Groupe de travail Réseau
Request for Comments : 2091
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

G. Meyer, Shiva
S. Sherry, Xyplex
janvier 1997

Extensions déclenchées dans RIP pour la prise en charge de circuits à la demande

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document définit une modification qui peut être appliquée aux protocoles de diffusion des informations de l'algorithme Bellman-Ford (de vecteur de distance) - par exemple RIP IP, RIP Netware ou SAP Netware – qui rend possible leur fonctionnement sur des réseaux de données publics en mode connexion. Cette proposition présente un certain nombre d'avantages en matière d'efficacité sur la proposition Demande RIP de la (RFC1582).

Remerciements
Les auteurs tiennent à remercier Richard Edmonstone de Shiva, Joahanna Kruger de Xyplex, Steve Waters de DEC et Guenter Roeck de Conware pour les nombreux commentaires et suggestions qui ont amélioré ce travail.

Conventions
Les conventions de langage suivantes sont utilisées dans les éléments de spécification de ce document :
- DOIT – l'élément est une exigence absolue de la spécification. DOIT n'est utilisé que lorsque l'élément est en fait exigé pour l'interfonctionnement, et non pour essayer d'imposer une méthode particulière aux mises en œuvre lorsque elles ne sont pas exigées pour l'interopérabilité.
- DEVRAIT – l'élément devrait être suivi sauf circonstances. exceptionnelles.
- PEUT ou facultatif – l'élément est vraiment facultatif et peut être suivi ou ignoré selon les besoins de la mise en œuvre.

Les mots "devrait" et "peut" sont aussi utilisés en minuscules, dans leur sens le plus ordinaire.

Table des matières

1. Introduction

Les routeurs sont utilisés sur les réseaux en mode connexion, tels que les réseaux à commutation de paquets X.25 et les réseaux RNIS, pour permettre une connexité potentielle avec un grand nombre de destinations distantes. Les circuits sur le réseau de large zone (WAN, *Wide Area Network*) sont établis à la demande et sont libérés lorsque le trafic se calme. Selon l'application, la connexion entre deux sites quelconques pour des données d'utilisateur peut en fait être courte et relativement peu fréquente.

La diffusion périodique par des protocoles de diffusion d'informations d'algorithme Bellman-Ford (vecteur de distance) IP RIP [1], IP RIP V2 [2] ou Netware RIP et SAP [3] empêche généralement les circuits de WAN d'être fermés. Même sur des liaisons en point à point fixes, la surcharge de la transmission périodique de diffusions RIP – et encore plus de SAP - peut sérieusement perturber le transfert normal de données simplement par la quantité d'informations qui envahissent la ligne toutes les 30 ou 60 secondes.

Pour surmonter ces limitations, la présente spécification modifie les protocoles de vecteur de distance de façon à n'envoyer les informations sur le WAN que lorsque il y a eu une mise à jour à la base de données d'acheminement OU qu'un changement dans l'accessibilité d'un routeur de prochain bond est indiqué par la tâche qui gère les connexions sur le WAN.

Comme il n'est pas garanti que les datagrammes passent à travers de tous les supports du WAN, un système d'accusé de réception et de retransmission est nécessaire pour assurer la fiabilité.

Les protocoles fonctionnent sans modification sur les réseaux de zone locale (LAN) et interopèrent donc de façon transparente avec les mises en œuvre qui adhèrent à la spécification d'origine.

La présente proposition diffère conceptuellement de RIP à la demande [4] par ce qui suit :

- Si un routeur a échangé toutes les informations d'acheminement avec son partenaire et si des informations d'acheminement changent ensuite, seules les informations modifiées sont envoyées au partenaire.

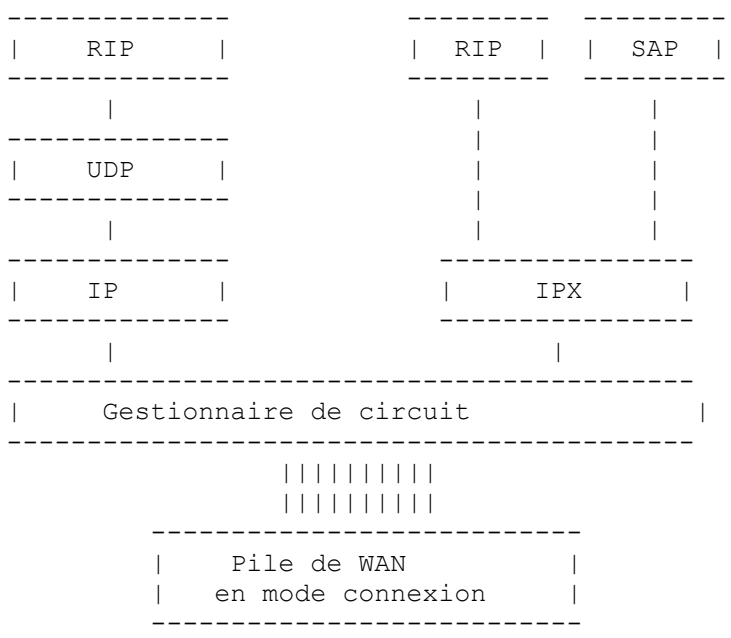
- Le receveur des chemins est capable d'appliquer immédiatement tous les changements dès réception des informations de son partenaire.

Ces différences conduisent à réduire encore le trafic d'acheminement et exigent aussi moins de mémoire que RIP à la demande [4]. RIP à la demande a aussi une limite supérieure de 255 fragments dans une mise à jour qui est relevée dans RIP déclenché (qui n'utilise pas la fragmentation).

2. Généralités

Les routeurs multi-protocoles sont utilisés sur les réseaux de large zone (WAN, *Wide Area Network*) en mode connexion, tels que les réseaux X.25 à commutation de paquets et les réseaux RNIS, pour interconnecter des LAN. En utilisant les propriétés de multiplexage de la technologie du WAN sous-jacent, plusieurs LAN peuvent être interconnectés simultanément à travers une seule interface physique sur le routeur.

