillées de cette figure. Les processus décrits dans les figures 5 à 8 auront la même structure générale. La différence principale d'un protocole à l'autre sera le format du paquet de la mise à jour du routage, qui doit être compatible avec un protocole précis.

Remarquez que la définition d'une destination peut varier d'un protocole à l'autre. La méthode décrite ici peut servir au routage vers des hôtes individuels, vers des réseaux ou vers des systèmes d'adressage hiérarchiques plus complexes. Le type de routage à utiliser dépendra du système d'adressage du protocole. La mise en œuvre actuelle de TCP/IP ne prend en charge que le routage vers des réseaux IP. La « destination » signifie donc l'adresse du réseau ou sous-réseau IP. Les informations à propos du sous-réseau ne sont conservées que pour les réseaux connectés.

Les figures 4 à 7 montrent le pseudocode pour divers éléments du processus de routage utilisé par la passerelle. Au début du programme, les protocoles et les paramètres acceptables pour décrire chaque interface sont entrés.

La passerelle ne gérera que les protocoles qui sont énumérés. Toute communication provenant d'un système qui n'utilise pas un des protocoles de la liste sera ignorée. Les entrées de données sont les suivantes :

- Les réseaux auxquels la passerelle est connectée.
- La bande passante non chargée de chaque réseau.

- La latence topologique de chaque réseau.
- La fiabilité de chaque réseau.
- L'occupation de canal de chaque réseau.
- La MTU de chaque réseau.

La métrique de chaque chemin des données est calculée à l'aide de l'équation 1. Remarquez que les trois premiers éléments sont à peu près définitifs. Ils dépendent de la technologie réseau sous-jacente et ne sont pas modifiés par la charge. Ils pourraient être définis à partir d'un fichier de configuration ou entrés directement par un opérateur. Veuillez noter qu'IGRP n'utilise pas de latence mesurée. Tant en théorie qu'en pratique, les protocoles qui utilisent la latence mesurée semblent avoir beaucoup de difficulté à maintenir la stabilité du routage. Il y a deux paramètres mesurés : la fiabilité et l'occupation de canal. La fiabilité est basée sur le taux d'erreurs signalé par le micrologiciel ou le matériel de l'interface réseau.

En plus de ces entrées, l'algorithme de routage a besoin des valeurs de plusieurs paramètres de routage. Ceci inclut les valeurs de minuteur, la variance et l'état d'activation des mises en attente. Ces valeurs sont normalement spécifiées par un fichier de configuration ou entrées par un opérateur. (Dans la version 8.2 de Cisco, la variance est définitivement réglée à 1.)

Une fois que les informations initiales sont entrées, les opérations de la passerelle sont déclenchées par des événements : l'arrivée d'un paquet de données à l'une des interfaces réseau ou l'échéance d'un minuteur. Les processus décrits dans les figures 4 à 7 sont déclenchés lors des événements suivants :

- Quand un paquet arrive, il est traité comme indiqué à la figure 4. Le paquet est alors acheminé vers une autre interface, abandonné ou accepté pour être encore traité.
- Quand un paquet est accepté par la passerelle pour être encore traité, il est analysé d'une manière propre à chaque protocole que nous ne décrirons pas ici. Si le paquet contient une mise à jour de routage, il est traité selon la figure 5.
- La figure 6 montre les événements déclenchés par un minuteur. Le minuteur est configuré pour générer une interruption chaque seconde. Quand il y a interruption, le processus décrit dans la figure 6 est exécuté.
- La figure 7 décrit une sous-routine de mise à jour de routage. Les appels à cette sous-routine se trouvent dans les figures 5 et 6.
- De plus, la figure 8 montre le détail du calcul de la métrique mentionné dans les figures 5 et 7.

