Groupe de travail Réseau
Request For Comments : 827
Traduction Claude Brière de L'Isle

Eric C. Rosen
Bolt Beranek and Newman Inc.
octobre 1982

Protocole de passerelle extérieure (EGP)

Il est proposé d'établir une norme pour les procédures de passerelle à passerelle qui permette aux passerelles d'être mutuellement soupçonneuses. Le présent document est un projet pour cette norme. Vous êtes vivement encouragés à y faire des commentaires.

Table des Matières

1. Introduction

On prévoit que le Catenet du DARPA sera un système en expansion continuelle, avec de plus en plus d'hôtes sur de plus en plus de réseaux participants. Bien sûr, cela va exiger de plus en plus de routeurs. Dans le passé, une telle expansion a eu lieu d'une façon relativement peu structurée. Les nouveaux routeurs, qui contiennent souvent des logiciels radicalement différents de ceux des routeurs existants, vont être ajoutés et vont immédiatement commencer à participer à l'algorithme d'acheminent commun via le protocole GGP. Cependant, comme l'Internet croît de plus en plus, cette méthode simple d'expansion devient de moins en moins praticable. Il y a un certain nombre de raisons à cela :

- la surcharge de l'algorithme d'acheminement devient excessive ;
- la prolifération de routeurs radicalement différents qui participent à un seul algorithme d'acheminement commun rend la maintenance et l'isolement des fautes presque impossibles, car on ne peut plus considérer l'Internet comme un système de communications intégré ;
- le logiciel et les algorithmes des routeurs, en particulier l'algorithme d'acheminement, deviennent trop rigides et inflexibles, car tout changement proposé doit être fait dans trop d'endroits différents et par trop de gens différents.

À l'avenir, l'Internet est supposé évoluer en un ensemble de domaines séparés ou "systèmes autonomes", dont chacun consiste en un ensemble d'un ou plusieurs routeurs relativement homogènes.

Les protocoles, et en particulier l'algorithme d'acheminement qu'utilisent entre eux ces routeurs sera une affaire privée, qu'il ne sera pas nécessaire de mettre en œuvre dans les routeurs à l'extérieur du domaine ou système particulier.

Dans le cas le plus simple, un système autonome peut consister simplement un seul routeur qui connecte, par exemple, un réseau local à l'ARPANET. Un tel routeur peut être appelé un "routeur d'extrémité", car son seul objet et de faire l'interface du réseau local avec le reste de l'Internet, et il n'est pas destiné à être utilisé pour traiter du trafic qui n'est ni généré ni destiné à ce réseau local particulier. Dan un avenir à moyen terme, on commencera à voir l'Internet comme un ensemble de systèmes autonomes, dont l'un est constitué des routeurs du DARPA sur ARPANET et SATNET, et les autres sont des routeurs d'extrémité pour des réseaux locaux. L'ancien système, que nous appellerons le système "cœur", sera utilisé comme système de transport ou "à longue portée" par ces derniers systèmes.

Finalement, l'Internet peut cependant consister en un certain nombre de systèmes autonomes sur un pied d'égalité, dont chacun peut être utilisé (avec certaines restrictions qu'on exposera plus loin) comme support de transport pour le trafic généré dans n'importe quel système et destiné à tout autre système. Lorsque on en vient à cette configuration plus complexe, il serait inapproprié de considérer un de ces systèmes autonomes comme un système "cœur". Pour être concret, et comme les mises en œuvre initiales du protocole de passerelle extérieure sont supposées se concentrer sur le cas de la connexion des "routeurs d'extrémité" aux routeurs DARPA sur ARPANET et SATNET, on utilisera souvent le terme de routeur "de cœur" dans nos exemples et discussions.

L'objet du protocole de passerelle extérieure (EGP, *Exterior Gateway Protocol*) est de permettre à un ou plusieurs systèmes autonomes d'être utilisés comme moyen de transport pour le trafic généré dans un autre système autonome et destiné encore à un autre, tout en permettant à l'utilisateur final de voir la composition de tous les systèmes autonomes comme un seul internet, avec un espace d'adresse plat, uniforme. Le chemin que prend un datagramme à travers l'internet, et le nombre de systèmes autonomes qu'il traverse, sont transparents à l'utilisateur final (sauf, bien sûr, si l'utilisateur final utilise l'option IP "route de source").

Pour décrire le protocole de passerelle extérieure, on a délibérément laissé une grande latitude aux concepteurs et aux mises en œuvre de systèmes autonomes particuliers, spécialement en ce qui concerne les valeurs de temporisateurs. Cela a été fait parce qu'on s'attend à ce que les différentes mises en œuvre de routeurs et les différents environnements d'internet puissent avoir des exigences et buts différents, de sorte qu'une seule spécification stricte de mise en œuvre ne pourrait pas s'appliquer à toutes. Cependant, cela ne signifie PAS que TOUTE mise en œuvre qui se conforme à la spécification va bien fonctionner, ou que les domaines dans lesquels on a laissé de la latitude ne sont pas cruciaux pour les performances. Le fait que, par exemple, une valeur de temporisation ne soit pas spécifiée ici ne signifie pas que tout va bien fonctionner quelle que soit la valeur qui est allouée.

Des numéros d'identification de 16 bits seront alloués aux systèmes autonomes (tout à fait de la même façon que sont maintenant alloués les numéros de réseau et de protocole) et tout en-tête de message EGP contient un mot pour ce numéro. Zéro ne sera alloué à aucun système autonome ; la présence d'un zéro dans ce champ va plutôt indiquer qu'aucun numéro n'est présent.

On a besoin d'introduire le concept qu'un routeur est un VOISIN d'un autre. Dans le cas le plus simple et le plus courant, on dit que deux routeurs sont "voisins" si il y a un réseau auquel chacun a une interface. Cependant, on aura besoin d'une notion un peu plus générale de "voisin" pour permettre les deux cas suivants :

a) Deux routeurs peuvent être considérés comme voisins si ils sont directement connectés non par un réseau (dans le sens usuel du terme) mais par un simple fil, ou ligne HDLC, ou quelque moyen similaire de "connexion directe".
b) Deux routeurs peuvent être considérés comme voisins si ils sont connectés par un "internet" qui leur est transparent. C'est-à-dire qu'on aimerait pouvoir dire que deux routeurs sont voisins même si ils sont connectés par un internet, pour autant que les routeurs n'utilisent pas la connaissance de la structure interne de leur internet dans leurs propres algorithmes de transmission de paquets.

Pour traiter tous ces cas, disons que deux routeurs sont VOISINS si ils sont connectés par un support de communications dont la structure interne leur est transparente. (Voir l'IEN 184 pour un exposé plus général de cette notion de voisin.)