Un gestionnaire de circuit fournit une interface entre les couches de réseau sans connexion, IP et IPX, et le WAN en mode connexion, X.25, RNIS, etc. La Figure 1 illustre une pile schématique représentant les relations entre les protocoles d'acheminement, les couches réseau, le gestionnaire de circuit et le WAN en mode connexion.



Un gestionnaire de circuit WAN prendra en charge divers protocoles de couche réseau sur son interface supérieure. Sur son interface inférieure, il peut prendre en charge un ou plusieurs sous-réseaux. Un sous-réseau peut prendre en charge un certain nombre de circuits virtuels.

Figure 1 :Pile représentative d'un routeur multi-protocoles

Le routeur a un tableau de traduction qui met en rapport l'adresse de couche réseau du routeur de prochain bond avec l'adresse physique utilisée pour établir un circuit virtuel (VC) avec lui.

Le gestionnaire de circuit prend les datagrammes des protocoles de couche réseau sans connexion et (si il n'en est pas de disponible actuellement) ouvre un VC pour le routeur de prochain bond. Un VC peut porter tout le trafic entre deux routeurs de point d'extrémité pour un certain protocole de couche réseau (ou avec l'encapsulation appropriée pour tous les protocoles de couche réseau). Un temporisateur d'inactivité (ou quelque autre mécanisme) est utilisé pour clore le VC lorsque les datagrammes cessent d'arriver au gestionnaire de circuit.

Si le gestionnaire de circuit a des données à transmettre (que ce soient des données d'utilisateur OU une mise à jour d'acheminement) et si il échoue à obtenir un VC, il va informer l'application d'acheminement que la destination est injoignable (circuit défaillant). Le gestionnaire de circuit est alors supposé effectuer ce qui est nécessaire pour restaurer la liaison. Une fois qu'il a réussi, il en informe l'application d'acheminement (circuit rétabli).

Dans RIP déclenché, les mises à jour d'acheminement ne sont transmises sur le WAN que lorsque elles sont requises :

1 Lorsque a été reçue une demande spécifique de mise à jour d'acheminement.
2 Lorsque la base de données d'acheminement est modifiée par de nouvelles informations provenant d'une autre interface.
3 Lorsque le gestionnaire de circuit indique qu'une destination a changé de l'état injoignable (circuit défaillant) à celui d'accessible (circuit restauré).
4 Et aussi lorsque une unité est mise sous tension pour s'assurer qu'au moins une mise à jour est envoyée. Cela peut être vu comme une transition d'un circuit défaillant à un circuit actif. Cela PEUT contenir des chemins ou services, et c'est utilisé pour purger les chemins ou services de la base de données de l'homologue.

Dans les cas 1, 3 et 4, tout le contenu de la base de données est envoyé. Dans le cas 2, seuls les derniers changements sont envoyés.

À cause de la non fiabilité inhérente d'un système fondé sur le datagramme, aussi bien les demandes que les réponses d'acheminement exigent un accusé de réception, et la retransmission dans le cas de non réception d'un accusé de réception.

3. Base de données d'acheminement

Les entrées dans la base de données d'acheminement peuvent être permanentes ou temporaires. Les entrées apprises de diffusions sur des LAN sont temporaires. Elles vont se périmer si elles ne sont pas rafraîchies périodiquement par de nouvelles diffusions.

Les entrées apprises d'une réponse déclenchée sur le WAN sont "permanentes". Elles NE DOIVENT PAS être périmées dans le cours normal des événements. Certains événements peuvent causer l'expiration de ces chemins.

3.1 Présomption d'accessibilité

Si une mise à jour d'acheminement est reçue d'un routeur de prochain bond sur le WAN, les entrées dans la mise à jour sont ensuite toujours considérées comme accessibles, jusqu'à preuve du contraire :

- Si dans le cours normal de l'acheminement des datagrammes, le gestionnaire de circuit échoue à établir une connexion avec le routeur de prochain bond, il notifie à l'application d'acheminement que le routeur de prochain bond n'est pas accessible par un message de circuit interne.

  Les entrées de base de données sont d'abord marquées comme temporaires et vieillissent normalement ; certaines mises en œuvre peuvent choisir d'omettre cette étape initiale de vieillissement. L'application d'acheminement marque alors les entrées appropriées de la base de données comme injoignables pour une période d'attente (le temporisateur d'attente RIP normal de 120 secondes).

- Si le gestionnaire de circuit est ensuite capable d'établir une connexion avec le routeur de prochain bond, il va notifier à l'application d'acheminement que le routeur de prochain bond est accessible par un message sur un circuit interne.

  L'application d'acheminement va alors échanger des messages avec le routeur de prochain bond de façon à réinitialiser leurs bases de données d'acheminement respectives avec des informations à jour.

Le routeur de prochain bond peut aussi être marqué comme inaccessible si un nombre excessif de retransmissions d'une mise à jour restent sans accusé de réception (voir au paragraphe 6.3).

Le traitement des messages sur le circuit montant et sur le circuit descendant exige que le gestionnaire de circuits prenne la responsabilité de l'établissement (ou du rétablissement) de la connexion lorsque un routeur de prochain bond devient inaccessible. Une description des processus qu'adopte le gestionnaire de circuits pour effectuer cette tâche sort du domaine d'application du présent document.

3.2 Chemins de remplacement

Une exigence de l'utilisation de RIP déclenché pour propager les informations d'acheminement est qu'AUCUNE information d'acheminement ne soit jamais perdue ou éliminée. Cela signifie que tous les chemins de remplacement DEVRAIENT être conservés.

Il est possible de fonctionner sur un sous-ensemble de tous les chemins de remplacement, mais cela ajoute de la complexité au protocole – ce qui n'est pas couvert par le présent document.

3.3 Horizon partagé avec inversion empoisonnée

Les règles de l'horizon partagé avec inversion empoisonnée DOIVENT être utilisées pour déterminer si et/ou comment un chemin est annoncé sur une interface fonctionnant avec ce protocole.

