Groupe de travail Réseau
Request for Comments : 2072
Catégorie : Information

H. Berkowitz, PSC International
janvier 1997
Traduction Claude Brière de L'Isle

Guide du dénumérotage des routeurs

Résumé
Les adresses IP actuellement utilisées par les organisations vont vraisemblablement subir des changements à court ou moyen terme. Ces changements peuvent devenir nécessaires pour diverses raisons, parmi lesquelles des réorganisations d'entreprise, des déplacements physiques des équipements, de nouvelles relations stratégiques, des changements de fournisseur d'accès Internet (FAI), de nouvelles applications, et le besoin de la connexité Internet mondiale. Une bonne gestion des adresses IP peut en général simplifier la poursuite de l'administration des systèmes ; un bon plan de dénumérotation est aussi un bon plan de numérotage. La plupart des actions prises pour faciliter un dénumérotage futur vont faciliter la routine de l'administration de réseau.

Les routeurs sont les composants qui interconnectent les parties de l'espace d'adresses IP identifiées par des préfixes univoques. Ils seront évidemment impactés par la dénumérotation. Les autres appareils d'interconnexion, tels que les ponts, les commutateurs de couche 2 (c'est-à-dire, des ponts spécialisés) et les commutateurs ATM peuvent être affectés par une dénumérotation. Les interactions de ces appareils d'interconnexion de couche inférieure doivent être considérées au titre de l'effort de dénumérotation.

Les routeurs interagissent avec de nombreux serveurs de l'infrastructure du réseau, y compris du DNS et de SNMP. Ces interactions, et pas seulement la pure structure d'adressage et d'acheminement, doivent être examinées au titre du dénumérotage de routeurs.

Table des matières

1. Introduction

Les organisations peuvent décider de dénuméroter tout ou partie de leur espace d'adresses IP pour diverses raisons. Les motivations générales d'un dénumérotage sont exposées dans la [RFC2071]. Le présent document traite des aspects d'un effort de dénumérotation qui se rapporte aux routeurs, une fois que la décision de dénuméroter a été prise.

Un effort de dénumérotation doit être bien planifié si on veut qu'il réussisse. Le présent document traite de la planification et de la mise en œuvre des lignes directrices pour les appareils d'interconnexion d'une entreprise. Parmi ces appareils, les routeurs sont les plus étroitement associés au plan de numérotation IP.

La planification commence par la compréhension du problème à résoudre. Une telle compréhension inclut à la fois les motivations de la dénumérotation et les problèmes techniques impliqués par un dénumérotage.

1. Commencer par une brève et claire déclaration des raisons du dénumérotage. La Section 3 expose les raisons courantes.
2. Comprendre les principes de la numérotation dans les environnements présent et prévu. La Section 4 examine le numérotage et suggère une méthode de description de la portée d'un dénumérotage.
3. Avant le dénumérotage réel, il peut être utile de faire évoluer l'environnement et la numérotation actuels vers un système plus maîtrisable. La Section 5 discute des moyens d'introduire une meilleure maîtrise de la dénumérotation dans les systèmes actuels.
4. Être conscient des pièges potentiels. Ils sont discutés à la Section 6.
5. Identifier les exigences potentielles pour les outils, discutées à la Section 7.
6. Évaluer les mécanismes spécifiques des routeurs qui seront affectés par la dénumérotation. Sections 8 à 13.
7. Établir un plan de transition spécifique. La Section 15 donne des lignes directrices pour un tel plan..

Lorsque on essaye de comprendre les interactions de la dénumérotation sur les routeurs, il faut se souvenir des différents aspects du problème, selon la portée impliquée par la dénumérotation. Il faut se souvenir que même une dénumérotation à l'échelle de l'entreprise ne va probablement pas affecter toutes les adresses IP visibles au sein de l'entreprise, car certaines adresses (par exemple, des fournisseurs d'accès Internet, des partenaires commerciaux externes) sont en dehors de l'espace d'adresse qui est contrôlé par l'entreprise.

2. Avertissement

La partie principale du présent document est destinée à être indépendante du fabricant. Toutes les caractéristiques de routeur discutées n'ont pas, bien sûr, été mises en œuvre sur tous les routeurs. Le présent document ne devrait pas être utilisé comme une comparaison générale de la richesse des caractéristiques des différentes mises en œuvre. Les références données ici portent seulement sur les caractéristiques affectées par la dénumérotation. Certaines illustrations données en exemple peuvent citer des caractéristiques spécifiques d'un fabricant. Ces exemples ne reflètent pas nécessairement l'état actuel des produits.

3. Motivations d'un dénumérotage

Les raisons d'un dénumérotage peuvent être technologiques, organisationnelles, ou les deux. Les raisons technologiques entrent dans plusieurs grandes catégories discutées ci-dessous. Tout comme il peut y avoir des motivations à la fois technologiques et organisationnelles pour un dénumérotage [RFC2071], il peut y avoir plusieurs raisons technologiques.

Il peut n'y avoir pas une ligne de séparation claire entre les raisons organisationnelles et techniques d'un dénumérotage. Bien que les réseaux aient un charme et une beauté propre, les raisons organisationnelles devraient être définies d'abord afin de justifier le budget pour le dénumérotage technique. Il peut aussi y avoir de pures raisons techniques au dénumérotage, comme des changements de technologie (par exemple, passer du pontage à l'acheminement).

Bien que le présent document soit intitulé "Guide du dénumérotage des routeurs", le dénumérotage peut être nécessaire à cause de l'installation initiale de routeurs dans un réseau ponté traditionnel. Les organisations peuvent avoir eu une solution pontée adéquate qui ne s'adapte pas à la croissance. Certaines organisations pourraient n'avoir pas été capables de passer au routeur tant qu'une amélioration des performances de transmission des routeurs ne serait pas comparable à celles du pontage [Carpenter].

D'autres considérations incluent la conformité avec l'acheminement en dehors de l'organisation. Les questions d'acheminement sont ici principalement celles de l'Internet mondial, mais peuvent aussi impliquer des liaisons bilatérales privées avec d'autres entreprises.

Certaines nouvelles technologies de transmission ont tendu à redéfinir la notion de base de sous-réseau IP. Le plan de numérotage doit fonctionner avec ces nouvelles idées. Les réseaux pontés traditionnels et les réseaux commutés à **leading-edge workgroup** *(voir note ci-dessous)* peuvent très bien devoir subir des changements de la structure des sous-réseaux. Les besoins du dénumérotage peuvent aussi se développer avec l'introduction de nouvelles technologies de WAN, en particulier des services de multi-accès sans diffusion (NBMA, *nonbroadcast multiaccess*) comme le relais de trame. D'autres technologies de WAN, telles que de supports à numérotation qui utilisent des modems ou le RNIS, peuvent aussi avoir de nouvelles exigences d'acheminement et de numérotation. Les services de circuit virtuel commuté comme l'ATM, X.25, ou le relais de trame commuté interagissent aussi avec l'acheminement et l'adressage.
(Note du traducteur : Il n'a pas été possible d'obtenir de Howard C. Berkowitz qu'il s'explique sur cette expression qu'il est seul au monde à utiliser. "Leading-edge" peut signifier selon le contexte "bord antérieur", "bord d'attaque", "front d'impulsion", "bout d'engagement", à quoi je n'ai pas trouve de sens dans ce contexte ci.)

3.1 Acheminement mondial sur l'Internet

De nombreuses discussions sur le dénumérotage soulignent les interactions entre les plans de numérotage des organisations et ceux de l'Internet mondial [RFC1900]. Il peut aussi y avoir de fortes motivations en faveur de la dénumérotation dans des organisations qui ne se connectent jamais à l'Internet mondial.

Selon la RFC1900, "Tant que des solutions de remplacement viables ne seront pas développées, un déploiement étendu de l'acheminement inter domaine sans classes (CIDR, *Classless Inter-Domain Routing*) est vital pour garder en vie le système d'acheminement de l'Internet et conserver sans interruption la poursuite de la croissance de l'Internet.....Pour contenir la croissance des informations d'acheminement, chaque fois qu'une telle organisation change de fournisseur de service, les adresses de l'organisation devront changer.

À l'occasion, les fournisseurs de service peuvent devoir eux-mêmes changer pour un nouveau bloc d'adresses plus grand. Dans l'un ou l'autre de ces cas, pour contenir la croissance des informations d'acheminement, les organisations concernées devront dénuméroter.... Si l'organisation n'est pas dénumérotée, les conséquences potentielles incluent (a) une connexité IP limitée (moins que l'Internet mondial) ou (b) des coûts supplémentaires pour supporter les redondances associées aux informations d'acheminement de l'organisation que les fournisseurs d'accès Internet devront entretenir, ou les deux."

3.2 Limitations des ponts ; utilisation interne de la commutation de LAN

L'introduction de commutateurs de groupes peut induire des besoins de dénumérotation subtils. Fondamentalement, les commutateurs de groupes sont des ponts spécialisés, à hautes performances, qui prennent leurs principales décisions de transmission sur la base des informations d'adresse de couche 2 (MAC). Même ainsi, ils sont rarement indépendants de la structure d'adresse de couche 3 (IP). La pure commutation de couche 2 a un espace d'adresse "plat" qui va devoir être dénuméroté dans un espace de sous-réseaux hiérarchisé, cohérent avec l'acheminement. Les réseaux pontés traditionnels partagent beaucoup des problèmes des commutateurs de groupes, mais ils ont des problèmes de performances supplémentaires lorsque la connexité pontée s'étend sur des liaisons de WAN lentes.

L'introduction de commutateurs seuls ou de piles de commutateurs peut ne pas avoir un impact significatif sur l'adressage, pour autant qu'on se souvienne que chaque système de commutateurs est un seul domaine de diffusion. Chaque domaine de diffusion devrait se transposer en un seul sous-réseau IP.

Les LAN virtuels (VLAN) étendent encore plus la complexité du rôle des commutateurs de groupes. Il est généralement vrai que de déplacer une station d'extrémité d'un accès de commutateur à un autre au sein d'un VLAN de même "couleur" ne va pas causer de changements majeurs de l'adressage. De nombreuses discussions sur cette technologie n'ont pas éclairci le point de savoir si le déplacement de la même station d'extrémité entre différentes couleurs va faire passer la station d'extrémité dans un autre sous-réseau IP, exigeant un changement d'adresse significatif.

Les commutateurs sont normalement gérés par des applications SNMP. Ces applications de gestion de réseau communiquent avec des appareils gérés utilisant IP. Même si le commutateur ne fait pas la transmission IP, il aura besoin pour lui-même d'adresses IP pour sa gestion. Aussi, si les clients et les serveurs dans le groupe sont gérés pas SNMP, ils auront besoin d'adresses IP. Le groupe devra donc apparaître comme un ou plusieurs sous-réseaux IP.

De plus en plus, les produits de l'inter-réseau ne sont plus des appareils de pure couche 2 ou couche 3. Un produit de commutateur de groupe comporte souvent une fonction de routeur, de sorte que le plan de numérotage doit prendre en charge à la fois des adresses de couche 2 plates et des adresses hiérarchiques de couche 3.