Si deux voisins font partie du même système autonome, on les appelle des VOISINS INTÉRIEURS ; Si deux voisins ne font pas partie du même système autonome, on les appelle des VOISINS EXTÉRIEURS. Pour qu'un système en utilise un autre comme moyen de transport, les routeurs qui sont des voisins extérieurs l'un pour l'autre doivent être capables de trouver quels réseaux peuvent être atteints par l'intermédiaire de l'autre. Le protocole de passerelle extérieure permet que ces informations soient passées entre les voisins extérieurs. Comme il y a un protocole d'interrogation, cela permet aussi à chaque routeur de contrôler le débit auquel il envoie et reçoit les informations d'accessibilité de réseau, permettant à chaque système de contrôler sa propre redondance. Cela permet aussi à chaque système d'avoir un algorithme d'acheminement indépendant dont le fonctionnement ne peut pas être interrompu par les défaillances des autres systèmes.

On doit bien comprendre que tout système autonome dans lequel doit être effectué un acheminement entre des routeurs au sein de ce système doit mettre en œuvre son propre algorithme d'acheminement. (Un algorithme d'acheminement n'est généralement pas nécessaire pour un simple système autonome qui consiste en un seul routeur d'extrémité.) Le protocole de passerelle extérieure N'EST PAS un algorithme d'acheminement. Il permet aux voisins extérieurs d'échanger des informations qui vont probablement être nécessaires pour tout algorithme d'acheminement, mais il NE spécifie PAS ce que les routeurs vont faire avec ces informations. Les "mises à jour d'acheminement" de l'algorithme d'acheminement intérieur de certains systèmes d'exploitation peuvent être ou non similaires en format aux messages du protocole de passerelle extérieure. Les passerelles dans le système "cœur" du DARPA vont initialement utiliser le protocole GGP (le vieux protocole de passerelle à passerelle) comme algorithme d'acheminement, mais cela va changer. Les routeurs des autres systèmes autonomes peuvent utiliser leur propre protocole de passerelle intérieure (des IGP), qui peuvent être ou non similaires à l'IGP de n'importe quel autre système autonome. Ils peuvent, bien sûr, utiliser GGP, mais il ne leur sera pas permis d'échanger des messages GGP avec les routeurs des autres systèmes autonomes.

Il doit aussi être clairement compris que le protocole de passerelle extérieure N'EST PAS destiné à fournir des informations qui pourraient être utilisées comme entrées d'un algorithme de zone complètement générale ou d'acheminement hiérarchique. Il est destiné à un ensemble de systèmes autonomes qui sont connectés dans une arborescence, sans cycles. Il ne permet pas le passage d'informations suffisantes pour empêcher les boucles d'acheminement si il existe des cycles dans la topologie.

Le protocole de passerelle extérieure a trois parties : (a) protocole d'acquisition de voisin, (b) protocole d'accessibilité de voisin, et (c) détermination de l'accessibilité du réseau. Noter que tous les messages définis par EGP sont destinés à ne voyager que sur un seul "bond". C'est-à-dire qu'il sont générés à un routeur et envoyés à un routeur voisin sans la médiation d'aucun routeur intermédiaire. Donc, le champ Durée de vie devrait être réglé à une valeur très faible. Les routeurs qui rencontrent des messages EGP dans leur flux de messages et qui ne leur sont pas adressés peuvent les supprimer.

2. Acquisition de voisins

Avant qu'il soit possible d'obtenir des informations d'acheminement d'un routeur extérieur, il est nécessaire d'acquérir ce routeur comme voisin direct. (La distinction entre voisin direct et indirect sera faite un peu plus loin.) Pour que deux routeurs deviennent des voisins directs, ils doivent être voisins, au sens défini ci-dessus, et ils doivent exécuter le protocole d'acquisition de voisin, qui est simplement une prise de contact en trois phases standard.

Un routeur qui souhaite initier l'acquisition de voisin avec un autre lui envoie une Demande d'acquisition de voisin. L'émission de ce message devrait être répétée (à un rythme raisonnable, peut-être toutes les 30 secondes à peu près) jusqu'à ce qu'une Réponse d'acquisition de voisin soit reçue. La demande va contenir un numéro d'identification qui est copié dans la réponse afin qu'on puisse faire correspondre demande et réponse.

Un routeur qui reçoit une demande d'acquisition de voisin doit déterminer si il souhaite devenir un voisin direct de la source de la demande. Sinon, il peut, à son choix, répondre par un message Refus d'acquisition de voisin, spécifiant facultativement la raison du refus. Autrement, il devrait envoyer un message Réponse d'acquisition de voisin. Il doit aussi envoyer un message Demande d'acquisition de voisin, à moins qu'il ne l'ait déjà fait.

Deux routeurs deviennent des voisins directs lorsque chacun a envoyé et reçu un message d'acquisition de voisin à la réponse d'acquisition de voisin correspondante de l'autre.

Les réponses ou refus sans correspondance devraient être éliminés après un délai raisonnable. Cependant, des informations sur de tels messages sans correspondance peuvent être utiles pour des besoins de diagnostic.

On devrait répondre à un message d'acquisition de voisin de la part d'un routeur qui est déjà un voisin direct avec une Réponse et un message d'acquisition de voisin.

Si on reçoit une réponse d'acquisition de voisin de la part d'un voisin prospectif, mais qu'il s'écoule un délai durant lequel aucun message d'acquisition de voisin n'est reçu de ce voisin prospectif, le protocole d'acquisition de voisin sera réputé inachevé. Un message Fin de voisinage *(Neighbor Cease)* (voir ci-dessous) devrait alors être envoyé. Si un routeur désire encore acquérir l'autre comme voisin, le protocole doit être répété depuis le début.

Si un routeur souhaite cesser d'être un voisin d'un routeur extérieur particulier, il envoie un message Fin de voisinage. Un routeur qui reçoit un message Fin de voisinage devrait toujours répondre par un accusé de réception de fin de voisinage. Il devrait cesser de traiter l'envoyeur du message comme voisin de quelque façon que ce soit. Comme il y a une quantité significative d'échanges de protocole entre les voisins directs (voir plus loin) si certains routeurs n'ont plus besoin d'être un voisin direct de certains autres, il est "poli" d'indiquer ce fait par un message Fin de voisinage. Le message Fin de voisinage devrait être retransmis (jusqu'à un nombre limite de fois) jusqu'à ce qu'en soit reçu un accusé de réception.

Une fois qu'un message Fin de voisinage a été reçu, le protocole d'accessibilité de voisin (ci-dessous) devrait cesser d'être exécuté.

Noter qu'on n'a pas spécifié la moyen par lequel un routeur décidé initialement qu'il veut devenir un voisin d'un autre. Bien que ce problème soit loin d'être trivial, cela ne fait pas partie du protocole de passerelle extérieure.