L'horizon partagé consiste à omettre les chemins appris d'un homologue lors du renvoi de mises à jour à cet homologue. Avec l'inversion empoisonnée, au lieu d'omettre ces chemins, ils sont annoncés comme inaccessibles (en réglant la métrique à l'infini).

Un chemin n'est empoisonné que si il est le meilleur chemin (plutôt qu'un chemin de remplacement inférieur) dans la base de données.

L'inversion empoisonnée est nécessaire parce que un routeur peut recevoir l'annonce d'un chemin pour un réseau vers son partenaire puis apprendre ultérieurement un meilleur chemin pour le même réseau de la part du partenaire. Sans l'inversion empoisonnée, le partenaire ne saura pas qu'il faut éliminer le chemin inférieur appris du premier routeur.

3.4 Gestion des mises à jour d'acheminement

La base de données d'acheminement DEVRAIT être considérée comme étant une séquence d'éléments ordonnés selon l'heure de leur dernière mise à jour. Si il y a un changement du meilleur chemin (c'est-à-dire, si un nouveau chemin est ajouté ou si la métrique d'un chemin a changé) le chemin est réordonné et reçoit un nouveau numéro de séquence plus élevé.

L'envoi de mises à jour à un homologue consiste à parcourir la base de données de la plus ancienne entrée à l'entrée la plus récente. Une fois qu'une entrée a été envoyée et qu'on en a reçu un accusé de réception, elle n'est généralement jamais envoyée à nouveau. Lorsque de nouvelles informations d'acheminement arrivent, seules les nouvelles informations sont envoyées.

3.5 Retransmissions

Le traitement de la retransmission des mises à jour est le plus simple si les mises à jour se restreignent à n'avoir jamais plus d'une mise à jour sans accusé de réception en cours - "un paquet en cours". Une copie du paquet de mise à jour peut être conservée et retransmise jusqu'à son accusé de réception – et ensuite les paquets de mise à jour suivants sont envoyés jusqu'à ce que la totalité de la base de données (actuelle) ait été envoyée et ait été acquittée.

Les choses deviennent plus compliquées si plusieurs paquets sont envoyés en succession rapide sans attendre d'accusé de réception entre les paquets - "plusieurs paquets en cours":

- Si les paquets arrivent en désordre, ils peuvent corrompre la base de données de l'homologue. Si la couche de liaison des données sous-jacente regroupe plusieurs VC, elle DOIT garantir de ne pas réordonner les datagrammes.

- Si les éléments qui constituent un paquet qui exige la retransmission changent à cause d'une altération de la base de données, des informations périmées incorrectes pourraient être envoyées (et de nouvelles informations pourraient remplacer d'anciennes informations).

Pour se garder contre cela lors de la "retransmission" d'un paquet lorsque la base de données est en flux, le paquet DOIT être recréé à partir de la base de données pour ne contenir que le sous-ensemble de chemins qui s'applique en fait. Et si aucun des chemin ne s'applique plus, rien ne sera "retransmis".

Pour simplifier la mise en œuvre, nous conseillons d'avoir seulement un paquet en cours. Cependant, si le "délai d'aller-retour" pour une réponse et son accusé de réception est assez long, cela peut retarder de façon significative de grosses mises à jour. Voir à l'Appendice A une explication de la complexité supplémentaire de la gestion de plusieurs paquets en cours.

4. Nouveaux types de paquets

Pour prendre en charge les mises à jour déclenchées, trois nouveaux types de paquet DOIVENT être pris en charge. Pour RIP IP version 1 [1] et RIP IP version 2 [2] ils sont identifiés par les valeurs du champ Commande suivantes :

- 9 – Demande de mise à jour
- 10 – Réponse de mise à jour
- 11 – Accusé de réception de mise à jour

Pour RIP Netware et SAP [3] le champ équivalent pour distinguer les types de paquet est appelé Opération et il prend les mêmes valeurs.

Ces types Commande et Opération exigent l'ajout d'un en-tête Mise à jour de 4 octets. Les trois types de paquet contiennent une version qui DOIT être 1. La Réponse et l'Accusé de réception de mise à jour ont aussi un numéro de séquence et un fanion Purge.

4.1 Demande de mise à jour

La Demande de mise à jour a la valeur de Commande/Opération de 9.

C'est une demande au système homologue qu'il envoie TOUS les éléments appropriés de sa base de données d'acheminement. Elle est retransmise à intervalles périodiques (toutes les 5 secondes) jusqu'à ce qu'un message Réponse de mise à jour soit reçu avec le fanion Purge établi.

Une Demande de mise à jour est transmise dans les circonstances suivantes :
- o D'abord, lorsque le routeur est mis sous tension.
- o Ensuite, lorsque le gestionnaire du circuit indique qu'une destination a été dans un état injoignable (circuit mort) et passe à l'état accessible (circuit actif).

Une Demande de mise à jour peut aussi être envoyée à d'autres moments pour compenser l'élimination d'informations d'acheminement non optimales ou si une Réponse de mise à jour continue de n'avoir pas d'accusé de réception (voir au paragraphe 6.3).

4.2 Réponse de mise à jour

La Réponse de mise à jour a la valeur de Commande/Opération de 10.

C'est un message qui contient zéro, un ou plusieurs chemins dans une mise à jour. Il est retransmis à des intervalles périodiques jusqu'à ce qu'un Accusé de réception de mise à jour soit reçu.

Un message Réponse de mise à jour DOIT être envoyé :
- o En réponse à une Demande de mise à jour. La Réponse de mise à jour DOIT avoir le fanion Purge établi. D'autres Réponses de mise à jour NE DEVRAIENT PAS être envoyées tant qu'un Accusé de réception de mise à jour n'a pas été reçu pour accuser réception du fanion Purge.

  Le reste de la base de données DOIT alors être envoyé comme une série de Réponses de mise à jour avec le fanion Purge NON établi.