Il y a quatre constantes de temps critiques qui contrôlent la propagation et l'expiration des routes. Ces constantes de temps peuvent être définies par l'administrateur système. Il y a quand même des valeurs par défaut. Ces constantes de temps sont :

- Le délai de diffusion : il indique la fréquence de la diffusion des mises à jour sur chaque interface connectée de toutes les passerelles. La valeur par défaut est de 90 secondes.
- Le délai d'invalidité : il indique la durée après laquelle un chemin est considéré comme non valide si aucune mise à jour n'a été reçue. Ce délai doit être de plusieurs fois le délai de diffusion afin de permettre de renvoyer des paquets contenant une mise à jour qui ont été perdus. La valeur par défaut est de trois fois le délai de diffusion.
- Le délai d'attente : il indique la durée de la mise en attente quand une destination ne peut plus être atteinte (ou si sa métrique a augmenté suffisamment pour déclencher l'empoisonnement). Quand la mise en attente est en vigueur, aucun nouveau chemin vers la destination concernée n'est accepté. Le délai d'attente indique la durée de cet état. Il doit être équivalent à plusieurs fois le délai de diffusion. La valeur par défaut est de trois fois le délai de diffusion plus 10 secondes. (Comme il est indiqué dans la section Désactiver les mises en

attente, il est possible de désactiver les mises en attente.)

- Le délai de nettoyage : il indique la durée après laquelle une entrée est retirée de la table de routage si aucune mise à jour la concernant n'a été reçue. Remarquez la différence entre le délai d'invalidité et le délai de nettoyage : Après le délai d'invalidité, le chemin est expiré et retiré. S'il ne reste aucun chemin vers une destination, celle-ci est maintenant inatteignable. L'entrée de la destination est cependant conservée dans la base de données. Elle est nécessaire pour appliquer la mise en attente. Après le délai de nettoyage, l'entrée est retirée de la base de données de la table. Il doit être plus long que la somme du délai d'invalidité et du délai de mise en attente. La valeur par défaut est de sept fois le délai de diffusion.

Ces figures présupposent les structures de données principales suivantes. Un ensemble distinct de ces structures de données est conservé pour chaque protocole pris en charge par la passerelle. Pour chaque protocole, un ensemble distinct de structures de données est conservé pour chaque type de service à prendre en charge.

Pour chaque destination connue du système, il y a une liste (possiblement vide) de chemins vers la destination, une heure de fin de la mise en attente et l'heure de la dernière mise à jour. L'heure de la dernière mise à jour indique la dernière fois qu'un chemin vers cette destination a été inclus dans la mise à jour d'une autre passerelle. Remarquez que le moment de la mise à jour de chaque chemin est également conservé. Quand le dernier chemin vers une destination est retiré, la destination est mise en attente, sauf si les mises en attente sont désactivées (consultez la section Désactiver les mises en attente pour plus de renseignements). L'heure de fin de la mise en attente indique l'heure à laquelle la mise en attente se termine. Si la valeur est différente de zéro, cela signifie que la destination est mise en attente. Afin de gagner du temps de calcul, il est aussi recommandé de conserver la « meilleure métrique » de chaque destination. Il s'agit simplement de la valeur la plus basse des métriques composites de tous les chemins vers la destination.

Chaque chemin vers une destination contient l'adresse du prochain saut, l'interface à utiliser et un vecteur de métriques qui caractérisent le chemin, ce qui inclut la latence topologique, la bande passante, la fiabilité et l'occupation de canal. Les autres informations associées à chaque chemin incluent le nombre de sauts, la MTU, la source de l'information, la métrique composite distante et une métrique composite calculée avec ces valeurs à l'aide de l'équation 1. Il y a également l'heure de la dernière mise à jour. La source de l'information indique la provenance de la plus récente mise à jour du chemin. En pratique, c'est la même que l'adresse du saut suivant. L'heure de la dernière mise à jour est simplement l'heure d'arrivée de la dernière mise à jour de ce chemin. Elle sert à déterminer quand les chemins inactifs expirent.

Remarquez qu'un message de mise à jour d'IGRP comporte trois parties : interne, système (signifiant « ce système autonome », mais pas interne) et externe. La section interne est pour les routes vers les sous-réseaux. Les informations de tous les sous-réseaux n'y sont pas incluses. Seuls les sous-réseaux d'un seul réseau s'y trouvent. Il s'agit du réseau associé à l'adresse à laquelle la mise à jour est envoyée. Normalement, les mises à jour sont diffusées par chaque interface. Il s'agit donc du réseau où la mise à jour est diffusée. (D'autres cas surviennent pour les réponses à une demande IGRP et IGRP point à point.) Les réseaux importants (par exemple, ceux qui ne sont pas des sous-réseaux) sont mis dans la partie système du message de mise à jour, sauf s'ils sont spécifiquement désignés comme étant externes.