3.3 Utilisation interne des services de nuage NBMA

Les services de "nuage" comme le relais de trame sont souvent plus économiques que les services traditionnels. À première vue, quand on convertit des réseaux d'entreprise existants en NBMA, il peut paraître que la structure de sous-réseau existante devrait être préservée, mais ce n'est souvent pas le cas.

De nombreuses organisations commencent souvent par traiter le "nuage" comme un seul sous-réseau, mais l'expérience montre qu'il est souvent préférable de traiter les circuits virtuels individuels comme des sous-réseaux distincts. Lorsque les VC point à point individuels deviennent des sous-réseaux distincts, l'utilisation efficace des adresses exige l'utilisation de préfixes /30 pour ces sous-réseaux. Cela veut normalement dire que l'adressage et le plan d'acheminement doivent prendre en charge cette longueur de préfixe, établissant une ou plusieurs longueurs de préfixe pour le support LAN avec plus de deux hôtes, et subdivisant un ou plusieurs de ces plus courts préfixes en préfixes /30 plus longs qui minimisent la perte d'adresses.

Il y a d'autres moyens de configurer l'acheminement sur des NBMA, en utilisant des mécanismes particuliers pour exploiter ou simuler des VC en point à multipoint. Ils ont souvent un impact significatif sur les performances du routeur, et peuvent être moins fiables parce qu'un seul point de défaillance est créé. Les mécanismes de ces solutions de remplacement sont exposés plus loin, mais leur motivations tendent à inclure :

1. le désir de ne pas utiliser VLSM, ce qui est souvent fondé sur la peur plutôt que sur la technologie ;
2. des questions de mise en œuvre de routeur qui limitent le nombre de sous-réseaux ou d'interfaces qu'un routeur peut prendre en charge ;
3. une application par nature en point à multipoint (par exemple, des hôtes distants sur un centre de données). Dans de tels cas, certaines des limitations sont dues au protocole d'acheminement dynamique utilisé. Dans de telles applications "en étoile", l'acheminement statique peut en fait être préférable du point de vue des performances et de la souplesse, car il ne produit pas de trafic d'acheminement et n'est pas affecté par l'horizon partagé.

Pour comprendre comment l'utilisation de services NBMA affecte la structure d'adressage et des routeurs, il vaut la peine de passer en revue les concepts de base des sous-réseaux IP. La vison traditionnelle est qu'un seul sous-réseau est associé à un seul support physique. Tous les hôtes physiquement connectés à ce support sont supposés être capables d'atteindre tous les autres hôtes sur le même support, en utilisant des services de niveau liaison. Ces services sont spécifiques du support : les hôtes connectés à un support de LAN peuvent faire des diffusions les uns aux autres, alors que les hôtes connectés à une ligne en point à point ont simplement besoin de transmettre à l'autre extrémité.

Lorsque un hôte désire transmettre à un autre, il détermine d'abord si la destination est locale ou distante. Une destination locale est sur le même sous-réseau et est supposée être accessible par des services de liaison de données. Une destination distante est sur un sous-réseau différent, et il est supposé que l'intervention d'un routeur est nécessaire pour l'atteindre.

Le premier problème de NBMA survient lorsque un seul sous-réseau est mis en œuvre sur un service NBMA. Le relais de trame fournit des circuits virtuels uniques entre les hôtes qui ont la connexité. Il est assez courant de concevoir les services de relais de trame comme des maillages partiels, où tous les hôtes n'ont pas de VC avec tous les autres. Lorsque l'ensemble des hôtes dans un maillage partiel est dans un seul sous-réseau IP, le maillage partiel viole le modèle local de pleine connexité. Même lorsque il y a un maillage complet, un modèle pessimiste mais raisonnablement fonctionnel doit considérer que les VC individuels échouent, et que la pleine connexité peut être perdue de façon transitoire.

Il y a plusieurs façons de traiter cette violation, chacune ayant ses propres limitations. Si un hôte "central" spécifique a la connexité avec tous les N autres hôtes, cet hôte central peut dupliquer toutes les trames qu'il reçoit d'un hôte sur les VC sortants qui le connectent avec les (N-1) autres hôtes dans le sous-réseau. Une telle réplication cause normalement une charge appréciable de CPU dans le routeur de réplication. Le routeur de réplication est aussi un seul point de défaillance pour le sous-réseau. Cette méthode ne s'adapte pas bien lorsque elle est étendue à des maillages plus complets au sein du sous-réseau.

Dans un protocole d'acheminement, tel que OSPF, qui a un concept de routeurs désignés, la configuration explicite est normalement nécessaire. Un autre problème de l'utilisation d'un sous-réseau maillé est que tous les VC peuvent ne pas avoir les mêmes performances, mais le routeur ne peut pas préférer des chemins individuels au sein du sous-réseau.

Une des méthodes les plus simples est de ne pas tenter d'émuler un support de diffusion, mais de traiter simplement chaque VC comme un sous-réseau distinct. Cela causera alors un besoin de dénumérotation. L'utilisation efficace de l'espace d'adresses impose l'utilisation d'un préfixe /30 pour les sous-réseaux par VC. Un tel préfixe a souvent besoin d'une prise en charge de VLSM dans les routeurs.

3.4 Expansion des services par numérotation

Les services par numérotation, en particulier ceux des fournisseurs d'accès Internet public, connaissent une croissance explosive. Ce succès représente une pression particulière sur la disponibilité de l'espace d'adresses, en particulier avec la pratique courante d'allouer des adresses univoques à chaque abonné.

Dans cette pratique, l'utilisateur individuel annonce son adresse au serveur d'accès en utilisant l'option de configuration IP de PPP [RFC1332]. Le serveur peut valider l'adresse proposée au vu d'un identifiant d'utilisateur, ou simplement rendre l'adresse active dans un sous-réseau auquel appartient le serveur d'accès (ou un ensemble de serveurs d'accès pontés).

Ces fonctions de serveur d'accès peuvent faire partie du logiciel d'un "routeur" et rentrent donc dans le domaine d'application du présent guide.

La technique préférée [RFC2050] est d'allouer de façon dynamique les adresses à l'utilisateur à partir d'un réservoir d'adresses disponibles au serveur d'accès. Divers mécanismes sont en fait utilisés pour faire cette allocation, et sont exposés au paragraphe 5.5.

3.5 Utilisation interne des services de circuit virtuel commutés

Des services comme les circuits virtuels ATM, le relais de trame commuté, etc., présentent des défis qui n'étaient pas pris en compte dans la conception IP originale. La décision de base de IP pour la transmission d'un paquet est de savoir si la destination est locale ou distante, en relation avec le sous-réseau de l'hôte de source. Les mécanismes de résolution d'adresse sont utilisés pour trouver l'adresse du support de la destination dans le cas de destinations locales, ou de trouver l'adresse du support du routeur dans le cas de routeurs distants.

Dans ces nouveaux services, il y a des cas où il est beaucoup plus efficace de "prendre un raccourci" par un nouveau circuit virtuel pour la destination. Si la destination est sur un sous-réseau différent de celui de la source, le raccourci est normalement par le routeur de sortie qui dessert le sous-réseau de destination.

L'avantage du raccourci dans un tel cas est qu'il évite la latence de plusieurs bonds de routeur, et réduit la charge sur les routeurs de "cœur de réseau". La décision du raccourci est normalement prise par un routeur d'entrée qui est au courant à la fois des environnements d'acheminement et de commutation.

Ce routeur d'entrée communique avec un serveur de résolution d'adresse en utilisant le protocole de résolution du prochain bond (NHRP, *Next Hop Resolution Protocol*) [RFC2332] [RFC2333]. Ce serveur transpose l'adresse réseau de destination en routeur de prochain bond (lorsque le raccourci n'est pas approprié) ou en un routeur de sortie atteint sur le service commuté. Évidemment, la base de données dans un tel serveur peut être affectée par la dénumérotation. Les clients peuvent avoir une adresse incorporée du serveur, qui elle aussi devra être changée.

Alors que les spécifications du protocole NHRP évoluent encore au moment de la rédaction du présent mémoire, les mises en œuvre commerciales fondées sur des projets du protocole standard sont utilisées.

4. Numérotage et dénumérotage

Quel est le rôle de tout plan de numérotage ? Pour comprendre le problème général, il peut être utile de revoir les principes de base des routeurs. Bien que la plupart des lecteurs en aient une bonne connaissance intuitive, les principes ont été précisés par l'usage courant de IP.

Un routeur reçoit un datagramme IP entrant sur une de ses interfaces, et il examine un certain nombre de bits de l'adresse de destination. La séquence de bits examinée par le routeur commence toujours à la gauche de l'adresse (c'est-à-dire, par le bit de poids fort). On appelle cette séquence un "préfixe."

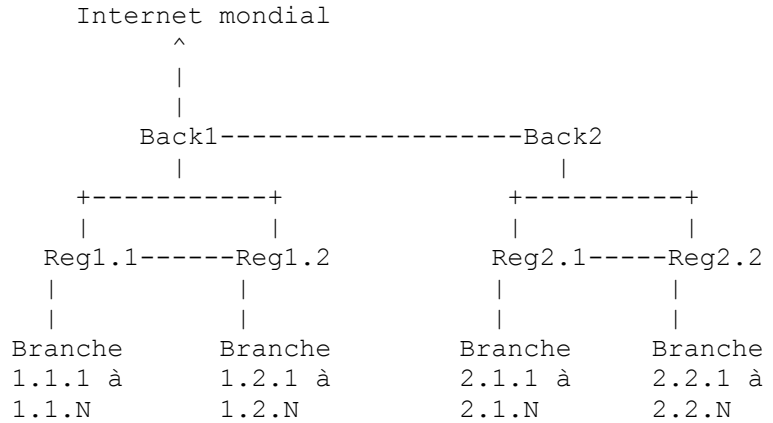
Les décisions d'acheminement sont prises sur les bits de totalPrefix, qui débute à la position binaire la plus à gauche (c'est-à-dire, de poids fort) de l'adresse IP. Ces totalPrefix bits peuvent être complètement sous le contrôle de l'entreprise (par exemple, si ils sont dans l'espace d'adresse privé) ou l'entreprise peut contrôler les lowOrderPrefix bits alors que les highOrderPrefix bits sont alloués par une organisation extérieure.

Le routeur cherche le préfixe dans son tableau d'acheminement (formellement appelé une base de données d'informations de transmission). Si le préfixe est dans le tableau d'acheminement, le routeur choisit alors une interface sortante qui va emmener le paquet acheminé à l'adresse IP du prochain bond sur le chemin de bout en bout. Si le préfixe ne peut être trouvé dans le tableau d'acheminement, le routeur retourne un message ICMP Destination inaccessible à l'adresse de source du datagramme reçu.

En supposant que le préfixe est trouvé dans le tableau d'acheminement, le routeur transmet alors le datagramme à travers l'interface sortante indiquée. Si l'acheminement en diffusion groupée est utilisé, le datagramme peut être copié et envoyé sur plusieurs interfaces sortantes.