- o Une Réponse de mise à jour avec le fanion Purge DOIT aussi être envoyée à la mise sous tension pour purger le tableau d'acheminement de l'homologue appris de la précédente session. Cette Réponse de mise à jour NE DEVRAIT PAS contenir de chemins. Cela évite toute possibilité qu'un accusé de réception soit reçu pour une réponse envoyée AVANT le redémarrage de l'unité, ce qui serait cause de confusion sur les chemins qui font l'objet de l'accusé de réception.

Les messages Réponse de mise à jour continuent d'être envoyés chaque fois qu'il y a des informations d'acheminement fraîches à propager.

Chaque nouvelle Réponse de mise à jour reçoit un numéro de séquence différent. Le numéro de séquence n'a de signification que pour l'envoyeur de la Réponse de mise à jour. La même Réponse de mise à jour envoyée à des homologues différents PEUT avoir un numéro de séquence différent.

Un paquet Réponse de mise à jour avec le fanion Purge établi DOIT être envoyé à un homologue :
- o À la mise sous tension.
- o En réponse à un paquet Demande de mise à jour.
- o Après une transition d'un état circuit mort à l'état circuit actif.

Après l'envoi d'une purge de mise à jour, la base de données complète DOIT être envoyée à la suite.

4.3 Accusé de réception de mise à jour

L'accusé de réception de mise à jour a la valeur de Commande/Opération de 11.

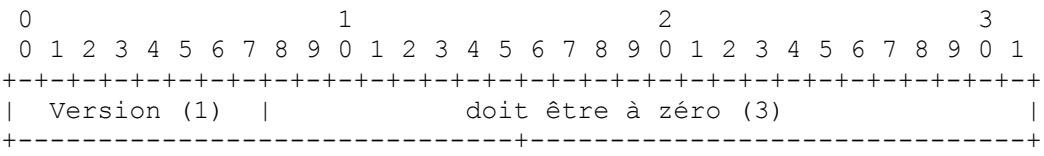
C'est un message envoyé en réponse à chaque paquet Réponse de mise à jour reçu. Si le paquet Réponse de mise à jour a le fanion Purge établi, le paquet Accusé de réception de mise à jour devrait l'avoir aussi.

5. Formats de paquet

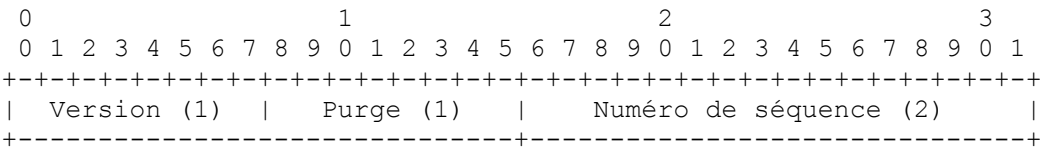
5.1 En-tête de mise à jour

Pour prendre en charge le mécanisme décrit dans la présente proposition, le format de paquet pour RIP version 1 [1], RIP version 2 [2], RIP Netware et SAP [3], est modifié pour inclure un petit en-tête supplémentaire quand on utilise les commandes Demande de mise à jour (9), Réponse de mise à jour (10) et Accusé de réception de mise à jour (11). Les commandes sont appelées Opérations dans Netware.

Demande de mise à jour (9):



Réponse de mise à jour (10) et Accusé de réception de mise à jour (11):



En-têtes de mise à jour de quatre octets, chaque pas représente un bit. Tous les champs sont codés dans l'ordre des octets du réseau (gros boutien).

Figure 2 : En-têtes de mise à jour

La version DOIT être 1 dans tous les en-têtes. Tout paquet reçu avec une version différente DOIT être éliminé en silence.

Le numéro de séquence DOIT être incrémenté chaque fois qu'un nouveau paquet Réponse de mise à jour est envoyé sur le WAN. Le numéro de séquence est inchangé pour les retransmissions. Le numéro de séquence revient à zéro à 65 535.

Purge est réglé à 1 dans une Réponse de mise à jour si l'homologue est requis de commencer à périmer ses entrées – autrement, il est mis à zéro. Toutes les autres valeurs DOIVENT être éliminées en silence.

L'homologue retourne un Accusé de réception de mise à jour contenant les mêmes Numéro de séquence et Purge.

5.2 Protocole d'informations d'acheminement IP version 1

IP RIP [1] est un protocole fondé sur UDP qui généralement envoie et reçoit des datagrammes sur le numéro d'accès UDP 520.

Pour prendre en charge le mécanisme décrit dans cette proposition, le format de paquet pour RIP version 1 [1] est modifié lorsque on utilise les commandes Demande de mise à jour (9), Réponse de mise à jour (10) et Accusé de réception de mise à jour (11). Voir la Figure 3.

5.3 Protocole d'informations d'acheminement IP version 2

IP RIP version 2 [2] est une amélioration de IP RIP version 1 qui permet aux mises à jour RIP d'inclure des informations de sous-réseau.

Pour prendre en charge le mécanisme décrit dans cette proposition, le format de paquet pour RIP version 2 [2] est modifié lorsque on utilise les commandes Demande de mise à jour (9), Réponse de mise à jour (10) et Accusé de réception de mise à jour (11). Voir la Figure 4.

5.4 Protocole d'informations d'acheminement Netware

Netware [3] prend en charge un mécanisme qui permet aux routeurs sur un internet d'échanger des informations d'acheminement en utilisant le Protocole d'informations d'acheminement (RIP) qui fonctionne sur le protocole d'échange de paquet Internet (IPX, *Internetwork Packet Exchange*) en utilisant le numéro de prise 453h.