Un réseau sera désigné comme externe s'il était dans la section externe d'un message de mise à jour reçu d'une autre passerelle. La mise en œuvre de Cisco permet également à l'administrateur système de déclarer certains réseaux comme externes. Les routes externes sont aussi désignées comme « candidats pour le routage par défaut ». Ce sont des routes qui vont vers ou passent par des passerelles qui sont considérées comme étant appropriées par défaut et qui peuvent être

utilisées quand il n'y a pas de routes définies vers une destination. Par exemple, à l'université Rutgers, la passerelle qui connecte l'université au réseau régional est configurée pour indiquer que la route vers la dorsale NSFnet est externe. La mise en œuvre de Cisco choisit une route par défaut en sélectionnant la route externe qui a la meilleure métrique.

Les sections suivantes ont pour but de clarifier certaines parties des figures 4 à 8.

Routage des paquets

La figure 4 décrit le traitement général des paquets en entrée. Elle sert simplement à clarifier la terminologie. Évidemment, ce n'est pas une description complète de ce qu'accomplit une passerelle IP.

Ce processus se sert de la liste des protocoles pris en charge et des informations sur les interfaces entrées lors de l'initialisation de la passerelle. Le détail du traitement d'un paquet dépend du protocole qu'il utilise. Ceci est déterminé à l'étape A. L'étape 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, on utilise la mise en œuvre de la figure 4 appropriée selon le type de protocole. Les détails du contenu du paquet sont décrits dans les spécifications du protocole. Les spécifications d'un protocole incluent une procédure pour déterminer la destination d'un paquet, une procédure pour comparer la destination et l'adresse de la passerelle pour déterminer si la passerelle est elle-même la destination, une procédure pour déterminer si un paquet est diffusé et une procédure pour déterminer si la destination fait partie d'un réseau spécifié. Ces procédures servent lors des étapes B et C de la figure 4. Le test de l'étape D nécessite une recherche parmi les destinations énumérées dans la table de routage. Le test est réussi si la table de routage contient une entrée pour cette destination et s'il existe au moins un chemin utilisable associé à celle-ci. Remarquez que les données relatives à la destination et au chemin utilisés au cours de cette étape et lors de la prochaine sont conservées séparément pour chaque type de service pris en charge. Donc, cette étape commence en déterminant le type de service spécifié par le paquet, puis en sélectionnant l'ensemble de structures de données correspondant qui sera utilisé au cours de cette étape et de la suivante.

Un chemin est considéré comme utile dans le cadre des étapes D et E si sa métrique composite distante est inférieure à sa métrique composite. Si la métrique composite distante d'un chemin est plus grande que sa métrique composite, son prochain saut est « plus éloigné » de la destination, comme l'indique sa métrique. C'est ce qu'on appelle un « chemin en amont ». On s'attendrait normalement à ce que l'utilisation des métriques empêche de choisir des chemins en amont. Il est évident qu'un chemin en amont ne peut jamais être le meilleur choix. Cependant, si la variance est grande, des chemins qui ne sont pas les meilleurs peuvent être empruntés. Certains d'entre eux pourraient être en amont.

L'étape E détermine le chemin à emprunter. Les chemins dont la métrique composite distante n'est pas inférieure à leur métrique composite ne sont pas pris en compte. S'il y a plusieurs chemins acceptables, ces chemins sont tous utilisés en round-robin de manière pondérée. La fréquence à laquelle un chemin est emprunté est inversement proportionnelle à sa métrique composite.

Réception des mises à jour de routage

La figure 5 décrit le traitement d'une mise à jour de routage reçue d'une passerelle voisine. Ces mises à jour sont composées d'une liste d'entrées qui contiennent chacune des informations sur une seule destination. Il peut y avoir plus d'une entrée pour la même destination dans une seule

mise à jour de routage afin de pouvoir gérer plusieurs types de service. Chacune de ces entrées est traitée individuellement, comme l'indique la figure 5. Si une entrée est dans la section externe de la mise à jour, la destination sera désignée comme externe si elle est ajoutée à la suite de ce processus.