4.1 Catégorisation de la topologie

Dans la perspective de la dénumérotation de routeur, l'impact d'une dénumérotation sera plus grand dans les parties les plus connectées du "cœur de réseau," et moindre dans les parties de "bout" du domaine d'acheminement qui ont un seul chemin au cœur de réseau.



Dans ce dessin, on suppose que Back1 et Back2 échangent des chemins complets ; Back1 est aussi le routeur extérieur. Les

routeurs régionaux (Reg) échangent des chemins complets les uns avec les autres et agrègent les adresses aux routeurs de cœur de réseau. Les routeurs de branche échangent par défaut avec les routeurs régionaux.

D'un pur point de vue topologique, plus on est haut dans la hiérarchie, plus on est apte à subir les effets du dénumérotage. C'est une première approximation pour apprécier la portée de la tâche, en supposant que les adresses ont été allouées systématiquement. Un espace d'adresses systématique est rarement le cas dans les réseaux traditionnels.

4.2 Catégorisation de l'espace d'adresses

Un inventaire de l'espace d'adresses présent et prévu est un pré requis pour la réussite d'un dénumérotage. On commence par identifier les préfixes existants ou prévus dans le réseau, et si ils ont été alloués d'une manière systématique et hiérarchique.

```
+--Non affecté par la dénumérotation [A]
|
+--Préfixes existants à dénuméroter
|   |
|   +----À dénuméroter directement le "jour J"
|   |
|   +----À dénuméroter initialement sur une adresse temporaire
|
+--Préfixes existants à retirer
|
+--Nouveaux préfixes prévus
    |
    +---Changement total de préfixe, longueur inchangée
    |
    +---Seule la partie de poids fort change, longueur inchangée
    |
    +---Seule la partie de moindre poids change, longueur inchangée
    |
    +---Seule la partie de poids fort change, sa longueur change
    |
    +---Seule la partie de moindre poids change, sa longueur change
    |
    +---Le préfixe total change, dans les parties de poids fort et de moindre poids
    |
    +---Seule la partie de poids fort change, longueur inchangée
```

Idéalement, un préfixe donné devrait être "inchangé", "vieux" ou "nouveau". Le dénumérotage sera plus facile si chaque "vieux" préfixe peut être transposé en un seul "nouveau" préfixe.

Malheureusement, l'idéal est souvent inaccessible. Il peut être nécessaire de faire évoluer des parties de l'espace d'adresse ancien et nouveau en parallèle.

Le dénumérotage s'applique d'abord aux préfixes et ensuite aux numéros d'hôte à la droite du préfixe. Pour comprendre la portée d'un dénumérotage, il est essentiel de :

1. identifier les préfixes (et éventuellement les champs d'hôte) potentiellement affectés par l'opération de dénumérotage ;

2. identifier l'autorité qui contrôle les valeurs du préfixe, ou de parties du préfixe, affectées par le dénumérotage.

Dans une entreprise, il peut y avoir des préfixes qui seront sous le contrôle complet ou partiel de l'entreprise, aussi bien que totalement en-dehors du contrôle de l'entreprise. Revoyons les principes du contrôle de l'espace d'adresses.

La plupart du temps, les bits de poids fort du préfixe sont alloués à l'entreprise par un registraire d'adresses (par exemple, InterNIC, RIPE, ou APNIC) ou par un fournisseur d'accès Internet (FAI). Cette allocation d'une valeur dans les positions binaires de poids fort a dans le passé été appelée un "numéro de réseau", quand la partie allouée de poids fort est longue de 8, 16, ou 24 bits. L'utilisation plus récente ne limite pas la partie allouée à une frontière d'octet. Le terme préféré pour la partie allouée est un "bloc CIDR" d'un certain nombre de bits [RFC1518].

L'entreprise étend alors le préfixe sur la droite, créant des "sous-réseaux". Il est critique de réaliser que les routeurs

prennent les décisions d'acheminement sur la base de la totalité du préfixe en cause, sans considération de qui contrôle quels bits. En d'autres termes, le routeur ne sait pas et ne veut pas savoir en réalité quelles sont les frontières de sous-réseau.

Il faut penser le sous-réseautage comme le moyen de créer un plus long préfixe. Même avant le CIDR, on agrégeait plusieurs sous-réseaux en une seule annonce de numéro de réseau envoyée aux routeurs externes. D'une façon plus générale, on pense maintenant à étendre le préfixe sur la droite au titre du sous-réseautage, et à l'agréger sur la gauche en terme de super-réseautage, agrégation, ou résumé. Selon l'usage du sous-réseautage ou de l'agrégation, différentes longueurs de préfixe sont significatives pour des interfaces de routeur différentes.

4.3 Portée d'un dénumérotage

Des préfixes tirés de l'espace d'adresse privé de la [RFC1918] peuvent n'être pas acheminables sur l'Internet mondial. Comme ces adresses ne sont pas acheminables sur l'Internet mondial, le changement de parties de préfixes de l'espace d'adresses privé est une décision locale de l'entreprise.

Si un préfixe est totalement en-dehors du contrôle de l'entreprise, il est externe, et ne sera que peu affecté par l'acheminement. Des interactions potentielles de préfixes externes avec la dénumérotation d'une entreprise incluent :

1) une altération ou suppression accidentelle d'adresses externes au titre de la reconfiguration de routeur,
2) la perte de connexité avec les serveurs d'application à l'intérieur de l'entreprise, parce que le client externe ne sait plus l'adresse interne du serveur,
3) DNS/BGP,
4) la sécurité.

Les préfixes qui sont partiellement sous le contrôle de l'entreprise peuvent changer. La portée de ce changement va largement varier selon que seule la partie contrôlée en externe change, ou si une partie de la partie contrôlée en interne doit être dénumérotée. Si la longueur de l'une ou l'autre des parties de poids fort ou de moindre poids change, le processus devient plus complexe.

Un dénumérotage de la seule partie de poids fort est le plus courant lorsque une organisation change de FAI, et a besoin de se renuméroter dans l'espace du nouveau fournisseur. L'ancien préfixe peut avoir été alloué à l'entreprise mais ne sera plus utilisé pour l'acheminement mondial, ou l'ancien préfixe peut avoir été alloué au fournisseur précédent. Noter que des procédures administratives peuvent être nécessaires pour restituer le préfixe précédent, bien que ceci soit habituellement fait par l'ancien fournisseur. Il sera souvent nécessaire d'avoir une période de coexistence entre l'ancien et le nouveau préfixe.

Les dénumérotations de la seule partie de moindre poids peuvent survenir lorsque une entreprise modifie sa structure interne d'acheminement, et que les changements n'affectent que la structure de sous-réseaux interne du réseau de l'entreprise. Ceci est typique des efforts impliqués par l'augmentation du nombre de sous-réseaux disponibles (par exemple, pour plus de supports en point à point) ou par l'augmentation du nombre d'hôtes sur un support (par exemple, un plus grand usage de commutateurs de groupes).

Les parties de poids fort et de moindre poids peuvent changer toutes deux. Cela peut arriver lorsque l'entreprise passe chez un nouveau FAI, qui alloue de l'espace d'adresse à partir d'un bloc CIDR plutôt que d'un réseau à classes utilisé précédemment. Avec une longueur de préfixe de poids fort différente, l'entreprise pourrait être forcée de changer sa structure de sous-réseaux.

5. Passer à un modèle de dénumérotage facile

Le dénumérotage affecte à la fois la configuration de "boîtes de routeur spécifiques, et le système global de routeurs dans un domaine d'acheminement. La présente section met l'accent sur les moyens de rendre plus facile le dénumérotage pour l'entreprise, avant qu'aucun préfixe ne soit réellement changé.

Le dénumérotage aura le moins d'impact lorsque le nombre minimum d'options de reconfiguration sont nécessaires. Lorsque on prévoit un dénumérotage sur des routeurs, on considère que beaucoup de configurations existantes peuvent contenir des adresses IP incorporées qui peuvent n'être pas nécessaires, même si le dénumérotage ne devait pas se produire. Une partie de l'effort de dénumérotage d'un routeur devrait inclure, chaque fois que possible, de remplacer les mécanismes de routeur fondés sur des adresses incorporées par des mécanismes plus souples.

Le dénumérotage sera aussi généralement plus facile si les changements de configuration peuvent être faits hors ligne sur des serveurs appropriés, puis téléchargés par le routeur, si la mise en œuvre de routeur le permet.

5.1 Chemins par défaut

Une méthode bien connue pour réduire la quantité de références d'un routeur aux autres routeurs est d'utiliser un chemin par défaut vers un routeur mieux connecté de niveau supérieur. Cela suppose une conception hiérarchique du réseau, qui est généralement souhaitable dans l'intérêt de l'adaptabilité.

Les chemins par défaut sont les plus appropriés pour les routeurs de bout au sein d'un domaine d'acheminement, et pour les routeurs frontières qui connectent le domaine à un seul FAI.

5.2 Récapitulation des chemins et CIDR

Lorsque il est nécessaire d'annoncer des chemins, résumer autant que faire se peut. Le résumé est le plus efficace lorsque les préfixes d'adresses ont été alloués de façon cohérente et contiguë, ce qui n'est souvent pas le cas dans les réseaux traditionnels. Néanmoins, il y a moins à changer quand on peut se référer à des blocs de préfixes.

Tous les mécanismes d'acheminement ne prennent pas en charge la constitution générale de résumés. Les mécanismes d'acheminement intérieur incluent RIPv2, OSPF, EIGRP, IS-IS, et les systèmes de chemins statiques. RIPv1 et IGRP prennent en charge la mise en résumé selon les classes de réseau (c'est-à-dire, seulement aux frontières de réseau de classe A/B/C).

Si les adresses existantes ont été allouées de façon hiérarchique, il est possible de dénuméroter en dessous du niveau de résumé, tout en cachant le résumé au reste du réseau. En d'autres termes, si tous les bits de l'adresse dénumérotée sont à la droite de la longueur du préfixe résumé, le changement peut être transparent au système d'acheminement global.

Même lorsque le résumé effectif est possible pour cacher les détails de l'acheminement, le DNS, les filtres, et les autres services peuvent être affectés par un dénumérotage.

5.3 Références aux serveurs dans les routeurs

Les routeurs communiquent couramment avec un assortiment de serveurs de gestion de réseau et autres serveurs de l'infrastructure. Des exemples de ces serveurs sont donnés à la Section 12 "Gestion de réseau". Le DNS lui-même peut cependant être une exception importante.

Chaque fois que possible, les serveurs devraient être référencés par le nom du DNS plutôt que par l'adresse IP. Si une mise en œuvre spécifique de routeur ne prend en charge que les références d'adresse explicites, cela devrait être documenté au titre du plan de dénumérotage.

Les routeurs peuvent aussi avoir besoin de transmettre des diffusions d'hôtes d'extrémité aux autres services d'infrastructure (par exemple, DNS, DHCP/BOOTP). Les configurations qui font cela vont vraisemblablement contenir des adresses IP incorporées des hôtes de destination ou de leurs sous-réseaux, qui vont devoir être changées au titre de la dénumérotation.