3. Protocole d'accessibilité de voisin

Il est important qu'un routeur conserve des informations en temps réel sur l'accessibilité de ses voisins. Si un routeur en arrive à la conclusion qu'un voisin particulier ne peut pas être joint, il devrait cesser de lui transmettre du trafic. Pour déterminer cela, il est nécessaire d'avoir un protocole d'accessibilité de voisin. Le protocole EGP fournit deux types de messages à cette fin – un message "Hello" et un message "Je t'entends".

Lorsque un message "Hello" est reçu d'un voisin direct, un "Je t'entends" doit être retourné "immédiatement" à ce voisin. Le délai entre la réception d'un"Hello" et le retour d'un "Je t'entends" ne devrait jamais dépasser quelques secondes.

Pour l'instant, l'algorithme de détermination d'accessibilité est laissé au choix des concepteurs du routeur. On pense à des algorithmes comme celui-ci :

Un voisin accessible devra être déclaré inaccessible si, durant la période pendant laquelle on a envoyé un "Hello", on a reçu moins de k "Je t'entends" en retour. Un voisin inaccessible devra être déclaré accessible si, durant la période pendant laquelle on a envoyé les m derniers "Hello", on a reçu au moins j "Je t'entends" en retour.

Cependant, la fréquence à laquelle sont envoyés les "Hello", et les valeurs des paramètres k, n, j, et m ne peuvent pas être spécifiées ici. Les résultats vont dépendre des caractéristiques du voisin et du réseau que partagent les voisins. Cela implique que les paramètres appropriés peuvent devoir être déterminée conjointement par les concepteurs et les mises en œuvre des deux routeurs voisins ; le choix des algorithmes et paramètres en solitaire, sans considérer les caractéristiques du voisin et du réseau de connexion ne peut être espéré donner les déterminations d'accessibilité optimales.

Les messages "Hello" et "Je t'entends" ont un champs État que le routeur envoyeur utilise pour indiquer si il pense que le routeur receveur est accessible ou non. Cette information peut être utile à des fins de diagnostic. Elle permet aussi à un routeur de greffer sa détermination d'accessibilité sur celle de l'autre : un seul routeur a en fait besoin d'envoyer des messages "Hello", et l'autre peut le déclarer actif ou mort sur la base du champ État dans le "Hello". C'est-à-dire que le routeur "passif" (qui envoie seulement des "Je t'entends") déclare à celui qui est "actif" (celui qui envoie seulement des "Hello") qu'il est accessible lorsque les "Hello" provenant de celui qui est actif indiquent qu'il a déclaré que celui qui est passif est accessible.

Bien sûr, cela ne peut fonctionner que si il y a un accord préalable sur quel voisin est celui qui est actif. (Les façons d'arriver à cet "accord préalable" ne font pas partie du protocole de passerelle extérieure.)

Un routeur voisin direct devrait aussi être déclaré injoignable si le réseau qui le connecte fournit un niveau d'informations de protocole inférieur à ce qui est nécessaire pour qu'on puisse le déduire. Donc, par exemple, si un routeur reçoit un message 1822 Destination morte de l'ARPANET qui indique qu'un voisin direct est mort, il devrait déclarer ce voisin injoignable. Le voisin ne devrait pas être déclaré à nouveau accessible jusqu'à ce que le nombre requis de paquets Hello/Je t'entends aient été échangés.

Un voisin direct qui est devenu inaccessible ne cesse pas cependant d'être un voisin direct. Le voisin peut être déclaré à nouveau accessible sans qu'il soit besoin de passer à nouveau par le protocole d'acquisition de voisin. Cependant, si le voisin reste inaccessible pendant une période extrêmement longue, comme une heure, le routeur devrait cesser de le traiter comme un voisin, c'est-à-dire, il devrait cesser de lui envoyer des messages Hello. Le protocole d'acquisition de voisin devrait alors être répété avant qu'il puisse redevenir un voisin direct.

Les messages "Hello" et "Je t'entends" du routeur G au routeur G' portent aussi le numéro d'identification du message d'interrogation NR (voir ci-dessous) que G a le plus récemment reçu de G'.

Les messages "Hello" et "Je t'entends" du routeur G au routeur G' portent aussi l'intervalle minimum en minutes auquel G accepte d'être interrogé par G' pour les messages NR (voir ci-dessous).

Les messages "Hello" provenant de sources autres que des voisins directs devraient être simplement ignorés. Cependant, l'enregistrement de la présence de tels messages dans les journaux d'incidents peut fournir des informations utiles de diagnostic.

Un routeur qui connaît une défaillance, ou dont l'interface avec le réseau qui le connecte à un voisin particulier a une défaillance, devrait envoyer un message Routeur en panne à tous les voisins directs auxquels il n'est plus capable d'accéder. Il devrait aussi retransmettre ce message (jusqu'à un certain nombre de fois) jusqu'à ce qu'il reçoive un accusé de réception de routeur en panne. Cela fournit aux voisins un avertissement anticipé d'une panne, et leur permet de s'y préparer d'une façon qui va minimiser le dérangement du trafic existant.

4. Message d'accessibilité réseau (NR)

Terminologie : Le routeur G a une interface au réseau N. On dit que G est un premier bond approprié pour le réseau M par rapport au réseau N (où M et N sont des réseaux distincts) si et seulement si la condition suivante est remplie :
Le trafic qui est destiné au réseau M, et qui arrive au routeur G sur son interface au réseau N, sera transmis à M par G sur un chemin qui ne comporte aucun autre routeur ayant une interface avec le réseau N.

En bref, G est un premier bond approprié pour le réseau M par rapport au réseau N seulement dans le cas où il n'y a pas de

meilleur routeur sur le réseau N par lequel acheminer le trafic qui est destiné au réseau M. Pour un acheminement optimal, le trafic du réseau N est destiné au réseau M devrait toujours être transmis à un routeur qui est un premier bond approprié.

Pour que les routeurs extérieurs G et G' (qui sont voisins sur le réseau N) soient capables de s'utiliser l'un l'autre comme commutateurs de paquets pour transmettre le trafic aux réseaux distants, chacun a besoin de savoir la liste des réseaux pour lesquels l'autre est un premier bond approprié. Le protocole de passerelle extérieure définit un message, appelé message d'accessibilité de réseau ou message NR *(Network Reachability)* pour transférer ces informations.

Soit G un routeur sur le réseau N. Le message NR que G envoie au sujet du réseau N doit contenir les informations suivantes : une liste de tous les réseaux pour lesquels G est un premier bond approprié par rapport au réseau N.

Si G' peut obtenir ces informations du voisin extérieur G, il sait alors qu'aucun trafic destiné aux réseaux qui NE SONT PAS dans cette liste ne devrait être transmis à G. (Il ne peut cependant pas simplement conclure que tout le trafic pour tout réseau de cette liste devrait être transmis via G, car G' peut aussi avoir d'autres voisins qui sont aussi des premiers bonds appropriés pour le réseau N. Par exemple, G et G" peuvent être chacun des voisins de G', mais peuvent être "équidistants" d'un réseau M. Chacun pourrait alors être un premier bond approprié.)