Tout le processus décrit dans la figure 5 doit être répété pour chaque type de service pris en charge par la passerelle à l'aide de l'ensemble des informations sur la destination et le chemin associé à ce type de service. Ceci est indiqué dans la boucle la plus à l'extérieur de la figure 5. La totalité de la mise à jour de routage doit être traitée pour chaque type de service. (Remarquez que la mise en œuvre actuelle d'IGRP ne prend pas en charge plusieurs types de service, donc la boucle la plus à l'extérieur n'est pas mise en œuvre en ce moment.)

Àl'étape A, des tests d'acceptabilité de base sont effectués sur le chemin. Ils devraient inclure des tests de raisonnabilité pour la destination. Les adresses de réseau impossibles (« martiennes ») doivent être rejetées. (Reportez-vous à RFC 1009 et RFC 1122 pour plus d'informations.) Les mises à jour sont également rejetées si la destination est mise en attente, c'est-à-dire que l'heure de fin de la mise en attente est différente de zéro et est ultérieure à l'heure actuelle.

Au cours de l'étape B, une recherche est effectuée dans la table de routage pour vérifier si cette entrée correspond à un chemin déjà connu. Un chemin est caractérisé dans la table de routage par sa destination, le saut suivant du chemin, l'interface de sortie à utiliser et la source de l'information (et l'adresse d'où provient la mise à jour qui, dans la pratique, est généralement identique à celle du saut suivant). L'entrée du paquet de mise à jour décrit un chemin dont la destination est indiquée dans l'entrée, dont l'interface de sortie est celle où a été reçue la mise à jour et dont le saut suivant et la source de l'information sont l'adresse de la passerelle qui a envoyé la mise à jour (la « source » S).

Au cours des étapes H et T, le processus de mise à jour décrit dans la figure 7 est planifié. Ce processus est exécuté une fois que tout le processus de la figure 5 est exécuté. Autrement dit, le processus de mise à jour décrit dans la figure 7 ne sera exécuté qu'une fois, même s'il a été déclenché à plusieurs reprises durant l'exécution de la figure 5. En outre, des précautions doivent être prises pour empêcher que des mises à jour soient émises trop fréquemment si le réseau change rapidement.

L'étape K s'exécute si la destination indiquée dans l'entrée actuelle du paquet de mise à jour existe déjà dans la table de routage. La nouvelle métrique composite calculée à partir des données du paquet de mise à jour est alors comparée à la meilleure métrique composite de la destination. Remarquez que la meilleure métrique composite n'est pas recalculée à ce moment, donc, si le chemin examiné est le même que celui qui est déjà dans la table de routage, ce test compare la nouvelle métrique à l'ancienne du même chemin.

L'étape L est exécutée pour les chemins qui sont moins bons que la meilleure métrique composite actuelle. Ceci inclut les nouveaux chemins qui sont moins bons que les chemins existants, ainsi que les chemins existants dont la métrique composite a augmenté. L'étape L vérifie si le nouveau chemin est acceptable. Remarquez que ce test met en œuvre le test pour vérifier si un nouveau chemin est assez bon pour être conservé et le test de l'empoisonnement de route. Pour être acceptable, la valeur de la latence doit être différente de la valeur spéciale qui indique qu'une destination est inatteignable (pour la mise en œuvre IP actuelle, tous les bits du champ de 24 bits doivent être des 1), et la métrique composite (calculée comme indiqué dans la figure 8) doit être acceptable. Pour déterminer si la métrique composite est acceptable, comparez-la avec les métriques composites de tous les autres chemins vers la destination. La variable M sera la valeur la plus basse de ces métriques composites. Le nouveau chemin est acceptable si sa métrique est inférieure à V x M, où V est la variance définie lors de l'initialisation de la passerelle. Si V = 1 (ce

qui est toujours vrai depuis la version 8.2 de Cisco), alors une métrique moins bonne que la métrique existante n'est pas acceptable. Il y a une exception à ceci : si le chemin existe déjà et que c'est le seul chemin vers la destination, le chemin sera conservé si la métrique n'a pas augmenté de plus de 10 % (ou quand le nombre de sauts n'a pas augmenté, si les mises en attente sont désactivées).