5.4 Le DNS et la dénumérotation de routeur

Le service des noms de domaines est un outils puissant dans tout effort de dénumérotage, et il peut aider les routeurs aussi bien que les hôtes d'extrémité. Si traceroute affiche les noms du DNS plutôt que les adresses IP, certaines options de débogage peuvent êtres transparentes à travers la transition d'adresse.

Il faut être conscient que les noms et adresses appris de façon dynamique peuvent être mis en antémémoire dans les tableaux d'acheminement des routeurs. Pour qu'un routeur apprenne les changements des correspondances de nom à adresse, il peut être nécessaire de redémarrer le routeur ou de purger explicitement l'antémémoire.

Autrement, les fichiers de configuration du routeur peuvent contenir des correspondances incorporées de nom/adresse qui ne seront pas affectées par un changement dans le serveur du DNS.

Différentes bases de données du DNS sont affectées par la dénumérotation. Par exemple, l'entreprise contrôle normalement sa propre base de données de "transmission", mais la base de données de transposition inverse peut être entretenue par son FAI. Cela peut exiger une coordination lors d'un changement de fournisseurs.

Normalement, une dénumérotation de routeur passe par une période de transition. Durant cette transition, anciennes et nouvelles adresses peuvent coexister dans le système d'acheminement. La coexistence sur une durée significative est particulièrement vraisemblable pour les références du DNS aux adresses qui sont connues dans l'Internet mondial [deGroot]. Divers serveurs DNS tout autour du monde peuvent mettre des adresses en antémémoire pendant plusieurs jours.

Si, par exemple, une certaine interface de routeur se trouve avoir une ancienne et une nouvelle adresse qui coexistent, il peut être approprié d'introduire la nouvelle adresse comme un nouvel enregistrement A pour la nouvelle adresse.

Les déclarations d'enregistrement de ressource (RR) du DNS peuvent se terminer par un point virgule qui indique que le reste de la ligne est un commentaire. Cela peut être utilisé comme outils de base pour renuméroter les noms du DNS en adresses de routeurs, en mettant un commentaire (par exemple, ";nouvelle adresse") à la fin des déclarations A des nouvelles adresses. Au moment approprié, un script peut générer un nouveau fichier de zone dans lequel les nouvelles adresses deviennent les définitions primaires dans les enregistrements A, et les anciennes adresses peuvent devenir des enregistrements A munis des commentaires appropriés. Ultérieurement, ces entrées commentées pourront être supprimées.

Il faut prendre soin de s'assurer que les entrées de transposition inverse de pointeur sont définies pour les nouvelles adresses, parce que les outils de certains fabricants de routeurs dépendent de la transposition inverse.

5.5 Adressage dynamique

Le dénumérotage est plus facile lorsque les adresses doivent être changées dans le plus petit nombre possible d'endroits. L'allocation dynamique des adresses est particulièrement intéressante pour les hôtes d'extrémité et les routeurs peuvent jouer un rôle clé dans ce processus. Les routeurs peuvent agir comme des serveurs et allouer en fait les adresses, ou peuvent être chargés de transmettre les demandes d'allocation d'adresse des hôtes d'extrémité aux serveurs d'allocation d'adresses.

L'utilisation la plus courante de l'allocation dynamique d'adresses est de fournir des adresses IP aux systèmes d'extrémité. L'allocation dynamique d'adresses est cependant aussi utilisée pour allouer des adresses IP aux interfaces des routeurs. Un serveur d'allocation d'adresse peut allouer une adresse IP à un routeur de la façon habituelle de DHCP, sur la base d'une adresse MAC dans le routeur, ou simplement sur la base de la connexité physique du nouveau routeur. En d'autres termes, tout routeur connecté sur une interface spécifique du routeur de configuration se verra alloué la même adresse IP.

5.5.1 Rôles de routeur dans une allocation d'adresse DHCP fondée sur le LAN

Les hôtes d'extrémité rattachés à des LAN obtiennent souvent des allocations d'adresses de serveurs BOOTP ou DHCP. Si le serveur n'est pas sur le même support que les hôtes d'extrémité, les routeurs peuvent avoir besoin de jouer un rôle dans l'établissement de la connexité entre l'hôte d'extrémité et le serveur d'adresses.

Si le client n'est pas sur le même support que le serveur d'allocation d'adresses, les routeurs doivent agir comme des services l'allocation d'adresse, ou transmettre des diffusions limitées à la localisation des serveurs appropriés.

Si le routeur agit comme serveur d'allocation d'adresses, sa base de données d'adresses qu'il peut allouer peut changer durant la dénumérotation. Si le routeur transmet à un serveur DHCP ou BOOTP, il doit savoir l'adresse de ce serveur. Cette adresse de serveur peut elle-même changer par suite du dénumérotage.

Bien que la perception habituelle de DHCP est qu'il alloue des adresses à partir d'un réservoir, de telle sorte que les allocations à un hôte donné à un moment donné soient aléatoires au sein du réservoir, DHCP peut aussi retourner une adresse IP constante pour une adresse MAC spécifique. Cela peut être beaucoup plus facile à gérer et dépanner, en particulier durant un dénumérotage.

Évidemment, si le serveur DHCP identifie des hôtes d'extrémité sur la base de leur adresse MAC, on doit veiller à faire que ces adresses soient univoques, et à changer la base de données DHCP si l'adresse MAC ou l'adresse IP change. Une façon de réduire de telles reconfigurations est d'utiliser des adresses administrées localement (LAA, *Locally-Administered Address*) sur les hôtes d'extrémité, plutôt que des adresses uniques au monde mémorisées dans une mémoire morte (ROM, *read-only memory*). L'utilisation des LAA résout le problème du changement des adresses MAC lorsque change une carte d'interface de réseau, mais les LAA ont leurs propres problèmes de gestion de configuration dans les systèmes d'extrémité et de conservation de l'unicité au sein de l'entreprise.

5.5.2 Rôles de routeur dans une allocation d'adresse par numérotation

Il y a plusieurs façons possibles pour un hôte d'extrémité à numérotation pour interagir avec des allocations d'adresse. Les serveurs routeurs/d'accès peuvent jouer un rôle critique dans ce processus, soit en fournissant la connexité entre client et serveur, soit en allouant directement les adresses.

Les différents fabricants traitent de différentes façons l'allocation d'adresse. Ces méthodes incluent :

1. Le serveur d'accès transmet la demande à un serveur DHCP, en utilisant un identifiant unique de 48 bits associé au client. Noter que ceci ne devrait normalement pas être l'adresse MAC du serveur d'accès, car la même adresse MAC

serait alors associée à des hôtes différents.
2. Le serveur transmet la demande à un serveur d'authentification, qui à son tour obtient une adresse dynamique :
   a. soit de réservoirs internes,
   b. soit d'un serveur DHCP auquel il transmet.
3. Le serveur choisit une adresse à partir de réservoirs configurés localement et la fournit à l'hôte numéroteur sans l'intervention d'autres services.

Lorsque le routeur contient des adresses allouables, celles-ci peuvent avoir besoin de changer au titre d'une dénumérotation. Autrement, les références incorporées au serveur d'allocation d'adresse ou d'authentification peuvent devoir être changées.

5.5.3 Auto configuration de routeur

Cette allocation initiale d'adresse peut ne fournir une adresse que pour une seule connexion (c'est-à-dire, entre le nouveau routeur et celui qui fait la configuration). La nouvelle adresse allouée peut alors être utilisée pour "amorcer" une configuration complète dans le nouveau routeur.

L'allocation dynamique d'adresse aux routeurs est probablement très courante chez les routeurs "de bout" ou "de bordure" qui se connectent à un serveur de configuration via des liaisons de WAN à une localisation centrale. De tels appareils de bordure peuvent être expédiés sur un site distant, branchés sur une ligne de WAN, et utiliser des méthodes non normalisées pour acquérir tout ou partie de leur configuration d'adresse.

Lorsque une telle autoconfiguration est utilisée sur des routeurs de bordure, il peut être nécessaire de forcer un redémarrage sur le routeur de bordure après la dénumérotation. Le redémarrage peut être la seule façon de forcer le routeur autoconfiguré à apprendre sa nouvelle adresse. D'autres méthodes hors bande peuvent être disponibles pour changer les adresses des routeurs de bordure.

5.6 Traduction d'adresse réseau

La traduction d'adresse réseau (NAT, *Network Address Translation*) est une technique précieuse pour une dénumérotation, ou même pour éviter le besoin de dénuméroter une partie significative d'une entreprise [RFC1631]. Elle n'est pas toujours transparente aux protocoles de couche réseau, aux protocoles de couche supérieure, et aux outils de gestion de réseau, et elle ne doit pas être considérée comme une panacée.

Dans la définition classique de la NAT, certaines parties du système d'acheminement sont appelés des domaines de bout, et ne sont connectés au domaine mondial que par des fonctions de NAT. Le traducteur d'adresse réseau contient un mécanisme de traduction qui transpose une adresse de bout en adresse mondiale. Ce mécanisme peut transposer de façon statique ou dynamique.

Un mécanisme de NAT plus général est souvent mis en œuvre dans les défenses de pare-feu des hôtes, qui isolent les adresses de "l'intérieur" et de "l'extérieur" à travers des passerelles authentifiées de niveau transport ou application. Les transpositions d'adresse "locale" ou "intérieure" en adresse mondiale ne sont souvent pas bijectives, parce que une adresse intérieure est transposée de façon dynamique en un accès TCP ou UDP sur une adresse d'interface extérieure.

En général, si il y a plusieurs NAT, leurs mécanismes de traduction devraient être synchronisés. Il y a des cas spécialisés lorsque une adresse de bout donnée apparaît dans plus d'un domaine de bout, et des ambiguïtés surviennent si on souhaite transposer, disons de 10.1.0.1/16 dans le domaine de bout A en 10.1.0.1/16 dans le domaine de bout B. Dans ce cas, les deux adresses 10.1.0.1 identifient des hôtes différents. Des mécanismes spéciaux devraient exister pour transposer l'adresse locale du domaine A en une adresse mondiale, et pour transposer l'adresse locale du domaine B en une adresse mondiale différente

La NAT peut jouer un rôle précieux dans un dénumérotage. Son utilisation intelligente peut grandement minimiser la quantité de dénumérotage qui doit être faite. La NAT n'est cependant pas complètement transparente.

Précisément, elle peut interférer avec le fonctionnement propre de tout protocole qui porte une adresse IP dans ses données, car la NAT ne comprend pas la différence entre les champs transportés et ne sait pas quels numéros doivent être changés.

Des exemples de protocoles affectés sont :
-- Les sommes de contrôle TCP et UDP qui sont en partie fondées sur l'en-tête IP. Cela inclut les schémas de chiffrement de bout en bout qui comportent la somme de contrôle TCP/UDP.
-- Les messages ICMP qui contiennent des adresses IP.
-- Les interrogations au DNS qui retournent des adresses ou envoient des adresses.
-- Les interactions FTP qui utilisent une adresse IP codée en ASCII au titre de la commande PORT.