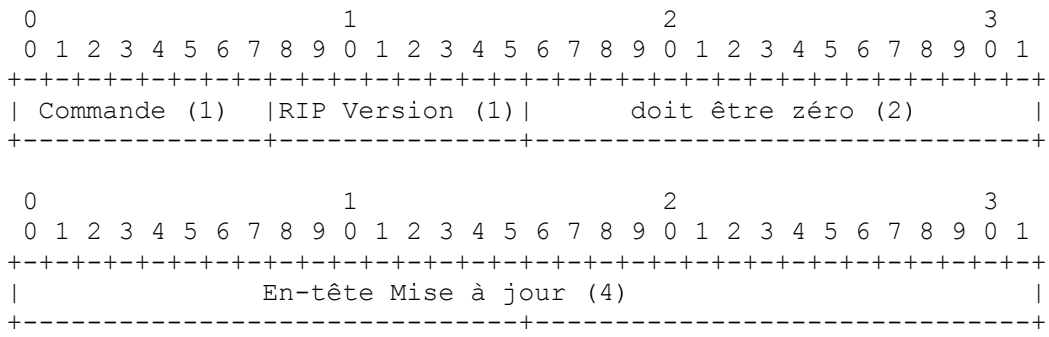
Pour prendre en charge le mécanisme décrit dans cette proposition, le format de paquet pour Novell RIP [3] est modifié quand on utilisé les opérations Demande de mise à jour (9), Réponse de mise à jour (10) et Accusé de réception de mise à jour (11). Voir la Figure 5.

5.5 Protocole d'annonce de service Netware

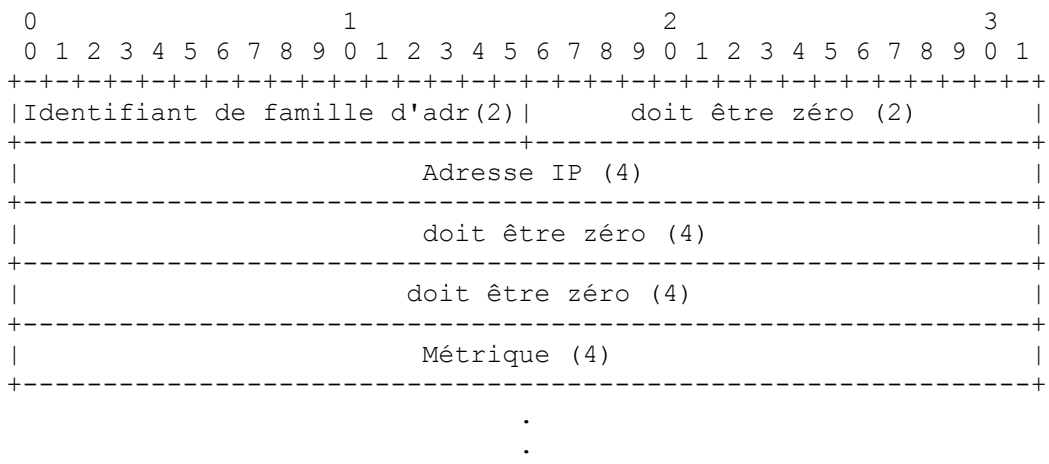
Netware [3] prend aussi en charge un mécanisme qui permet aux serveurs sur un internet d'annoncer leurs services par leurs

noms et types en utilisant le protocole d'annonce de service (SAP, *Service Advertising Protocol*) qui fonctionne avec le protocole d'échange de paquets Internet (IPX) en utilisant le numéro de prise 452h. SAP fonctionne sur des principes similaires à ceux de RIP. Les routeurs agissent comme des agents SAP, collectant les informations de service provenant de différents réseaux et les relayant aux parties intéressées.

Pour prendre en charge le mécanisme décrit dans cette proposition, le format de paquet pour le SAP de Novell [3] est modifié lors de l'utilisation des opérations Demande de mise à jour (9), Réponse de mise à jour (10) et Accusé de réception de mise à jour (11). Voir la Figure 6.



La Réponse de mise à jour a alors jusqu'à 25 entrées d'acheminements (chacune de 20 octets) :

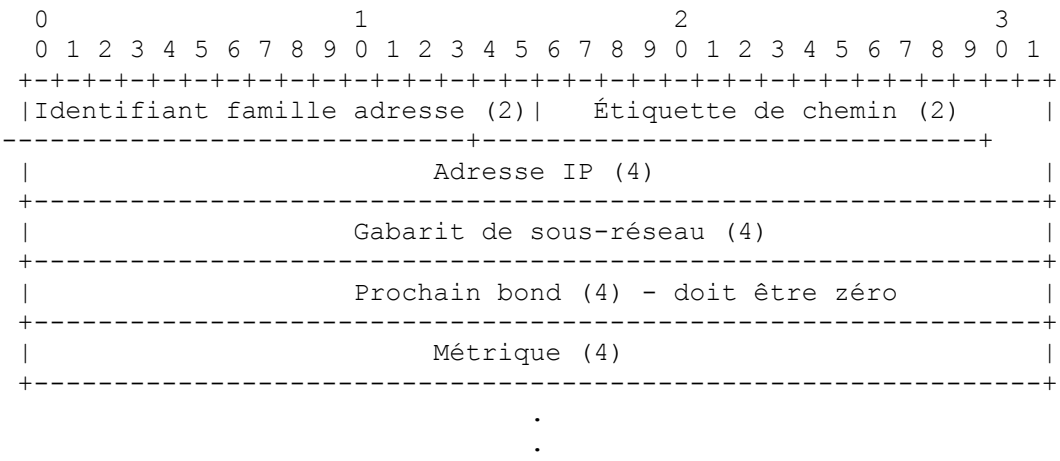


Format d'un datagramme RIP IP en octets, chaque espace représentant un bit. Tous les champs sont codés dans l'ordre des octets du réseau (gros boutien).

Les quatre octets de l'en-tête Mise à jour sont inclus dans les paquets de Demande de mise à jour (Commande 9), Réponse de mise à jour (10) et Accusé de réception de mise à jour (11). Ils ne sont pas présents dans les types de paquet dans la spécification RIP version 1 d'origine.