L'étape V est exécutée quand les nouvelles informations à propos d'un chemin indiquent que la métrique composite diminuera. Les métriques composites de tous les chemins vers la destination D sont comparées. Au cours de cette comparaison, la nouvelle métrique composite pour P est utilisée plutôt que celle figurant dans la table de routage. La métrique composite la plus basse M est calculée. Puis tous les chemins vers D sont examinés de nouveau. Si la métrique composite d'un des chemins est supérieure à M x V, ce chemin est retiré. V est la variance qui a été entrée lors de l'initialisation de la passerelle. (Dans la version 8.2 de Cisco, la variance est définitivement réglée à 1.)

Traitement périodique

Le processus décrit dans la figure 6 est déclenché chaque seconde. Il examine les différents minuteurs dans la table de routage pour voir si l'un d'eux a expiré. Ces minuteurs sont décrits ci-dessus.

Àl'étape U, le processus décrit dans la figure 7 est exécuté.

Les étapes R et S sont nécessaires parce que les métriques composites stockées dans la table de routage dépendent de l'occupation de canal qui change au fil du temps en fonction des mesures. L'occupation de canal est périodiquement recalculée à l'aide d'une moyenne mobile des mesures du trafic de l'interface. Si la valeur recalculée diffère de la valeur existante, toutes les métriques composites utilisant cette interface doivent être ajustées. Tous les chemins de la table de routage sont examinés. La métrique composite de tout chemin dont le saut suivant passe par l'interface « I » est recalculée. Ce recalcul est effectué avec l'équation 1 en utilisant comme occupation de canal la valeur la plus élevée stockée dans la table de routage comme élément de la métrique du chemin et l'occupation de canal nouvellement calculée de l'interface.

Génération des messages de mise à jour

La figure 7 décrit comment la passerelle génère les messages de mise à jour à envoyer aux autres passerelles. Un message distinct est créé pour chaque interface réseau de la passerelle. Ce message est ensuite envoyé à toutes les passerelles atteignables par l'interface (étape J). Pour ce faire, le message est généralement diffusé. Cependant, si la technologie réseau ou le protocole ne permet pas la diffusion, le message pourrait devoir être envoyé individuellement à chaque passerelle.

En général, le message est construit en ajoutant une entrée pour chaque destination dans la table de routage à l'étape G. Remarquez que les données de la destination et du chemin associées à chaque type de service doivent être utilisées. Dans le pire des cas, une nouvelle entrée est ajoutée à la mise à jour pour chaque destination de chaque type de service. Cependant, avant d'ajouter une entrée au message de mise à jour à l'étape G, les entrées déjà ajoutées sont analysées. Si la nouvelle entrée est déjà dans le message de mise à jour, elle ne sera pas ajoutée de nouveau. Une nouvelle entrée est un doublon d'une entrée existante quand les destinations et les passerelles du saut suivant sont les mêmes.

Pour des raisons de simplicité, le pseudocode omet que les messages de mise à jour d'IGRP ont

trois parties (interne, système et externe), ce qui signifie qu'il n'y a vraiment que trois boucles pour les destinations. La première n'inclut que les sous-réseaux du réseau auquel la mise à jour est envoyée. La deuxième inclut tous les réseaux importants (par exemple, ceux qui ne sont pas des sous-réseaux) qui ne sont pas désignés comme externes. La troisième inclut tous les réseaux importants qui sont désignés comme externes.

L'étape E met en application le test d'horizon partagé. Normalement, ce test échoue pour les routes dont le meilleur chemin passe par l'interface d'où la mise à jour est envoyée. Cependant, si la mise à jour est envoyée à une destination spécifique (par exemple, en réponse à une requête IGRP d'une autre passerelle ou dans le cadre d'« IGRP point à point »), le test d'horizon partagé échoue uniquement si le meilleur chemin est le même que cette destination (si l'adresse de la « source d'information » est la même que celle de la destination) et que l'interface de sortie est la même que celle qui a reçu la requête.

Calcul des informations de la métrique

La figure 8 décrit comment les informations de la métrique sont traitées à partir des messages de mise à jour reçus par la passerelle et comment elles sont générées pour les messages de mise à jour envoyés par la passerelle. Remarquez que l'entrée n'utilise qu'un chemin précis vers la destination. S'il y a plus d'un chemin vers la destination, le chemin dont la métrique composite est la plus basse est choisi. Si plusieurs chemins ont la métrique composite la plus basse, une règle arbitraire est utilisée pour briser l'égalité. (Pour la plupart des protocoles, cette règle est basée sur l'adresse de la passerelle du saut suivant.)