Il est possible d'éviter le conflit si seulement certains hôtes utilisent les protocoles affectés. On pourrait n'allouer à de tels hôtes que des adresses mondiales, si la topologie du réseau et le plan d'acheminement le permettent.

Les premières expériences de NAT suggéraient qu'elle avait besoin d'une base de données de transposition du trafic épars de bout en bout pour avoir des performances raisonnables. Cela peut être ou non un problème dans des mises en œuvre de NAT fondées plus sur le matériel.

Un autre problème avec la NAT est que les adresses univoques d'hôte sont cachées en-dehors des domaines locaux de bout. Cela peut en fait être souhaitable pour la sécurité, mais peut soulever des problèmes de gestion de réseau. Une possibilité serait de développer une MIB *(base de données d'informations de gestion)* de NAT qui pourrait être interrogée par SNMP pour trouver les transpositions spécifiques de local à mondial utilisées.

Il y a aussi des problèmes pour le DNS, DHCP, et d'autres services de gestion d'adresses. On peut supposer qu'il sera besoin de serveurs locaux au sein des domaines de bout, de sorte que les demandes d'adresse soient résolues de façon univoque dans chaque bout (ou qu'elles retournent des adresses mondiales appropriées).

6. Pièges potentiels du dénumérotage de routeur

Une façon de catégoriser les pièges potentiels est de regarder ceux qui sont associés au plan de numérotage global lui-même et aux annonces d'acheminement, et à ceux associés au comportement du protocole. En général, le premier cas est statique et le dernier est dynamique.

6.1 Statique

Des problèmes peuvent être impliqués par la structure d'adresse/acheminement elle-même. Ils peuvent inclure des défaillances de composants à comprendre un adressage de préfixe arbitraire (c'est-à-dire, d'acheminement sans classe), d'accessibilité due à des chemins par défaut ou agrégés inappropriés, etc.

6.1.1 Considérations sur l'acheminement sans classe

Parmi les raisons majeures d'un dénumérotage se trouve le gain d'espace global d'adresses acheminables. Dans l'Internet mondial, l'espace d'adresse acheminable se fonde sur des préfixes de longueur arbitraire plutôt que sur les classes d'adresses traditionnelles. L'acheminement inter domaine sans classes (CIDR, *Classless Inter-Domain Routing*) est la réalisation administrative de l'adressage par préfixes dans l'Internet mondial. À l'intérieur des entreprises, on appelle souvent l'adressage par préfixes de longueur arbitraire un gabarit de sous-réseau de longueur variable (VLSM, *Variable Length Subnet Masking*) ou "sous-réseautage d'un sous-réseau."

Les règles générales de l'adressage par préfixe doivent être suivies dans le CIDR. Parmi elles se trouve celle de permettre l'usage de sous-réseaux tout de zéros et tout de uns [RFC1812], et de ne pas supposer qu'un chemin pour un "numéro de réseau de classe A/B/C" implique des chemins pour tous les sous-réseaux de ce réseau. On ne devrait pas non plus faire la supposition que une longueur de préfixe est impliquée par la structure des bits de poids fort de l'adresse IP (c'est-à-dire, la "règle du premier octet").

Cet idéal n'est malheureusement pas partagé par un nombre significatif de routeurs (et de serveurs d'accès terminaux qui participent à l'acheminement) et un nombre encore plus significatif de mises en œuvre d'hôte IP.

Lorsqu'ils prévoient une dénumérotation, les concepteurs de réseau doivent savoir si la nouvelle adresse a été allouée en utilisant les règles de CIDR plutôt que l'adressage traditionnel par classes. Si les règles de CIDR ont été suivies pour l'allocation des adresses, des mesures doivent alors être prises pour s'assurer que le routeur les comprend, ou alors des mesures appropriées doivent être prises pour créer une interface entre l'environnement existant et l'environnement de CIDR.

L'expérience actuelle suggère qu'il est préférable, lors d'un dénumérotage, de préserver la compatibilité future en passant à un environnement d'acheminement qui prend en charge le CIDR. Bien que cela soit vu habituellement comme signifiant l'introduction d'un protocole d'acheminement dynamique sans classes, cela ne veut pas dire que l'acheminement devient beaucoup plus complexe. Dans un environnement RIPv1, passer à RIPv2 peut être un changement relativement simple. D'autres méthodes simples incluent d'établir un chemin par défaut d'un domaine d'acheminement non conforme à CIDR à un fournisseur de service conforme à CIDR, ou d'utiliser des chemins statiques qui soient conformes à CIDR.

Certains routeurs prennent en charge l'acheminement sans classes sans autre configuration ; d'autres routeurs prennent en charge l'acheminement sans classes mais exigent des mesures de configuration spécifiques pour l'activer, alors que d'autres routeurs ne comprennent que l'acheminement par classes. En général, la plupart des dénumérotages vont finalement exiger la prise en charge de l'acheminement sans classes. Il est essentiel de savoir si un certain routeur peut prendre en charge l'acheminement sans classes. Si il ne le fait pas, des contournements sont peut-être possibles. Des contournements ont toutes chances d'être nécessaires.

6.1.1.1 Problèmes d'agrégation

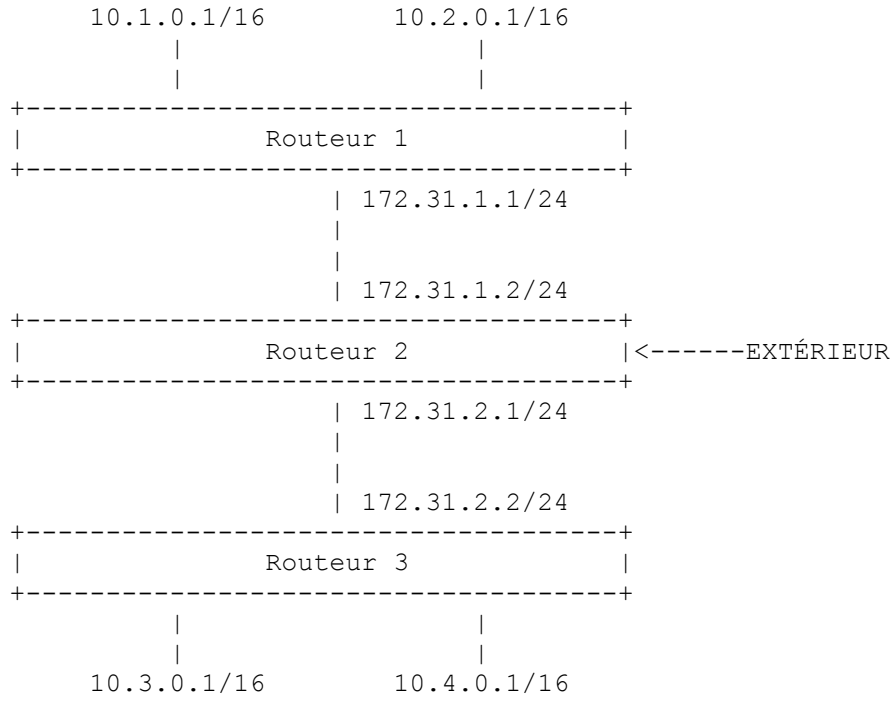
Lors de l'expérimentation de l'utilisation de CIDR sur un numéro de réseau anciennement de classe A, la [RFC1879] a montré que les règles de conformité à CIDR doivent être activées explicitement dans certains routeurs, alors que d'autres routeurs ne comprennent pas les règles de CIDR.

La [RFC1897] a démontré des problèmes avec certains équipements existants, en particulier, "les équipements qui dépendent de l'utilisation d'un protocole d'acheminement à classes, comme RIPv1, sont enclins aux défauts de configuration. Les exemples vérifiés sont courants : les matériels Ascend et Livingston, qui continuent d'utiliser RIPv1 comme protocole d'acheminement par défaut ou comme seul protocole. L'utilisation de RIPv1 va créer une annonce agrégée .... Il a été demandé au routeur Ascend d'annoncer 39.1.28/24, mais comme RIPv1 ne peut pas le faire, le matériel Ascend a envoyé 39/8 à la place." RIPv1, comme tous les protocoles intérieurs à classes est obsolescent.

6.1.1.2 Réseaux non contigus

Un autre problème qui peut survenir avec des routeurs ou des mécanismes d'acheminement qui ne comprennent pas qu'un adressage de préfixe de longueur arbitraire est celui de réseaux non contigus. Il est facile de créer involontairement ce problème lors d'un dénumérotage. Dans l'exemple ci-dessous, on suppose que l'entreprise a utilisé 10.0.0.0/8 comme préfixe principal, mais qu'elle a introduit un FAI dont les adresses enregistrées sont dans 172.31.0.0/16.

On suppose un système RIPv1 de trois routeurs :



Le routeur 1 peut atteindre ses deux sous-réseaux connectés localement, 10.1.0.0/16 et 10.2.0.0/16. Il va les agréger en une seule annonce de 10.0.0.0/8 lorsque il annonce à partir de l'interface 172.31.1.1.

De la même manière, le routeur 3 peut atteindre ses deux sous réseaux connectés localement, 0.3.0.0/16 et 10.4.0.0/16. Il va les agréger en une seule annonce de 10.0.0.0/8 lorsque il annonce à partir de l'interface 172.31.2.2.

Lorsque le routeur 2 reçoit un paquet de son interface "extérieure" destiné, par exemple, à 10.1.1.56/16, où l'envoi-t-il ? Le routeur 2 a reçu deux annonces de 10.0.0.0 sur des interfaces différentes, sans aucun détail de sous-réseau à l'intérieur de 10.0.0.0. Le routeur 2 a un tableau d'acheminement ambigu en termes de prochain bond vers un sous-réseau de 10.0.0.0. On

appelle ce problème, lorsque des parties du même réseau à classes sont séparées par différents réseaux, des sous-réseaux non contigus.

Deux problèmes surviennent dans cette configuration. Le routeur 2 ne sait pas où envoyer les paquets externes destinés à un sous-réseau de 10.0.0.0. La connexité sera cependant aussi rompue entre les routeurs 1 et 3, parce que le routeur 2 ne connaît pas le prochain bond pour tout sous-réseau de 10.0.0.0.

Il y a plusieurs façons de contourner ce problème. Évidemment, l'une d'elles serait de passer à un mécanisme d'acheminement qui annonce bien les sous-réseaux. Une autre sera d'établir un tunnel IP sur IP à travers le routeur 2, et de donner à cela un sous-réseau dans 10.0.0.0. Ce sous-réseau supplémentaire ne serait visible que dans les routeurs 1 et 3. Cela résoudrait le problème de connexité entre les routeurs 1 et 3, mais le routeur 2 ne serait toujours pas capable de transmettre les paquets externes. Cela peut être une solution parfaitement acceptable si le routeur 2 est simplement utilisé pour connecter deux parties de 10.0.0.0.