Figure 3 : Format de paquet IP RIP version 1

La Réponse de mise à jour a alors jusqu'à 25 entrées d'acheminements (chacune de 20 octets):

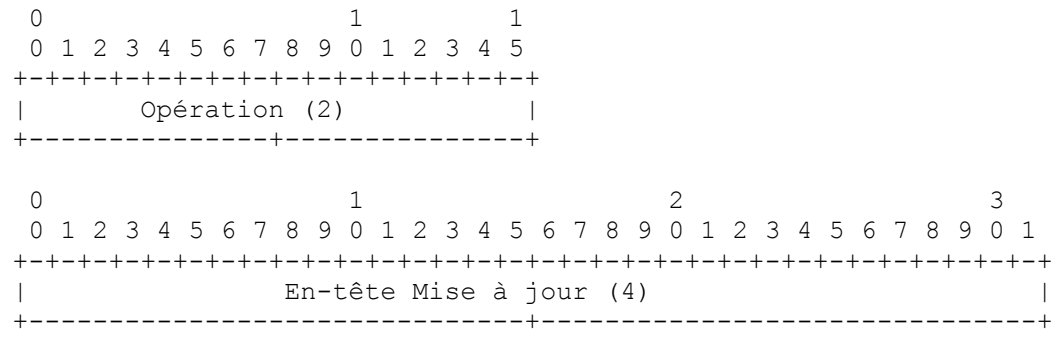


Format d'un datagramme RIP IP version 2 en octets, chaque espace numéroté représentant un bit. Tous les champs sont codés dans l'ordre des octets du réseau (gros boutien).

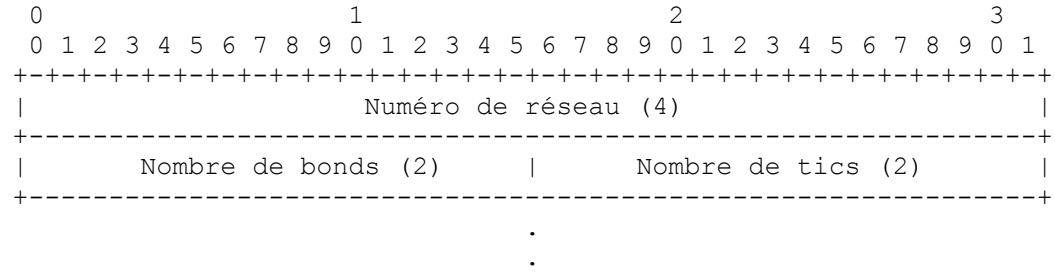
Les quatre octets de l'en-tête Mise à jour sont inclus dans les paquets de Demande de mise à jour (Commande 9), Réponse de mise à jour (10) et Accusé de réception de mise à jour (11). Ils ne sont pas présents dans les types de paquet dans la spécification RIP version 2 d'origine.

Prochain bond DOIT être zéro, car RIP déclenché NE PEUT PAS annoncer de chemin au nom de routeurs d'autres WAN. Si l'authentification est utilisée, elle suit immédiatement l'en-tête Mise à jour.

Figure 4 : Format de paquet RIP IP version 2



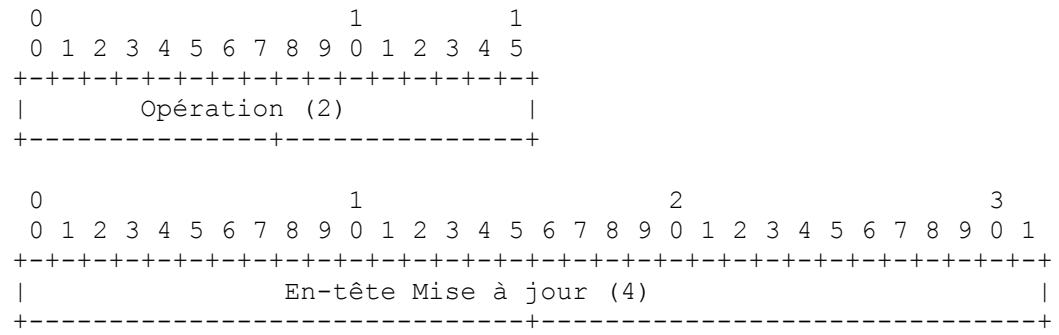
Réponse de mise à jour a alors jusqu'à 50 entrées d'acheminement (chacune de 8 octets):



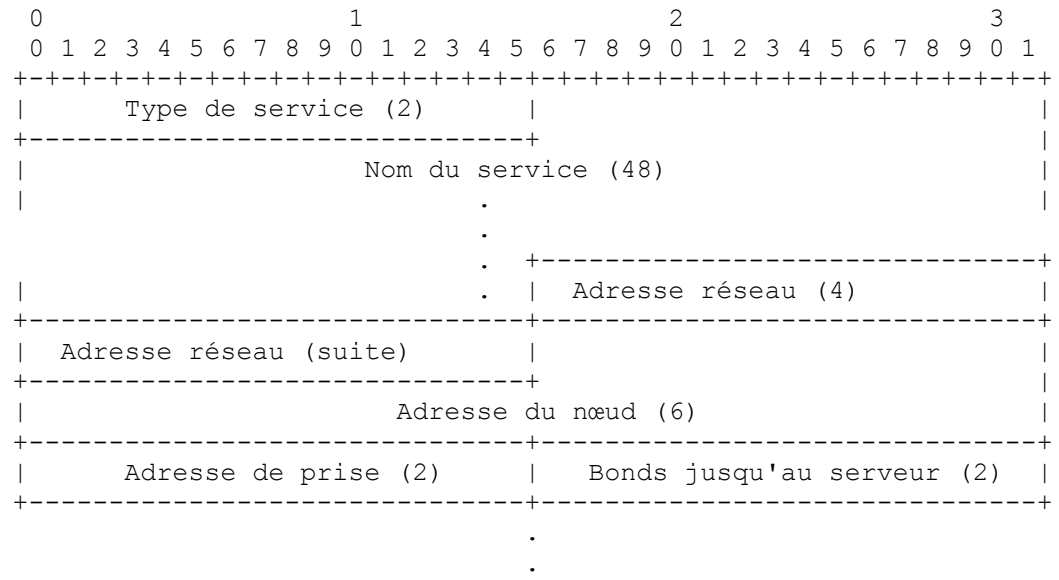
Format d'un datagramme RIP Netware en octets, chaque espace numéroté représentant un bit. Tous les champs sont codés dans l'ordre des octets du réseau (gros boutien).