Pour chaque réseau de la liste, le message NR contient aussi un octet qui spécifie la "distance" (conformément à une certaine métrique dont la définition est laissée aux concepteurs du système autonome dont est membre le routeur G) de G à ce réseau. Ces informations peuvent (ou non) être utiles dans l'algorithme d'acheminement intérieur du routeur G', ou pour des besoins de diagnostic.

La valeur maximum de distance (255) devra être prise comme signifiant que le réseau est INACCESSIBLE. Toutes les autres valeurs seront prises pour signifier que le réseau est accessible.

Si un message NR provenant d'un routeur G omet de mentionner un réseau N qui était mentionné dans le précédent message NR provenant de G, on devra supposer que N est toujours accessible à partir de G. Cependant, si N n'est pas mentionné dans deux messages NR successifs provenant de G, cela devra être compris comme signifiant que N n'est plus accessible à partir de G. Cette procédure est nécessaire pour s'assurer que les réseaux qui ne peuvent plus être atteints, mais qui ne sont jamais déclarés explicitement inaccessibles, arrivent en fin de temporisation et sont retirés de la liste des réseaux accessibles.

Il peut être souvent le cas que G et G' soient des voisins extérieurs sur le réseau N, que G connaisse beaucoup plus de routeurs voisins sur le réseau N, et sache pour quels réseaux ces autres voisins sont le premier bond approprié. Comme G' peut ne pas savoir qui sont tous ces autres voisins, il est pratique et souvent plus efficace qu'il soit capable d'obtenir ces informations de G. Donc, le message NR EGP contient aussi des champs qui permettent à G de spécifier les informations suivantes :

a) Une liste de tous les voisins (intérieurs et extérieurs) de G (sur le réseau N) que G a déterminé de façon fiable comme étant accessibles. Les routeurs ne devraient être inclus dans cette liste que si G fait fonctionner activement son protocole d'accessibilité de voisin avec eux.
b) Pour chacun de ces voisins, la liste des réseaux pour lesquels ce voisin est un premier bond approprié (par rapport au réseau N).
c) Pour chacune de ces paires <voisin, réseau>, la "distance" de ce voisin à ce réseau.

Donc, le message NR donne les moyens qui permettent à un routeur de "découvrir" de nouveaux voisins en regardant si un voisin qu'il connaît déjà a des voisins supplémentaires sur le même réseau. Cette information rend aussi possible la mise en œuvre de la stratégie de voisin indirect définie ci-dessous.

Une description plus précise du message NR serait la suivante.

La portion de données du message va largement consister en blocs de données. Chaque bloc va avoir en en-tête une adresse de routeur, qui sera l'adresse soit du routeur qui envoie le message, soit d'un des voisins de ce routeur. Chaque adresse de routeur sera suivie par une liste des réseaux pour lesquels ce routeur est un premier bond approprié, et la distance de ce routeur à chaque réseau.

Précédant la liste des blocs de données, il y a :

a) L'adresse du réseau auquel ce message se rapporte. Si G et G' sont voisins sur le réseau N, alors dans le message NR qui va de G à G', c'est l'adresse du réseau N. Par convention, quatre octets ont été alloués à cette adresse – les un, deux ou trois octets de queue devraient être à zéro.
b) Le compte (un octet) du nombre de routeurs intérieurs de G pour lesquels ce message contient des blocs de données. Par convention, ce compte va inclure le bloc de données pour G lui-même, qui devrait être le premier à apparaître.
c) Le compte (un octet) du nombre de voisins extérieurs de G pour lesquels son message contient des blocs de données.

Suivent ensuite les blocs de données eux-mêmes, d'abord le bloc pour G lui-même, puis les blocs pour tous les voisins intérieurs de G (s'il en est) puis les blocs pour les voisins extérieurs. Comme tous les routeurs mentionnés sont sur le même réseau, dont l'adresse a déjà été donnée, les adresses de routeur sont données en omettant la partie adresse de réseau (un, deux ou trois octets) pour économiser l'espace.

Chaque bloc comporte un compte d'un octet du nombre de réseaux pour lesquels le routeur est le premier bond approprié. Dans la liste des réseaux, chaque adresse de réseau est d'un, deux ou trois octets, selon que c'est un réseau de classe A, de classe B, ou de classe C. Aucun octet de queue n'est utilisé.

Il peut parfois être nécessaire de fragmenter le message NR. Le message NR contient un octet qui indique le numéro de ce fragment (les fragments sont numérotés à partir de zéro) et un octet qui contient le numéro du dernier fragment (NON le nombre de fragments). Si la fragmentation n'est pas utilisée, ces octets doivent tous deux être à zéro. Chaque fragment doit être un message NR pleinement auto suffisant. C'est-à-dire, que chaque fragment va commencer par un compte des voisins intérieurs et extérieurs, et aura un nombre entier de blocs de données de routeur. Le nombre de blocs de données dans chaque fragment doit correspondre aux comptes de voisins du début de ce fragment. Cependant, seul le premier fragment devrait commencer par un bloc de données décrivant le routeur qui envoie.

Ce schéma permet que chaque fragment soit traité de façon indépendante, et n'exige pas de complexes mécanismes de réassemblage. Il permet aussi le traitement d'un message dont tous les fragments n'ont pas été reçus. Si, après un certain délai et un certain nombre de retransmissions d'une interrogation, tous les fragments n'ont pas été reçus, les fragments qui sont présents devront être traités comme si ils constituaient le message NR complet. (Cela signifie que les réseaux mentionnés seulement dans le fragment manquant vont conserver les valeurs de "distance" qu'ils avaient dans le précédent message NR provenant de ce routeur. Cependant, si aucune nouvelle valeur n'est reçue pour un réseau particulier dans le prochain message NR de ce routeur, le réseau sera déclaré injoignable.)

5. Appel de messages NR

Aucun routeur n'est obligé d'envoyer des messages NR aux autres routeurs, sauf en réponse à une interrogation NR d'un voisin direct. Cependant, un routeur est obligé de répondre à une interrogation NR d'un voisin direct dans les quelques secondes (sous réserve de la qualification donnée à deux paragraphes d'ici) même si le routeur croit que le voisin est mort.

Le message EGP Interrogation NR est défini à cette fin. Aucun routeur ne peut en interroger un autre par un message NR plus souvent qu'une fois par minute. Un routeur qui reçoit plus d'une interrogation par minute peut simplement ignorer les interrogations excédentaires, ou peut retourner un message d'erreur. Les messages Hello et Je t'entends qu'envoie le routeur G au routeur G' indiquent l'intervalle minimum que G va accepter comme intervalle d'interrogation de la part de G'. C'est-à-dire que G' ne va pas garantir de répondre aux interrogations de G qui arrivent séparées par moins que cet intervalle.