Une autre façon de traiter le problème du réseau non contigu est d'allouer des adresses secondaires dans le 10.0.0.0 aux interfaces R1-R2 et R2-R3, ce qui va permettre que les sous-réseaux 10.0.0.0 soient annoncés à R2. Cela va fonctionner tant qu'il n'y a pas de problème pour annoncer les sous-réseaux 10.0.0.0 dans le système d'acheminement de R2. Il restera encore un problème, par exemple, si l'adresse 10.0.0.0 était dans l'espace d'adresses privé mais que les adresses principales de R2 étaient enregistrées, et que R2 annonce les adresses 10.0.0.0 à l'extérieur.

Ce problème peut être traité si R2 a des mécanismes de filtrage qui puissent bloquer sélectivement les annonces de 10.0.0.0 au monde extérieur. Cependant, la configuration va devenir de plus en plus compliquée.

6.1.1.3 Interactions entre routeur et hôte

La situation peut n'être pas aussi sombre si les hôtes ne comprennent pas l'adressage par préfixe mais que les routeurs le font. Il existe des méthodes pour cacher une structure de VLSM aux hôtes qui ne le comprennent pas. Cela implique des mécanismes de protocole qui contournent la difficulté, mais le problème fondamental est celui de la compréhension par les hôtes des longueurs arbitraires de préfixe.

Un mécanisme clé est le mandataire ARP (*Address Resolution Protocol*, protocole de résolution d'adresse) [Carpenter]. Le mécanisme de base de l'utilisation du mandataire ARP dans un dénumérotage fondé sur le préfixe est de faire que les hôtes produisent un ARP chaque fois qu'ils veulent communiquer avec une destination. Si la destination est en fait sur le même sous-réseau, elle va répondre directement à l'ARP. Si la destination ne l'est pas, le routeur va répondre comme si il était la destination, et l'hôte d'origine va envoyer le datagramme au routeur. Une fois que le datagramme est dans le routeur, le routeur a capacité VLSM peut le transmettre.

Cependant, de nombreux hôtes d'extrémité ne vont produire d'ARP que si ils arrivent à la conclusion que la destination est sur leur propre sous-réseau. Tout le trafic autre est envoyé à une adresse de routeur par défaut incorporée. Dans de tels cas, des contournements peuvent être nécessaires pour forcer l'hôte à l'ARP pour toutes les destinations.

Une solution de rechange implique une mauvaise configuration délibérée des hôtes. Les hôtes qui ne comprennent que les routeurs par défaut ne sont également aptes qu'à comprendre l'adressage par classes. Si on dit à l'hôte que son réseau majeur (c'est-à-dire, à classes) n'a pas de sous-réseaux, même si le plan d'adresses est en fait en sous-réseaux, cela va souvent le persuader d'envoyer un ARP à toutes les destinations.

Cela fonctionne aussi pour les hôtes qui ne comprennent pas du tout le sous-réseautage. Un exemple va servir pour les deux niveaux de compréhension de l'hôte. Supposons que l'entreprise utilise 172.31.0.0/16 comme adresse majeure, qui est dans le format de classe B. Elle est en fait subdivisée en sous-réseaux avec huit bits de sous-réseau -- 172.31.0.0/24. Cependant les hôtes individuels sans capacité VLSM vont déduire la classe B de la valeur d'adresse, ou apprennent que le gabarit de sous-réseau effectif est 255.255.0.0.

Encore une autre approche qui aide les hôtes à trouver les routeurs est de faire fonctionner un RIP passif sur les hôtes, afin qu'ils entendent les mises à jour d'acheminement. On suppose que tout hôte qui produit des mises à jour d'acheminement doit être un routeur, de sorte que le trafic pour des destinations non locales peut y être transmis. Bien que RIPv1 ne prenne pas en charge les préfixes arbitraires, le ou les routeurs qui produisent les mises à jour d'acheminement peuvent avoir des capacités supplémentaires qui leur permettent de transmettre correctement un tel trafic. La priorité est donc d'obtenir les routeurs non locaux pour un routeur qui comprend la structure globale d'acheminement, et RIP passif peut être une façon viable de le faire.

Il peut être approprié de trancher site par site [Lear]. Dans une telle approche, certains sites ont des hôtes à capacité VLSM, mais d'autres n'en ont pas. Tant que la structure d'acheminement prend en charge VLSM, des solutions de remplacement peuvent être appliquées lorsque nécessaire.

6.1.2 Interactions d'adresses MAC

Bien qu'il soit maintenant assez peu courant qu'un routeur acquière une des adresses de ses interface comme un client DHCP, cela peut devenir plus commun. Lorsque un routeur acquiert ainsi des adresses, il faut faire attention que l'adresse MAC présentée au serveur DHCP soit en fait univoque.

Les routeurs modernes prennent habituellement en charge des architectures de protocole qui vont au-delà de IP. Certaines de ces architectures, notamment DECnet, Banyan VINES, Xerox Network Services, et IPX, peuvent modifier les adresses MAC des routeurs de telle sorte qu'une certaine adresse MAC apparaisse sur plus d'une interface. Bien que cela ne soit normalement pas un problème, cela peut causer des difficultés lorsque l'adresse MAC est supposée être unique.

D'autres situations surviennent où la même adresse MAC peut apparaître sur plus d'une interface. Il y a des options de forte disponibilité IBM qui établissent des instances principales et de sauvegarde de la même adresse MAC sur différentes interfaces physiques de contrôleurs de communications 37x5.

Certains hôtes d'extrémité qui font fonctionner des piles de protocoles autres que IP, notamment DECnet, peuvent changer leur adresse MAC à partir de l'adresse incorporée à portée mondiale.

6.2 Dynamique

Des mécanismes de protocole dynamique qui dépendent dans une certaine mesure des adresses IP peuvent être affectés par la dénumérotation des routeurs. Cela inclut des mécanismes qui allouent ou résolvent les adresses (par exemple, DHCP, DNS), des mécanismes qui utilisent les adresses IP pour l'identification (par exemple, SNMP), des mécanismes de sécurité et d'authentification, etc. Les mécanismes cités sont aptes à avoir des fichiers de configuration qui seront affectés par un dénumérotage.

Un autre domaine de comportement dynamique qui peut être affecté est la mise en antémémoire. Les serveurs d'application, les fonctions de répertoire telles que le DNS, etc., peuvent mettre des adresses IP en antémémoire. Lorsque le routeur est dénuméroté, ces serveurs peuvent pointer sur les vieilles adresses. Certaines fonctions de serveur mandataire peuvent résider sur des routeurs, et le routeur peut avoir besoin d'être redémarré pour remettre l'antémémoire à niveau.

Les points d'extrémité des tunnels TCP qui se terminent sur des routeurs peuvent être identifiés en interne par des paires adresse/accès à chaque extrémité. Si l'adresse change, même si l'accès reste le même, le tunnel va vraisemblablement devoir être réinitialisé.

7. Outils et méthodes du dénumérotage

La fonction d'un outil de dénumérotage peut être réalisée par une procédure manuelle ou par un logiciel. La présente section traite des fonctions d'outils hypothétiques et donc généraux de dénumérotage plutôt que de leur mise en œuvre.

Avertissement général : les outils devraient savoir si l'environnement accepte l'adressage sans classes. Si il ne le fait pas, les nouvelles adresses devraient être vérifiées pour voir si elles ne comportent pas de valeurs de sous-réseau toutes de zéros ou de uns.

7.1 Mécanismes de recherche

Des outils seront nécessaires pour chercher les fichiers de configuration et autres bases de données pour identifier les noms et adresses qui seront affectés par la réorganisation. Cette recherche devrait se fonder sur l'inventaire des adresses décrit ci-dessus.

En particulier lors d'une recherche de noms, les outils de recherche communs qui utilisent des expressions régulières (par exemple, grep) peuvent être très utiles. Certains outils de recherche supplémentaires peuvent être nécessaires. Certains vont convertir les arguments de recherche en décimal séparé par des point en binaire et ne faire qu'ensuite la comparaison.

La comparaison peut devoir être faite sous la contrainte d'un gabarit. Un tel comparateur devrait aussi être pertinent pour la seconde phase qui cherche une adresse IP et d'autres chaînes pertinentes dans les MIB.

7.2 Modification d'adresse

Le mécanisme général de la modification d'adresse est la substitution d'un nombre arbitraire de bits dans une adresse. Dans les cas les plus simples, il y a une correspondance biunivoque entre les positions binaires ancienne et nouvelle.

En particulier lorsque la modification d'adresse est manuelle, on devrait se souvenir que les bits affectés peuvent être masqués par la notation en décimal séparé par des points. Il faut travaille en notation binaire, ou au moins la prendre en compte, pour assurer la précision.

Plusieurs fonctions de base peuvent être définies :
zerobits(position,longueur): supprimer <longueur> bits commençant à <position>
oubits(position,longueur,nouveauxbits) : OU la chaîne de bits <nouveauxbits> de <longueur> commençant à <position>

Dans ces exemples, l'indice [j] est utilisé pour identifier les entrées dans la base de données de l'inventaire des adresses existantes, tandis que [k] identifie les nouvelles adresses.

Se souvenir que ces outils fonctionnent au niveau du bit, de sorte que les nouvelles adresses devront être reconverties en décimal séparé par des points, MIB ASN.1, ou autre notation avant qu'elles puissent être remplacées dans les fichiers de configuration.

7.2.1 Changement de préfixe sans changement de longueur

Si le nouveau préfixe entier a le même nombre de bits que la vieille partie externe, n'exigeant pas de changement du sous-réseautage, la partie routeur du dénumérotage peut être très simple. Si les configurations du routeur sont disponibles sous une forme lisible en machine, comme des fichiers texte ou des données SNMP analysables, c'est une tâche relativement simple que de définir un outil pour examiner les adresses IP dans la configuration, identifier celles qui commencent par l'ancien préfixe, et y substituer le nouveau préfixe bit par bit.

```
pour chaque adresse[j],
  zerobits(0,PrefixLength[j])
  orbits(0,PrefixLength[j],NewPrefix[j])
```

Noter que la partie hôte n'est pas affectée. Les spécifications de sous-réseau (par exemple, pour les annonces de chemins) et les références spécifiques des hôtes seront toutes deux changées correctement dans ce cas simple.

7.2.2 Changement de highOrderPart

Les choses sont légèrement plus complexes lorsque le changement ne s'applique qu'à la partie contrôlée en externe du préfixe, comme ce peut être le cas lorsque une organisation change de FAI et se renumérote dans l'espace d'adresse du nouveau FAI sans changer la structure interne des sous-réseaux.