Les quatre octets de l'en-tête Mise à jour sont inclus dans les paquets de Demande de mise à jour (Opération 9), Réponse de mise à jour (10) et Accusé de réception de mise à jour (11). Ils ne sont pas présents dans les types de paquet dans la spécification RIP Novell d'origine

Figure 5 : Format de paquet RIP Netware



Réponse de mise à jour a alors jusqu'à huit entrées de service (chacune de 64 octets):



Format d'un datagramme SAP Netware en octets, chaque espace numéroté représentant un bit. Tous les champs sont codés dans l'ordre des octets du réseau (gros boutien).

Les quatre octets de l'en-tête Mise à jour sont inclus dans les paquets de Demande de mise à jour (Opération 9), Réponse de mise à jour (10) et Accusé de réception de mise à jour (11). Ils ne sont pas présents dans les types de paquet dans la spécification SAP Netware d'origine.

Figure 6 : Format de paquet SAP Netware

6. Temporisateurs

Trois temporisateurs sont mis en œuvre pour traiter le mécanisme de mise à jour déclenchée :
- o temporisateur de base de données.
- o temporisateur de garde.
- o temporisateur de retransmission.

Un temporisateur facultatif de sur-souscription PEUT aussi être mis en œuvre.

6.1 Temporisateur de base de données

Les chemins appris par une Réponse de mise à jour sont normalement considérés comme permanents.

Lorsque est reçue une Réponse de mise à jour avec le fanion Purge établi, tous les chemins appris de ce routeur de prochain bond devraient commencer leur temporisation comme si ils venaient d'être appris d'une Réponse conventionnelle (Commande 2).

En fait chaque chemin existe pendant que le temporisateur de l'entrée de la base de données (normalement 180 secondes)

est en cours et il est annoncé sur les autres interfaces comme si il était toujours présent. Le chemin est alors annoncé comme injoignable lorsque le temporisateur de garde suivant est admis à arriver à expiration.

6.2 Temporisateur de garde

Un temporisateur de garde de 120 secondes est lancé sur un chemin :
- o lorsque le temporisateur de la base de données pour le chemin expire,
- o lorsque un chemin précédemment accessible devient injoignable dans une réponse entrante,
- o lorsque une annonce de circuit mort est reçue du gestionnaire de circuit.

Lorsque le temporisateur de garde fonctionne, les chemin sont annoncés comme injoignables sur les autres interfaces.

Lorsque le temporisateur de garde arrive à expiration, le chemin PEUT être supprimé de la base de données POURVU QUE son inaccessibilité ait été bien propagée à toutes les destinations du WAN, ou que les destinations restantes du WAN soient dans un état de circuit mort. Si un chemin ne peut pas être supprimé lorsque le temporisateur de garde arrive à expiration, il PEUT être supprimé ensuite lorsque chacun des homologues est soit à jour, soit est dans l'état de circuit mort.

Si le temporisateur de garde est déjà en cours, il N'EST PAS remis à zéro par un événement qui le lancerait.

6.3 Temporisateur de retransmission

La tâche d'acheminement fait fonctionner un temporisateur de retransmission :

- o Un paquet Demande de mise à jour est retransmis périodiquement jusqu'à réception d'un paquet Purge de mise à jour. Un paquet Purge de mise à jour est un paquet Réponse de mise à jour avec le champ Purge établi. Il n'a pas besoin de contenir de chemin.

- o Un paquet Réponse de mise à jour est retransmis périodiquement jusqu'à réception d'un paquet Accusé de réception de mise à jour, contenant le même numéro de séquence.

Avec un temps d'établissement de l'ordre de une seconde sur le WAN, une valeur de cinq secondes pour le temporisateur de retransmission est appropriée.

Pour se prémunir contre les défaillances du gestionnaire de circuit, une limite DEVRAIT être mise au nombre de retransmissions. Si aucune réponse n'a été reçue après une durée configurable (disons 180 secondes) les chemins via le routeur de prochain bond sont marqués comme injoignables, le temporisateur de garde est lancé, et l'entrée est annoncée comme injoignable sur les autres interfaces.

Le routeur de prochain bond peut alors être interrogé avec des Demandes de mise à jour à une fréquence réduite. Un intervalle d'interrogation convenable serait de l'ordre de quelques minutes plutôt que de quelques secondes. Autrement, une Demande de mise à jour pourrait être initiée par une action administrative. Lorsque une réponse sera reçue, les routeurs devraient effectuer un échange complet d'informations d'acheminement.

6.4 Temporisateur de sur souscription

La sur-souscription est lorsque il y a plus de routeurs de prochain bond qui envoient des mises à jour sur le WAN qu'il n'y a de canaux. Par exemple, trois routeurs de prochain bond sont accédés par une interface RNIS au débit de base (BRI, *Basic Rate Interface*) qui ne peut prendre en charge que deux appels simultanément.

Pour éviter une oscillation de chemin, les routes NE PEUVENT PAS être marquées comme injoignables immédiatement en recevant un message circuit mort du gestionnaire de circuit. Une temporisation PEUT être utilisée pour retarder le marquage des chemins inaccessibles pendant suffisamment longtemps pour permettre que les appels soient "multiplexés en répartition temporelle" sur les canaux disponibles. Une temporisation de la longueur de la temporisation de chemin RIP régulière de 180 secondes PEUT convenir. En général, plus la sur-souscription est importante, plus la temporisation devrait être longue.

Les mises en œuvre qui souhaitent prendre en charge la sur-souscription peuvent mettre le délai en place au sein du gestionnaire de circuits ou au sein de l'application d'acheminement.