Les interrogations ne doivent être envoyées qu'aux voisins directs qui sont déclarés accessibles par le protocole d'accessibilité de voisin.

Un message Interrogation NR contient un numéro d'identification choisi par le routeur interrogateur. Le routeur interrogé va retourner ce numéro dans le message NR qu'il envoie en réponse à l'interrogation, pour permettre au routeur interrogateur de faire correspondre les messages NR reçus avec les interrogations. Il sera de la responsabilité du routeur interrogateur de choisir un numéro d'identification qui soit suffisamment "unique" pour permettre la détection des messages NR déclassés qui pourraient être encore en train de flotter dans le réseau. Comme les interrogations sont relativement peu fréquentes, on ne s'attend pas à ce que cela pose beaucoup de problèmes. Cependant, pour aider au choix d'un numéro d'identification, les messages Hello et Je t'entends portent le numéro d'identification de la dernière interrogation NR reçue du voisin auquel ils sont envoyés.

En général, une interrogation devrait être retransmise un certain nombre de fois (avec un intervalle raisonnable entre les retransmissions) jusqu'à ce qu'un message NR soit reçu. Si aucun message NR n'est reçu passé le nombre maximum de retransmissions, le routeur interrogateur devrait supposer que le routeur interrogé n'est pas un premier bond approprié pour un quelconque réseau. Les paramètres optimaux pour l'algorithme d'interrogation/retransmission vont dépendre des caractéristiques des deux voisins et du réseau qui les connectent.

Si seuls certains fragments d'un message NR sont reçus passé le nombre maximum de retransmissions, les fragments qui sont présents devront être traités comme constituant la totalité du message NR.

Les messages NR reçus dont le numéro d'identification ne correspond pas au numéro d'identification de la plus récente interrogation envoyée devront être ignorés. Aucune disposition n'est prise pour de multiples interrogations en instance pour le même voisin.

6. Envoi des messages NR

En général, les messages NR sont à envoyer seulement en réponse à une interrogation. Cependant, entre deux interrogations successives d'un voisin extérieur, un routeur peut envoyer un seul message NR non sollicité à ce voisin. Cela lui donne une capacité limitée à annoncer rapidement des changements d'accessibilité de réseau qui peuvent être survenus dans l'intervalle depuis la dernière interrogation. Les messages NR non sollicités excédentaires peuvent être ignorés, ou un message d'erreur peut être retourné.

Un message NR devrait être envoyé dans les quelques secondes qui suivent la réception d'une interrogation. Omettre de répondre à temps à une interrogation NR peut résulter en ce que le routeur interrogateur décide que le routeur interrogé n'est pas un premier bond approprié pour tout réseau.

Les messages NR envoyés en réponse à des interrogations portent le numéro d'identification du message d'interrogation dans les champs "Numéro d'identification". Les messages NR non sollicités portent le numéro d'identification de la dernière interrogation reçue, et ont le bit "non sollicité" établi. (Noter que cela ne permet qu'un seul message NR non sollicité par période d'interrogation.)

Pour faciliter l'envoi des messages NR non sollicités, le message d'interrogation NR a un octet qui indique l'intervalle d'interrogation en minutes.

Les interrogations qui proviennent de non voisins, de voisins qui ne sont pas déclarés accessibles, ou avec de mauvais champs de réseau IP de source, devraient avoir en réponse un message d'erreur EGP avec le champ de cause approprié. Si G envoie à G' une interrogation NR avec le réseau IP de source N, et si G' n'est pas un voisin de G sur son interface au réseau N (ou si G' n'a pas d'interface avec le réseau N) le champ Réseau de source est alors considéré comme "mauvais".
Les interrogations dupliquées (des interrogations successives avec le même numéro d'identification) devraient avoir pour réponse des copies du même message NR. Si ce message est fragmenté, le même fragment devra être envoyé à chaque fois. Noter qu'il n'y a aucune disposition pour le traitement de multiples interrogations en instance provenant d'un seul voisin. Noter que si les mêmes fragments ne sont pas envoyés en réponse à des interrogations dupliquées, le résultat probable sera un réassemblage incorrect. Cependant, si la fragmentation n'est pas utilisée, il ne devrait résulter aucun dommage de la réponse à une interrogation dupliquée avec un message NR différent (qu'on présume plus récent).

7. Voisins indirects

Il faut trois étapes pour devenir un "voisin direct" d'un routeur extérieur : (a) acquisition de voisin, (b) lancement d'un protocole d'accessibilité de voisin, et (c) interrogation périodique du voisin avec des messages NR. Supposons, cependant, que le routeur G reçoive un message NR de G', dans lequel G' indique la présence d'autres voisins G1, ..., Gn, dont chacun est un premier bond approprié pour un certain ensemble de réseaux auxquels G' n'est pas lui-même un premier bond approprié. Il devrait alors être permis à G de transmettre du trafic pour ces réseaux directement à celui de G1, ..., Gn qui est approprié sans avoir à l'envoyer d'abord à G'. Dans ce cas, G peut être considéré comme un voisin INDIRECT de G1, ..., Gn, car il est un voisin de ces autres routeurs pour les besoins de la transmission du trafic, mais il n'effectue pas l'acquisition de voisin, l'accessibilité de voisin, ou l'échange de messages NR avec eux. Les informations de voisin et d'accessibilité de réseau sont obtenues indirectement via G', d'où la désignation de "voisin indirect". On dit que G est un voisin indirect de G1, ..., Gn via G'.

Si G est un voisin indirect de G' via G", et si G reçoit alors un message NR de G" qui ne mentionne pas G', G devrait traiter G' comme étant devenu injoignable.

8. Comment être un routeur d'extrémité

L'application la plus courante de EGP sera probablement pour permettre à un routeur d'extrémité de communiquer avec un des routeurs du cœur du DARPA, de façon à permettre les flux de données entre les réseaux accessibles seulement via le bout et les réseaux accessibles seulement via le système de routeurs centraux. Comme exposé précédemment, un routeur d'extrémité peut être considéré comme étant un système internet à un routeur sans voisin intérieur. Il est probablement utilisé pour assurer l'interface avec un ou des réseaux locaux avec un réseau de transport à longue portée (comme l'ARPANET ou le SATNET) sur lequel il y a un routeur central. Dans ce cas, le bout ne va pas vouloir que les routeurs centraux lui transmette du trafic autre que celui qui est destiné au ou aux réseaux qui ne peuvent être atteints que via le bout. En général, le bout ne voudra pas effectuer de services pour le système de transport internet qui ne serait pas nécessaire afin d'être capable de passer le trafic de et vers les réseaux qui ne peuvent pas être atteints autrement.