Le processus de substitution ressemble beaucoup au cas précédent à l'exception du changement des bits de poids fort :

```
pour chaque adresse,
  zerobits(0,highOrderPartLength[j])
  orbits(0,highOrderPartLength,newHighOrderPart[k])
```

7.2.3 Changement de lowOrderPart

Des organisations peuvent ne dénuméroter que la partie de moindre poids (lowOrderPart) (c'est-à-dire, le champ de sous-réseau) de leur espace d'adresse. Cela peut être fait pour nettoyer un espace d'adresse afin d'avoir des blocs contigus avant d'introduire un système d'acheminement qui agrège les adresses, comme OSPF.

```
pour chaque adresse[j],
  zerobits(highOrderPartLength[j],lowOrderPartLength[j])
  orbits(highOrderPartLength[j], lowOrderPartLength[j],newLowOrderPart[k])
```

7.2.4 Changement de lowOrderPart, Changement de longueur de lowOrderPart

Lorsque change la longueur du champ de sous-réseau dans tout ou partie de l'espace d'adresses, les choses deviennent significativement plus complexes. Un cas très simple survient lorsque le champ d'hôte est substantiellement trop long, au moins dans les sous-réseaux affectés. Ceci est courant, par exemple, lorsque l'espace d'adresses est récupéré dans un réseau existant de classe B avec 8 bits de sous-réseautage. Certains préfixes à /24 bits sont étendus à /30 et réalloués pour des supports point à point réels ou virtuels (par exemple, DLCI).

```
pour chaque adresse [j]
  si l'adresse est affectée par la dénumérotation
  si newLowOrderPartLength[k] > oldLowOrderPartLength[j]
  alors
  zerobits(highOrderPartLength[k],newLowOrderPartLength[k])
  orbits(highOrderPartLength[k],newLowOrderPartPart[k])
  fin
```

7.2.5 Changement de highOrderPart, Changement de longueur de highOrderPart

Lorsque la longueur de la partie de poids fort change, mais qu'on désire garder la structure existante de sous-réseaux, les contraintes s'appliquent. La situation est très simple si la nouvelle partie de poids fort est plus courte que la partie de poids fort existante.

Si la nouvelle partie de poids fort est plus longue que la vieille partie de poids fort, les contraintes sont plus complexes. La clé est de voir si un des <k> bits de moindre poids de l'ancienne partie de poids dort, qui se chevauche avec les <k> bits de moindre poids de la nouvelle partie de poids fort (newHighOrderPart), sont différents de zéro. Si aucun bit n'est différent de zéro, il peut être plus simple de recouvrir les bits du nouveau préfixe.

7.3 Désignation

Il vaut la peine de remarquer que l'utilisation par un routeur d'un nom du DNS ne signifie pas nécessairement que ce nom est défini dans un serveur de noms. Les routeurs contiennent souvent des adresses statiques pour désigner des transpositions locales au routeur, de sorte que les fichiers de zone du DNS et les fichiers de configuration du routeur peuvent tous deux devoir être vérifiés.

Ce qu'on veut faire d'abord est générer une liste de transpositions de nom en adresse, le mécanisme de transposition de chaque instance (par exemple, d'entrée statique dans un fichier de configuration, de RR dans le DNS de notre zone, de RR dans un fichier de zone en dehors de la notre) la déclaration de définition (ou son équivalent si les routeurs sont configurés avec SNMP) et l'adresse IP actuelle. On va ensuite vouloir comparer les adresses dans cette liste à celle définie précédemment pour les préfixes affectés par la dénumérotations. L'intersection de ces listes définit quand on doit faire des changements.

Noter que la déclaration explicite de définition, ou au moins ses variables, devrait être conservée. Dans le monde réel, les transpositions d'adresses IP statiques en hôtes peuvent n'avoir pas été conservées aussi systématiquement que le sont les enregistrements de ressource (RR) dans un serveur du DNS. Il est entièrement possible que différentes entrées de transposition d'hôte pour le même nom pointent sur des adresses différentes.

7.3.1 Outils du DNS

Le DNS lui-même peut aussi bien retarder qu'accélérer le dénumérotage de routeur. Les antémémoires dans les serveurs du DNS à la fois à l'intérieur et à l'extérieur de l'organisation peuvent avoir une persistance suffisante pour qu'une conversion au "jour J" ne soit pas praticable si on veut conserver la connexité mondiale. Le DNS peut cependant aider à faire fonctionner une période de coexistence de l'ancienne et de la nouvelle adresse.

Si, par exemple, une certaine interface de routeur peut avoir une coexistence de la nouvelle et de l'ancienne adresse, il peut être approprié d'introduire la nouvelle adresse comme un alias de CNAME pour la nouvelle adresse.

Les déclarations de RR du DNS peuvent se terminer par un point-virgule, indiquant que le reste de la ligne est un commentaire. Cela peut être utilisé comme outil de base pour dénuméroter les noms du DNS pour les adresses de routeur, en mettant un commentaire (par exemple, ";nouvelle adresse") à la fin des déclarations de CNAME pour les nouvelles adresses. Au moment approprié, un script pourrait générer un nouveau fichier de zone dans lequel les nouvelles adresses deviendront les définitions principales sur les enregistrements A, et les vieilles adresses pourraient devenir des enregistrements CNAME munis d'un commentaire approprié. Ultérieurement, ces entrées de CNAME commentées pourront être supprimées.

Il faut prendre soin de s'assurer que les entrées de transposition inverse de pointeur sont définies pour les nouvelles adresses, parce que les outils de certains fabricants de routeurs dépendent de la transposition inverse.

7.3.2 Outils en rapport avec la désignation

En particulier sur de l'UNIX et d'autres qui font de l'acheminement, il peut y avoir des définitions statiques de noms. De telles définitions sont probablement plus difficiles à conserver que des entrées dans le DNS, simplement parce qu'elles sont plus largement distribuées.

Plusieurs outils sont disponibles pour générer des entrées plus gérables. Un script perl appelé h2n convertit les tableaux d'hôtes en fichiers de données de zone qui peuvent être ajoutés sur le serveur DNS. Il est disponible à ftp://ftp.uu.net/published/oreilly/nutshell/dnsbind/dns.tar.Z. Un autre outil, makezones, fait partie de la distribution BIND actuelle, et peut aussi être obtenu à ftp://ftp.cus.cam.ac.uk/pub/software/programs/DNS/makezones.

Voir le répertoire des ressources du DNS à http://www.dns.net/dnsrd.

8. Identifiants de routeurs

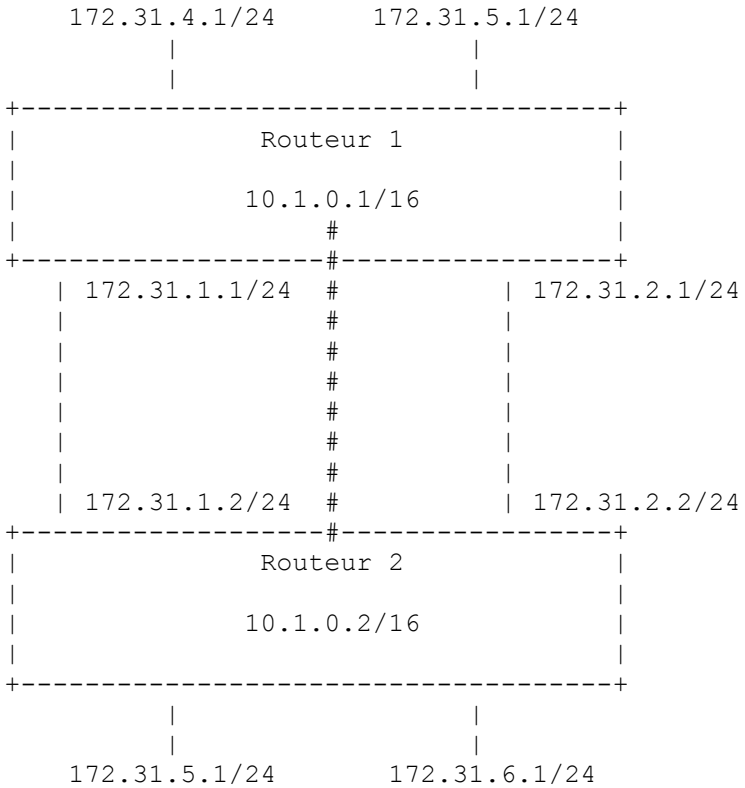
Les commandes de configuration dans cette catégorie allouent des adresses IP aux interfaces physiques ou virtuelles sur un seul routeur. Elles incluent aussi des commandes qui allouent des informations en rapport avec les adresses IP à la "boîte" de routeur elle-même, et des commandes qui impliquent les interactions du routeur avec ses voisins en dessous du niveau de l'acheminement (par exemple, des passerelles par défaut, ARP).

Les routeurs peuvent avoir d'autres identifiants univoques, comme les noms du DNS utilisés pour l'ensemble des adresses sur la "boîte," ou des chaînes SNMP systemID.

8.1 Identification mondiale de routeur

Les routeurs IP traditionnels n'ont pas d'identifiant univoque, mais sont plutôt traités comme des collections d'adresses IP associées à leurs interfaces. Certains mécanismes de protocole, notamment OSPF et BGP, ont besoin d'une adresse pour le routeur lui-même, normalement pour établir les points d'extrémité du tunnel entre les routeurs homologues. D'autres applications incluent des "interfaces non numérotées" utilisées pour conserver l'espace d'adresse pour des supports de série, pratique exposée plus loin.

Dans l'illustration ci-dessous, l'espace d'adresse 10.1.0.0/16 est utilisé pour des identifiants mondiaux. Un tunnel TCP court de 10.1.0.1 à 10.1.0.2, mais son trafic est à partage de charge sur les deux liaisons réelles, 172.31.1.0 et 172.31.2.0.



Une pratique courante pour fournir des identifiants de routeurs est d'utiliser la "plus forte adresse IP" sur le routeur comme

identifiant de la "boîte". De nombreuses mises en œuvre on un mécanisme par défaut pour établir l'identifiant de routeur, qui peut être la plus forte adresse configurée, ou la plus forte adresse active.

Les applications typiques d'un identifiant mondial de routeur peuvent ne pas exiger qu'il soit une adresse IP "réelle" qui est annoncée sur tout le domaine d'acheminement, mais que ce soit simplement un identifiant local de 32 bits pour chaque routeur. Lorsque c'est le cas, cet identifiant peut venir de l'espace d'adresses privé de la [RFC1918] plutôt que de l'espace d'adresses enregistré de l'entreprise.

Permettre la sélection par défaut de l'identifiant de routeur peut être instable et n'est pas recommandé. La plupart des mises en œuvre ont un moyen pour déclarer une adresse pseudo-IP pour le routeur lui-même par opposition à l'un de ses accès.

Les changements à cette pseudo-adresse peuvent avoir des implications pour le DNS. Même si ce n'est pas une adresse réelle, des enregistrements de ressources A et PTR peuvent avoir été établis pour elle, de sorte que des diagnostics peuvent afficher des noms plutôt que des adresses.

Une autre implication potentielle pour le DNS est qu'un CNAME peut avoir été établi pour l'ensemble entier des adresses d'interface sur un routeur. Cela permet des essais, telnet, etc., sur le routeur via tout chemin accessible.