Si le délai est mis en œuvre au sein de l'application d'acheminement, les entrées d'acheminement NE DOIVENT PAS commencer la temporisation durant le délai. Cela permet au message qui remonte le circuit d'être ignoré si la temporisation n'est pas encore arrivée à expiration après avoir reçu le message qui descend le circuit. Cela évite toute confusion si l'homologue avait précédemment produit une commande Purge de chemin et se trouve engagé dans une mise à jour.

7. Considérations pour la sécurité

On exige du gestionnaire de circuits qu'ils possède une liste des adresses physiques pour lui permettre d'établir un appel au routeur de prochain bond. Le gestionnaire de circuit DEVRAIT ne permettre d'accepter des appels entrants que de cette liste bien définie de routeurs.

Il y aura ailleurs dans le système un ensemble de couples d'adresse logiques et physiques pour permettre aux protocoles réseau de fonctionner sur le circuit correct. Cela peut être un tableau de recherche, ou dans certaines instances il peut y avoir un algorithme de conversion entre les deux adresses.

La tâche d'acheminement (ou d'annonce de service) DOIT être approvisionnée avec une liste d'adresses logiques auxquelles sont à envoyer les mises à jour déclenchées sur le WAN. La liste PEUT être un sous-ensemble de la liste des routeurs de prochain bond conservée par le gestionnaire de circuits.

RIP version 2 permet aussi l'authentification des paquets de RIP déclenché.

Appendice A Suggestion de mise en œuvre

La présente section suggère une façon de structurer la base de données pour traiter RIP déclenché.

Chaque entrée de la base de données reçoit un numéro unique de chemin. Chaque fois que change un meilleur chemin pour un réseau, un numéro de chemin global est incrémenté et le chemin changé reçoit le nouveau numéro de chemin. Noter que ce numéro de chemin est complètement interne au routeur et n'a pas de conséquence sur le numéro de séquence envoyé dans les Réponses de mise à jour envoyées à l'homologue.

La taille du numéro de chemin devrait être assez grande pour n'avoir pas besoin de revenir à zéro – ou les chemins devraient pouvoir être renumérotés avant que cela devienne un problème. Le renumérotage exige que l'environnement de la base de données soit stable (Les Réponses de mise à jour ne sont pas mises en file d'attente en attendant leur Accusé de réception).

Il est probablement plus facile de gérer les chemins si ils sont aussi chaînés ensemble en utilisent un pointeur sur une entrée postérieure (et éventuellement aussi un pointeur sur une entrée antérieure) qui va refléter le numéro/âge du chemin.

Effectuer une mise à jour complète consiste alors à parcourir les chemins du plus ancien au plus récent et à les envoyer dans les Réponses de mise à jour. Les changements ultérieurs à la base de données sont traités comme des envois des seules entrées modifiées (de l'ancienne plus ancienne à la plus nouvelle nouvelle).

Lorsque il est permis d'avoir plusieurs paquets en cours, il faut faire attention aux retransmissions. Une "retransmission" de Réponse de mise à jour PEUT être différente de l'originale. Lors de la transmission d'une séquence de Réponses de mise à jour, chaque paquet de réponse contient un numéro de chemin qui est un entier qui représente une série de chemins qui ont des numéros de chemin consécutifs. Si nous considérons l'envoi de trois Réponses de mise à jour avec les numéros de séquence 10, 11 et 12, chacune contenant dix chemins :

Numéro de séquence	Chemins représentés par les numéros de chemin
10	101, 102, 103, 104, 105, 106, 107, 108, 109, 110
11	111, 112, 113, 114, 115, 116, 117, 118, 119, 120
12	121, 122, 123, 124, 125, 126, 127, 128, 129, 130

Si ces Réponses de mise à jour ne sont pas acquittées, mais si pendant ce temps la base de données d'acheminement a subi des changements et les chemins représentés par les numéros 104, 112 - 116 et 127 ont été changés et ont reçu les nouveaux numéros de chemin 131 - 137, la retransmission va ressembler à :

Numéro de séquence	Chemins représentés par les numéros de chemin
10	101, 102, 103, 105, 106, 107, 108, 109, 110
11	111, 117, 118, 119, 120
12	121, 122, 123, 124, 125, 126, 128, 129, 130
13	131, 132, 133, 134, 135, 136, 137

Pour effectuer une retransmission, il est TRÈS IMPORTANT que la retransmission ne contienne que le SOUS-ENSEMBLE de numéros de chemins qui s'appliquent actuellement. Si il n'y a PAS de chemin convenable à envoyer, il n'est pas nécessaire d'envoyer une retransmission vide.

Une autre stratégie de "retransmission" est de toujours utiliser des numéros de séquence différents lors de nouveaux envois de mises à jour. Considérons la transmission de paquets avec des numéros de séquence de 10 à 20 – et des réponses qui sont reçues de tous les paquets sauf ceux qui ont les numéros de séquence 14 et 17. Dans ce cas, seules les données dans les paquets 10 à 13 peuvent être considérées comme ayant été acquittées. Les données à partir du paquet 14 DOIVENT être envoyées à nouveau et recevoir un numéro de séquence commençant à 21.

Références

[1] C. Hedrick, "Protocole d'informations d'acheminement", RFC1058, juin 1988. *(Historique)*

[2] G. Malkin, "RIP v2, portage d'informations supplémentaires", RFC1723, novembre 1994. *(remplacée par RFC 2453)*

[3] Novell Incorporated., "IPX Router Specification", Version 1.20, octobre 1993.

[4] Meyer. G., "Extensions to RIP to Support Demand Circuits", Spider Systems, février 1994.

Adresse des auteurs

Gerry Meyer
Shiva
Stanwell Street
Edinburgh EH6 5NG
Scotland, UK
téléphone : (UK) 131 554 9424
fax : (UK) 131 467 7749
mél : gerry@europe.shiva.com

Steve Sherry
Xyplex
295 Foster St.
Littleton, MA 01460
téléphone : (US) 508 952 4745
fax : (US) 508 952 4887
mél : shs@xyplex.com