Le routeur d'extrémité devrait avoir des tableaux configurés avec les adresses d'un petit nombre des routeurs centraux (pas plus que deux ou trois) avec lesquels il a un réseau commun. Il sera de la responsabilité du routeur d'extrémité d'initier l'acquisition de voisin avec ces routeurs. Lorsque un routeur d'extrémité et un routeur central deviennent des voisins directs, le routeur central va commencer à envoyer des messages Hello.

Lorsque le routeur d'extrémité déclare que les routeurs centraux avec lesquels il est un voisin direct sont accessibles, il devrait interroger ces routeurs avec des messages NR à un rythme qui n'excède par une fois par minute (ou comme spécifié dans les messages Hello provenant des routeurs centraux). Les routeurs centraux vont aussi interroger le routeur d'extrémité pour des messages NR.

Le message NR envoyé par le routeur d'extrémité devrait être le plus simple admissible. C'est-à-dire qu'il devrait avoir seulement un bloc de données, précédé de sa propre adresse (sur le réseau qu'il a en commun avec le routeur central voisin) énumérant juste les réseaux pour lesquels il est un premier bond approprié. Ce seront en général juste les réseaux qui ne peuvent pas être atteints d'une autre façon.

Le routeur central va envoyer des messages NR complets, contenant des informations sur tous les autres routeurs sur les réseaux communs, les routeurs centraux (qui devront être énumérés comme voisins intérieurs) et les autres routeurs (qui devront être énumérés comme voisins extérieurs, et qui peuvent inclure le routeur d'extrémité lui-même). Ces informations vont permettre au routeur d'extrémité de devenir un voisin indirect de tous ces autres routeurs. C'est-à-dire que le routeur d'extrémité devra transmettre le trafic directement à ces autres routeurs comme approprié, mais il ne devra pas devenir leur voisin direct.

Les routeurs centraux vont faire rapport des distances inférieures à 128 si le réseau peut être atteint sans quitter le système central (c'est-à-dire, sans traverser de routeur autre qu'un routeur central) et supérieur ou égal à 128 autrement.

Le routeur d'extrémité NE DEVRAIT JAMAIS transmettre du trafic à aucun routeur central du voisinage (direct ou indirect) pour lequel ce routeur n'est pas un premier bond approprié, comme indiqué dans un message NR. Bien sûr, cela ne s'applique pas aux datagrammes qui utilisent l'option Route de source ; tous ces datagrammes devraient toujours être transmis comme indiqué dans le champ Option route de source, même si cela exige de transmettre à un routeur qui n'est pas un premier bond approprié.

Si les voisins directs d'un routeur d'extrémité font tous défaut, il sera de la responsabilité du routeur d'extrémité d'acquérir au moins un nouveau voisin direct. Il peut le faire en choisissant un des routeurs centraux qui a eu comme voisin indirect, et en exécutant avec lui le protocole d'acquisition de voisin. (Il est possible que pas plus d'un routeur central accepte jamais de devenir un voisin direct avec un certain routeur d'extrémité à la fois.)

Si le routeur d'extrémité ne répond pas à temps aux messages Hello provenant du routeur central, il peut être déclaré injoignable. Si il ne répond pas à temps aux messages d'interrogation NR, son réseau peut être déclaré injoignable. Dans ces deux cas, le routeur central peut éliminer le trafic destiné à ces réseaux, retournant le message ICMP "Réseau de destination injoignable" aux hôtes de source.

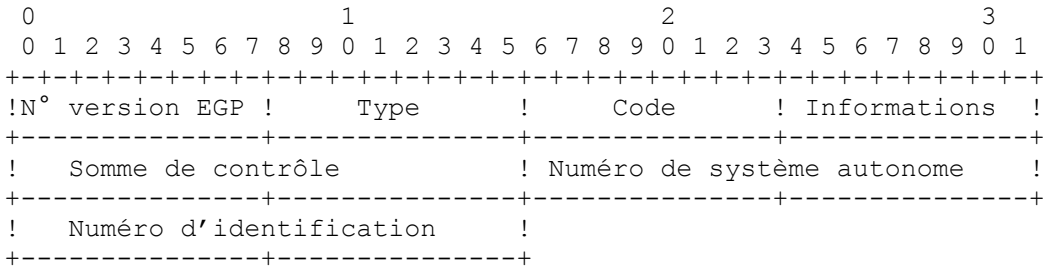
Le routeur d'extrémité est supposé exécuter pleinement le protocole ICMP, ainsi que le protocole EGP. En particulier, il doit répondre aux demandes d'écho ICMP, et doit envoyer les messages ICMP Destination morte lorsque approprié. Il est aussi obligé d'envoyer des messages ICMP Redirection lorsque approprié.

9. Limitations

On doit bien comprendre que le protocole de passerelle extérieure ne constitue pas par lui-même un algorithme d'acheminement réseau. De plus, il ne fournit pas toutes les informations nécessaires pour mettre en œuvre un algorithme d'acheminement de zone générale. Si la topologie de l'ensemble de systèmes autonomes n'est pas structurée en arborescence (c'est-à-dire, si il a des cycles) le protocole de passerelle extérieure de fournit pas assez d'informations topologiques pour empêcher les boucles.

Si un routeur envoie un message NR avec de fausses informations, prétendant être un premier bond approprié pour un réseau qu'il ne peut en fait atteindre, le trafic destiné à ce réseau peut n'être jamais livré. Les mises en œuvre doivent garder cela en mémoire.

Message d'acquisition de voisin



Description : Les messages Acquisition de voisin sont utilisés pas les routeurs intérieurs et extérieurs pour devenir voisins l'un de l'autre.

N° de version EGP : 1

Type : 3

Code
Code = 0 Demande d'acquisition de voisin
Code = 1 Réponse d'acquisition de voisin
Code = 2 Refus d'acquisition de voisin (voir le champ Informations)
Code = 3 Message Fin de voisin (voir le champ Informations)
Code = 4 Accusé de réception de fin de voisin

Somme de contrôle : La somme de contrôle EGP est le complément à un sur 16 bits de la somme des compléments à un du message EGP, commençant par le champ Numéro de version EGP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être à zéro.

Numéro de système autonome : Ce numéro de 16 bits identifie le système autonome qui contient le routeur qui est la source de ce message.