Figure 4 : Traitement des paquets entrants

```
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 de routage entrantes

```
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 : Génération de 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 du calcul de la métrique

Cette section décrit la procédure pour calculer les métriques et les nombres de sauts d'une mise à jour de routage entrante. La variable d'entrée de cette fonction est l'entrée vers une destination spécifique dans le paquet de mise à jour de routage. Le résultat est un vecteur de métriques qui peut servir à calculer une métrique composite et un nombre de sauts. Si ce chemin est ajouté à la table de routage, la totalité du vecteur des métriques sera entrée dans la table. Les paramètres de l'interface utilisés dans les définitions suivantes sont ceux définis lors de l'initialisation de la passerelle pour l'interface par laquelle la mise à jour de routage a été reçue, sauf l'occupation de canal et la fiabilité qui sont plutôt basées sur une moyenne mobile du trafic mesuré sur l'interface.

- Latence = latence des paquets + latence topologique de l'interface
- Bande passante = la plus grande valeur entre la bande passante du paquet et celle de l'interface
- Fiabilité = la plus petite valeur entre la fiabilité du paquet et celle de l'interface
- Occupation des canaux = la plus grande valeur entre l'occupation de canal du paquet et celle de l'interface(La plus grande valeur est utilisée pour la bande passante, car la métrique de

bande passante est stockée de façon inverse) Conceptuellement, nous voulons la valeur de bande passante la plus basse.) Remarquez que l'occupation de canal initiale du paquet doit être enregistrée, car elle sera nécessaire pour recalculer l'occupation de canal réelle quand l'occupation de canal de l'interface changera.

Les éléments suivants ne font pas partie du vecteur de la métrique, mais sont également conservés dans la table de routage comme caractéristiques du chemin :

- Nombre de sauts = le nombre de sauts du paquet.
- MTU = la plus petite valeur entre la MTU du paquet et celle de l'interface.
- Métrique composite distante = calculée à l'aide de l'équation 1 avec les valeurs de la métrique du paquet. C'est-à-dire que les éléments de la métrique sont ceux du paquet et ne sont pas mis à jour, comme indiqué ci-dessus. Évidemment, ils doivent être calculés avant que les ajustements indiqués ci-dessus ne soient effectués.
- Métrique composite = calculée à l'aide de l'équation 1 en utilisant les valeurs de la métrique calculées comme indiqué dans cette section.

Le reste de cette section décrit la procédure pour calculer les métriques et les nombres de sauts de la mise à jour de routage à envoyer.

Cette fonction détermine les informations de la métrique et le nombre de sauts à inclure dans le paquet de mise à jour sortant. Elle utilise un chemin spécifique vers une destination, s'il y a un chemin utilisable. S'il n'y a aucun chemin utilisable ou si tous les chemins sont en amont, la destination est désignée « 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 la mise en œuvre IP