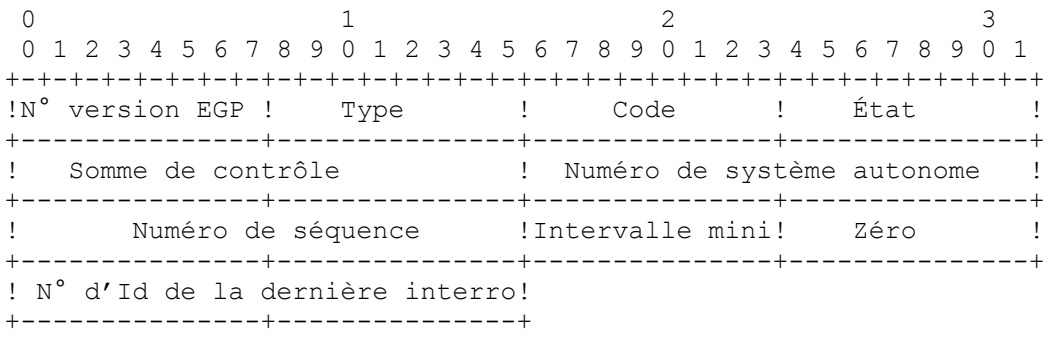
Informations :
Pour le message de refus, donnent la raison du refus :
- 0 Non spécifié
- 1 Hors de l'espace du tableau
- 2 Interdiction administrative

Pour le message de fin, donne la raison pour cesser d'être voisin :
- 0 Non spécifié
- 1 Fermeture
- 2 Plus nécessaire

Autrement, ce champ DOIT être à zéro.

Numéro d'identification : Il aide à faire correspondre les demandes et les réponses.

Message Hello/Je t'entends de voisin



Description : Les voisins extérieurs utilisent les messages EGP Hello et Je t'entends de voisin pour déterminer la connexité de voisin. Lorsque un routeur reçoit d'un voisin un message EGP Hello de voisin, il devrait répondre par un message EGP Je t'entends.

Numéro de version EGP : 1

Type : 5

Code
Code = 0 pour Hello
Code = 1 pour Je t'entends

Somme de contrôle : La somme de contrôle EGP est le complément à un sur 16 bits de la somme des compléments à un du message EGP en commençant par le champ numéro de version EGP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être à zéro.

Numéro de système autonome : Ce numéro de 16 bits identifie le système autonome qui contient le routeur source de ce message.

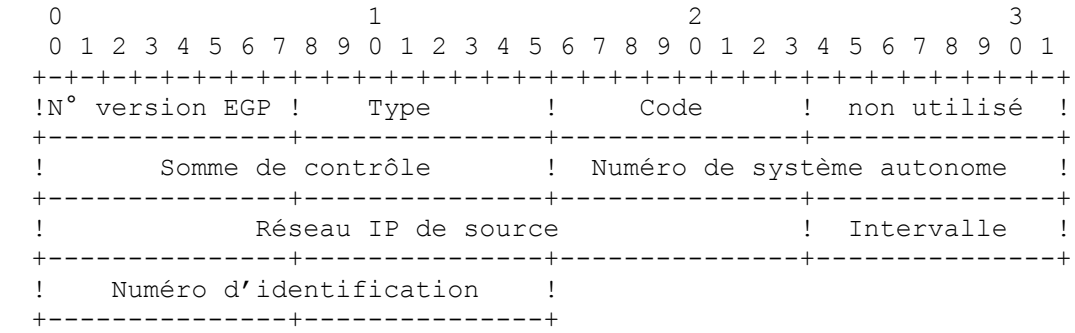
Numéro de séquence : Pour aider à faire correspondre les demandes et les réponses.

État
0 Aucun état n'est donné
1 Vous m'apparaissez accessible
2 Vous m'apparaissez inaccessible selon le protocole d'accessibilité de voisin
3 Vous m'apparaissez inaccessible selon les informations d'accessibilité du réseau (comme les messages 1822 "Destination morte" de l'ARPANET)
4 Vous m'apparaissez inaccessible à cause de problèmes avec mon interface réseau

Numéro d'identification de la dernière interrogation : C'est le numéro d'identification du dernier message d'interrogation NR reçu du voisin auquel ce message est envoyé.

Intervalle minimum d'interrogation : Ce routeur ne devrait pas être interrogé par des messages NR plus d'une fois dans ce nombre de minutes.

Message Interrogation NR



Description : Un routeur qui veut recevoir un message NR d'un routeur extérieur va envoyer un message d'interrogation NR. Chaque routeur mentionné dans le message NR aura une interface sur le réseau qui est dans le champ Réseau IP de source.
Numéro de version EGP : 1

Type : 2

Code : 0

Somme de contrôle : La somme de contrôle EGP est le complément à un sur 16 bits de la somme des compléments à un du message EGP en commençant par le champ numéro de version EGP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être à zéro.

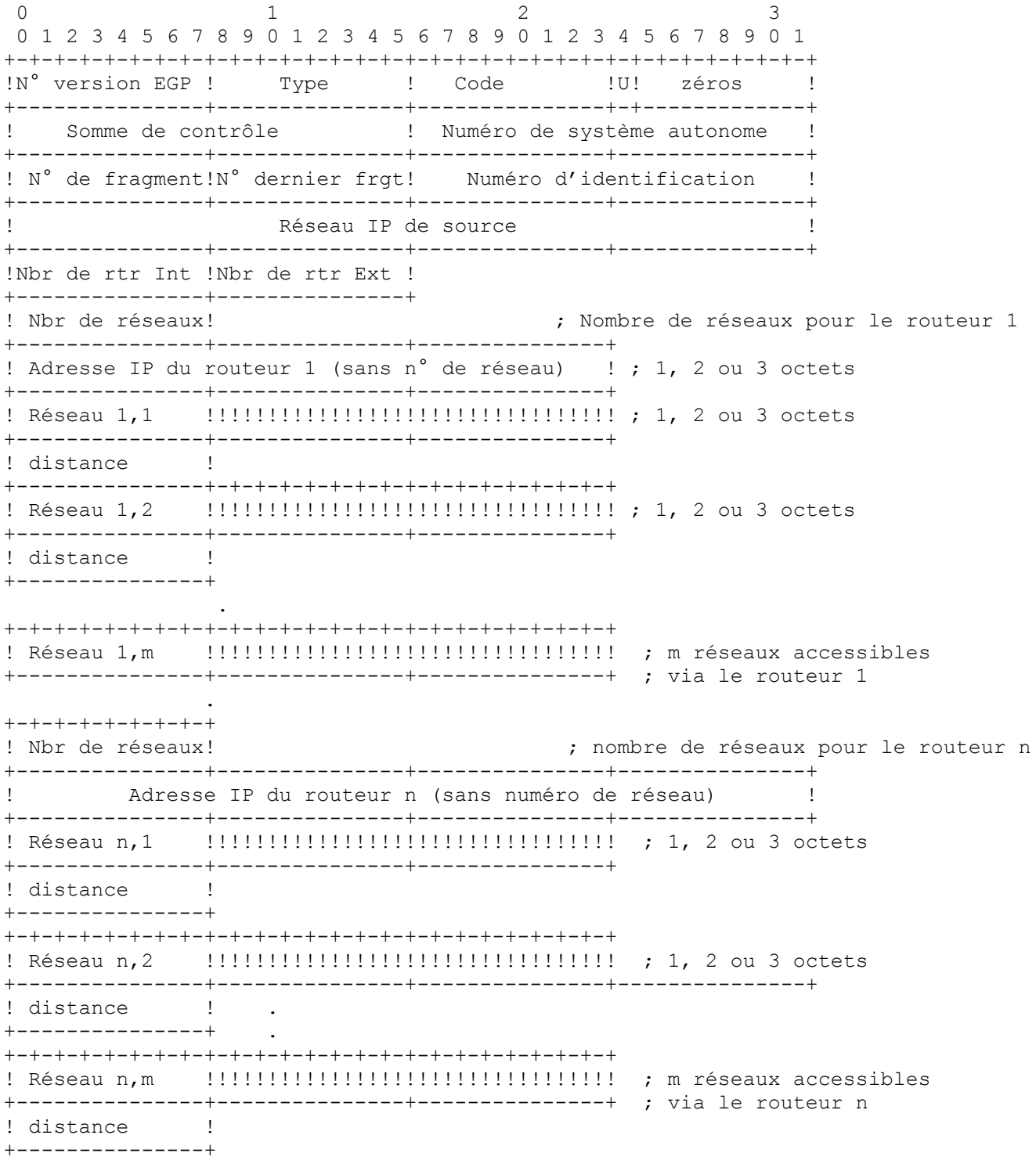
Numéro de système autonome : Ce numéro de 16 bits identifie le système autonome qui contient le routeur source de ce message.

Numéro d'identification : Pour aider à faire correspondre demandes et réponses.

Réseau IP de source : Chaque routeur mentionné dans le message NR aura une interface sur le réseau qui est dans le champ Réseau IP de source. Le réseau IP de source est codé avec un octet pour le numéro de réseau suivi par deux octets de zéros pour les réseaux de classe A, deux octets de numéro de réseau suivis par un octet de zéros pour les réseaux de classe B, et trois octets de numéro de réseau pour les réseaux de classe C.

Intervalle : C'est l'intervalle d'interrogation en minutes.

Message d'accessibilité réseau



Description : Le message d'accessibilité réseau (NR, *Network Reachability*) est utilisé pour découvrir quels réseaux peuvent être atteints par les routeurs extérieurs. Le message NR est envoyé en réponse à un message Interrogation NR.

Numéro de version EGP : 1

Type : 1

Code : 0

Somme de contrôle : La somme de contrôle EGP est le complément à un sur 16 bits de la somme des compléments à un du message EGP en commençant par le champ Numéro de version EGP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être à zéro.

Numéro de système autonome : Ce numéro de 16 bits identifie le système autonome qui contient le routeur qui est la source de ce message.

Bit U (non sollicité) : Ce bit est établi si le message NR est envoyé sans être sollicité.

Numéro d'identification : C'est le numéro d'identification du dernier message d'interrogation NR reçu du voisin auquel ce message NR est envoyé. Ce numéro est utilisé pour aider à faire correspondre interrogations et réponses.

Numéro de fragment : Indique de quel fragment il s'agit dans le message NR. Zéro, si la fragmentation n'est pas utilisée.

Numéro du dernier fragment : Numéro du dernier fragment dans le message NR. Zéro, si la fragmentation n'est pas utilisée.

Réseau IP de source : Chaque routeur mentionné dans le message NR aura une interface sur le réseau qui est dans le champ Réseau IP de source.

Nombre de routeurs intérieurs : Nombre de routeurs intérieurs qui sont mentionnés dans ce message.

Nombre de routeurs extérieurs : C'est le nombre de routeurs extérieurs qui sont mentionnés dans ce message.

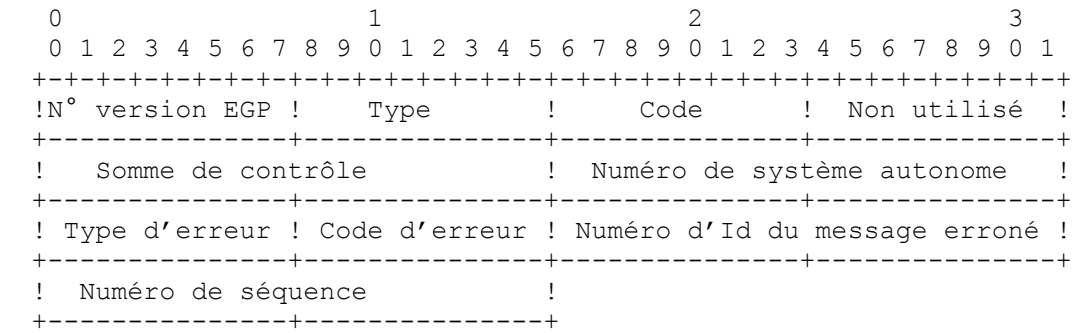
Nombre de réseaux : C'est le nombre de réseaux pour lesquels le routeur dont l'adresse IP suit immédiatement est le premier bond approprié.

Adresse IP du routeur : 1, 2 ou 3 octets d'adresse IP du routeur (sans le numéro de réseau).

Adresse réseau : 1, 2, ou 3 octets d'adresse réseau du réseau qui peut être atteint via le routeur précédant.

Distance : 1 octet de distance en nombre de bonds.

Message d'erreur EGP



Description : Un message d'erreur EGP est envoyé en réponse à un message EGP qui a une mauvaise somme de contrôle ou a une valeur incorrecte dans un de ses champs.

Numéro de version EGP : 1

Type : 8

Code : 0

Somme de contrôle : La somme de contrôle EGP est le complément à un sur 16 bits de la somme des compléments à un du message EGP en commençant par le champ Numéro de version EGP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être à zéro.

Numéro de système autonome : Ce numéro de 16 bits identifie le système autonome qui contient le routeur qui est la source de ce message.

Type d'erreur : C'est le type du message EGP qui était erroné.

Code d'erreur : C'est le code du message EGP qui était erroné.

Numéro d'identification du message erroné : Numéro de séquence du message EGP qui était erroné.

Raison : C'est la raison pour laquelle le message EGP était erroné. Les raisons suivantes sont définies :
0 - Non spécifiée
1 - Mauvaise somme de contrôle EGP
2 - Mauvaise adresse IP de source dans l'interrogation ou la réponse NR
3 - Type ou code EGP indéfini
4 - Interrogation reçue d'un non voisin
5 - Message NR non sollicité reçu en excès
6 - Interrogation reçue en excès
7 - Comptes erronés dans le message NR reçu
8 - Pas de réponse reçue à l'interrogation NR
9 - Tous les fragments du message NR n'ont pas été reçus

Numéro de séquence : C'est le numéro de séquence alloué par le routeur qui envoie le message d'erreur.