Cette section décrit brièvement les formats de paquet utilisé par l'IGRP de Cisco. L'IGRP est envoyé à l'aide de datagrammes IP par le protocole IP 9 (IGP). Tout d'abord, il y a l'en-tête. Après l'en-tête IP, le paquet commence.

```
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 les messages de mise à jour, les informations de routage suivent immédiatement l'en-tête.

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

Le code d'opération peut être 1 pour une mise à jour ou 2 pour une requête.

Il indique le type de message. Les formats des deux types de messages se trouvent ci-dessous.

Edition est un numéro de série qui est incrémenté chaque fois qu'il y a un changement dans la table de routage. (Cela arrive quand les conditions sont réunies pour que le pseudocode plus haut déclenche une mise à jour de routage.) Le numéro de version permet aux passerelles d'éviter de traiter des mises à jour contenant des informations qu'elles ont déjà reçues. (Cette fonctionnalité n'est pas actuellement mise en œuvre. C'est-à-dire que le numéro de version est généré correctement, mais qu'il est ignoré en entrée. Comme il est possible que des paquets soient perdus, il n'est pas garanti que le numéro de version soit suffisant pour éviter le traitement en double. Il serait nécessaire de s'assurer que tous les paquets associés à la version ont été traités.)

Asystem est le numéro du système autonome. Dans la mise en œuvre de Cisco, une passerelle peut faire partie de plus d'un système autonome. Chacun de ses systèmes utilise son propre protocole IGRP. Conceptuellement, il y a des tables de routage distinctes pour chaque système autonome. Les routes qui arrivent par l'intermédiaire d'IGRP depuis un système autonome ne sont envoyées que dans les mises à jour pour ce système autonome. Ce champ permet à la passerelle de sélectionner quel ensemble de tables de routage elle doit utiliser pour traiter ce message. Si la passerelle reçoit un message IGRP concernant un système autonome pour lequel elle n'est pas configurée, elle l'ignorera. En fait, la mise en œuvre de Cisco permet aux informations de « filtrer » d'un système autonome à l'autre. Cependant, je considère que c'est un outil administratif et que ça ne fait pas partie du protocole.

Ninterior, *nsystem* et *nexterior indiquent le nombre d'entrées de chacune des trois sections des messages de mise à jour.* Ces sections ont été décrites plus haut. Il n'y a aucune démarcation entre les sections. Les premières entrées ninterior sont considérées comme internes, les entrées nsystem qui suivent sont considérées comme système et les entrées nexterior finales sont considérées comme externes.

Checksum est une somme de contrôle IP calculée à l'aide du même algorithme de somme de contrôle qu'UDP. La somme de contrôle est calculée à partir de l'en-tête IGRP et des informations de routage qui suivent. Le champ de somme de contrôle est mis à zéro lors du calcul de la somme de contrôle. La somme de contrôle n'inclut pas l'en-tête IP et il n'y a pas d'en-tête virtuel comme dans UDP et TCP.

Requêtes

Une requête IGRP demande au destinataire d'envoyer sa table de routage. Le message de requête ne contient qu'un en-tête. Seuls les champs de la version, du code d'opération et du système autonome sont utilisés. Tous les autres champs sont à zéro. On s'attend alors à ce que le destinataire envoie un message de mise à jour IGRP normal au demandeur.

Mises à jour

Un message de mise à jour IGRP contient un en-tête, suivi immédiatement des entrées de routage. Un datagramme peut contenir autant d'entrées que le permet sa capacité de 1500 bits (en incluant l'en-tête IP) Les déclarations de structure actuelles permettent jusqu'à 104 entrées.

S'il y a plus d'entrées à transmettre, plusieurs messages de mise à jour sont envoyés. Comme les entrées des messages de mise à jour sont traitées une à la fois, il n'y a aucun avantage à envoyer un seul message fragmenté plutôt que plusieurs messages indépendants.

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 en formats uchar[2] et uchar[3] sont simplement des entiers de 16 et de 24 bits, en ordre normal de réseau IP.

Le numéro indique la destination qui est décrite. Il s'agit d'une adresse IP. Pour économiser de l'espace, seuls les trois premiers octets de l'adresse IP sont donnés, sauf dans la section interne. Dans cette dernière, ce sont les trois derniers octets qui sont donnés. Pour des routes système et externes, aucun sous-réseau n'est possible, donc le dernier octet est toujours égal à zéro. Comme les routes internes sont toujours des sous-réseaux d'un réseau connu, le premier octet de ce réseau est fourni.

La latence est en unités de 10 microsecondes. Cela donne une plage de 10 microsecondes à 168 secondes, ce qui semble suffisant. Une latence dont tous les bits sont des 1 indique que le réseau est inaccessible.

La bande passante est une bande passante inverse en bits par seconde multipliée par un facteur de 1,0e10. La plage est de 1200 b/s à 10 Gb/s. (C'est-à-dire que si la bande passante est de N kb/s, le nombre utilisé sera 10 000 000/N.)

Le MTU est en octets.

La fiabilité est une fraction de 255. C'est-à-dire que 255 équivaut à 100 %.

La charge est aussi une fraction de 255.

Le nombre de sauts est tout simplement un nombre.

En raison des unités relativement ésotériques utilisées pour la bande passante et la latence, quelques exemples semblent nécessaires. Voici 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 de la métrique

Voici une description de la manière dont est réellement calculée la métrique composite 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