8.2 Adresse d'interface

Les adresses d'interface sont peut-être l'endroit de base par où commencer un dénumérotage de routeur. La configuration de l'interface exigera une adresse IP, et normalement un gabarit de sous-réseau ou une longueur de préfixe. Certaines mises en œuvre peuvent n'avoir pas de gabarit de sous-réseau dans la configuration existante, parce qu'elles utilisent un "gabarit par défaut" fondé sur une hypothèse de classes sur l'adresse. Il faut être conscient de la possibilité qu'il soit besoin d'une spécification explicite d'un gabarit de sous-réseau ou d'une autre spécification de longueur de préfixe lorsque qu'aucune n'a été spécifiée antérieurement. Cela sera particulièrement courant sur les plus anciens routeurs fondés sur un hôte.

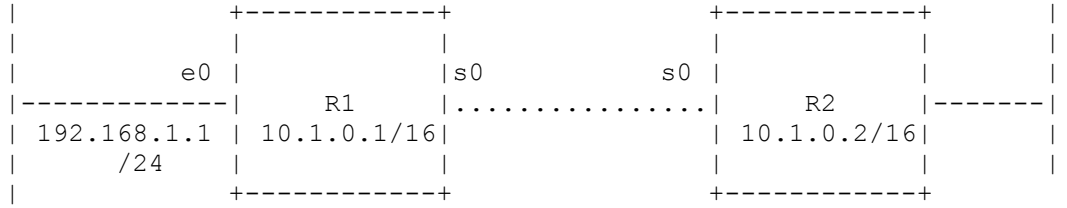
Plusieurs adresses IP, dans différents sous-réseaux, peuvent être allouées à la même interface. C'est souvent une technique valable dans un dénumérotage, parce que l'interface de routeur peut être configurée pour répondre aux deux adresses, l'ancienne et la nouvelle.

Il faut cependant faire attention lorsqu'on utilise plusieurs adresses de sous-réseau sur la même interface. Les mises en œuvre de OSPF et de IS-IS peuvent ne pas annoncer les adresses supplémentaires, ou peuvent contraindre leurs annonces à être toutes dans la même zone.

Lorsque cette méthode est utilisée pour faire répondre l'interface à l'ancienne et à la nouvelle adresse, et que le processus de dénumérotage est achevé, il faut faire attention lorsqu'on retire l'ancienne adresse. Certaines mises en œuvre de routeur ont une compréhension particulière de l'ordre des déclarations d'adresses sur une interface. Il est très vraisemblable que des routeurs, ou au moins l'interface, doivent être redémarrés après la suppression d'une adresse.

8.3 Interfaces non numérotées

Comme mentionné précédemment, plusieurs conventions ont été utilisées pour éviter de gâcher de l'espace de sous-réseau sur des lignes en série. Un mécanisme est de mettre en œuvre des schémas propriétaires de "demi-routeur", dans lesquels la liaison non numérotée entre les paires de routeurs est traitée comme un "bus interne" créant un "routeur virtuel" tel que la portée de l'interface non numérotée soit limitée à la paire de routeurs.



Dans l'exemple ci-dessus, le logiciel dans les routeurs R1 et R2 transmet automatiquement chaque paquet reçu sur l'interface de série s0 à l'interface Ethernet e0. Ils transmettent chaque paquet sur e0 dans leur s0 local. Aucun s0 n'a d'adresse IP. R1 a l'identifiant de routeur 10.1.0.1/16 et R2 a 10.1.0.2/16.

Il est donc impossible d'envoyer un ping spécifique aux interfaces S0, ce qui rend difficile de vérifier si un problème de connectivité est d$u à S0 ou à E0. Une certaine gestion est possible pour autant qu'au moins une adresse IP soit accessible sur le routeur (par exemple, e0) car cela permettra la connexion de SNMP avec le routeur. Une fois que le routeur est accessible via SNMP, l'interface non numérotée peut être interrogée à travers la ifTable de la MIB.

Une autre approche est d'utiliser l'identifiant mondial de routeur comme une pseudo-adresse pour chaque interface non

numérotée sur un routeur. Dans l'exemple ci-dessus, R1 utiliserait 10.1.0.1 comme identifiant. Cela procure une adresse à utiliser pour des fonctions telles que l'option d'enregistrement de chemin IP, et pour fournir une adresse de prochain bond pour les routes.

La seconde approche est plus propre, mais peut encore créer des difficultés de fonctionnement. Si il y a plusieurs interfaces non numérotées sur un routeur, laquelle (s'il en est) devrait répondre à un ping ? Les autres mécanismes de gestion de réseau ne fonctionnent pas bien avec les interfaces non numérotées.

Au titre d'un effort de dénumérotage, on devrait se pencher sur le besoin d'interfaces non numérotées. Si le processus de dénumérotage fait passer le domaine à l'adressage sans classes, on peut alors donner aux liaisons en série des adresses avec un préfixe /30, ce qui va minimiser la consommation d'espace d'adresses.

Pour des liaisons spécialisées en point à point ou virtuelles au sein d'une organisation, une autre solution de remplacement au fonctionnement sans numéro est d'utiliser l'espace d'adresses privé de la [RFC1918]. Les liaisons inter-routeur ont rarement besoin d'un accès à partir de l'Internet sauf utilisation explicite pour l'acheminement extérieur. Les traceroutes externes vont aussi échouer à faire une recherche de DNS inverse.

Si on conserve des interfaces non numérotées, et si la convention d'identifiant de routeur est utilisée, il sera probablement plus stable de s'appuyer sur un identifiant de routeur explicitement configuré que sur un identifiant par défaut à partir d'une adresse d'interface non numérotée.

La situation devient encore plus bizarre si on souhaite utiliser des interfaces non numérotées sur des services NBMA tels que le relais de trame. OSPF, par exemple, utilise l'adresse IP d'interfaces numérotées comme identifiant univoque pour cette interface. Comme les interfaces non numérotées n'ont pas leur propre adresse univoque, OSPF n'a pas de façon évidente d'identifier ces interfaces. Un indice physique (par exemple, ifTable) pourrait être utilisé, mais devrait être étendu pour avoir une entrée pour chaque entrée logique (c'est-à-dire, chaque VC) multiplexée sur l'interface physique.

8.4 Résolution d'adresse

Lors de la transposition d'adresses IP en adresses MAC de LAN, qui est habituellement faite automatiquement par le logiciel de routeur, il va y avoir des cas où une transposition particulière sera peut-être nécessaire. Par exemple, l'adresse MAC qui est utilisée par les interfaces de routeur peut être administrée en local (c'est-à-dire, réglée à la main) plutôt que sur l'adresse incorporées dans le matériel. Elle peut faire partie d'une méthode non normalisée qui alloue de façon dynamique les adresses MAC aux interfaces. Dans de tels cas, une adresse IP peut faire partie des déclarations de configuration d'adresse MAC et devra être changée.

La transposition manuelle en adresses du support va habituellement être nécessaire pour les supports en NBMA et commutés. Lors d'un dénumérotage d'adresses IP, les déclarations qui transposent les adresses IP en DLCI de relais de trame, en adresses X.121, en adresses SMDS et ATM, en numéros de téléphone, etc., devront être changées en la nouvelle adresse. Les exigences locales peuvent requérir une période de fonctionnement en parallèle, où la vieille et la nouvelle adresse IP se transposent en la même adresse de support.

8.5 Traitement de la diffusion

La [RFC1812] spécifie que les interfaces de routeurs NE DOIVENT PAS transmettre des diffusions limitées (c'est-à-dire, à l'adresse de destination toute de uns, 255.255.255.255). Il est cependant courant d'avoir des circonstances où un segment de LAN n'est rempli que par des clients qui communiquent avec des serveurs clés (par exemple, DNS ou DHCP) en envoyant des diffusions limitées. Les interfaces de routeur peuvent s'accommoder de cette situation en traduisant l'adresse de diffusion limitée en adresse de diffusion dirigée ou en une adresse d'hôte spécifique, qu'il est légitime de transmettre.

Lorsqu'une traduction d'adresse limitée est faite pour des segments sans serveur, et que la nouvelle adresse cible est dénumérotée, la règle de traduction doit être reconfigurée sur chaque interface avec un segment sans serveur. Il faut être sûr de reconnaître qu'un certain segment peut avoir un serveur du point de vue d'un service (par exemple, DHCP), mais pourrait être sans serveur pour d'autres services (par exemple, NFS ou DNS).

8.6 Prise en charge de l'adressage dynamique

Les routeurs peuvent participer à l'adressage dynamique avec RARP, DHCP, BOOTP, ou PPP. Dans un effort de dénumérotage, plusieurs sortes de changements peuvent être faits sur les routeurs qui participent à l'adressage dynamique.

Si le routeur agit comme serveur pour l'allocation dynamique d'adresses, les adresses qu'il alloue devront être dénumérotées. Ce peut être les adresses spécifiques associées aux adresses MAC ou les accès de numérotation, ou ce peut être un réservoir d'adresses. On peut voir des réservoirs d'adresses dans de purs environnements IP, ou dans des situations multi protocoles telles que le MacIP de Apple.

Si le routeur n'alloue pas d'adresses, il peut être chargé de transmettre les demandes d'allocation d'adresses au ou aux serveurs appropriés. Si c'est le cas, il peut y avoir des références incorporées aux adresses IP de ces serveurs, qui pourraient devoir être changées au titre du dénumérotage.

9. Filtrage et contrôle d'accès

Les routeurs peuvent mettre en œuvre des mécanismes pour filtrer les paquets sur la base de critères autres que la destination du prochain bond. De tels mécanismes sont souvent mise en œuvre de façon différente pour les paquets en envoi individuel (le cas le plus courant) et pour les paquets en diffusion groupée (y compris les mises à jour d'acheminement). Les règles de filtrage peuvent contenir des adresses IP de source et/ou de destination qui vont devoir être changées au titre de la dénumérotation.

Le filtrage peut être fait pour mettre en œuvre des politiques de sécurité ou pour le contrôle du trafic. Dans l'un et l'autre cas, une extrême prudence doit être gardée si on change les règles, pour éviter les fuites d'informations sensibles, le déni d'accès aux utilisateurs légitimes, ou l'encombrement du réseau.

Les routeurs peuvent mettre en œuvre l'enregistrement des événements de filtrage, normalement le déni d'accès. Si l'enregistrement est mis en œuvre, les serveurs d'enregistrement auxquels les événements enregistrés sont envoyés de préférence devraient être identifiés par le nom du DNS. Si le serveur d'enregistrement est référencé par une adresse IP, son adresse peut devoir être changée durant le dénumérotage. Il faut veiller à ce que des données critiques d'analyse ne soient pas perdues durant le changement d'adresse.

9.1 Mécanismes de contrôle d'accès statique

Les filtres de routeur contiennent normalement un certain nombre de règles d'inclusion/exclusion qui définissent quoi inclure/exclure dans une transmission. Ces règles contiennent normalement un argument d'adresse et des indications sur la longueur du préfixe. Cette indication de longueur pourrait être un compte, un gabarit de sous-réseau, ou quelque autre gabarit.

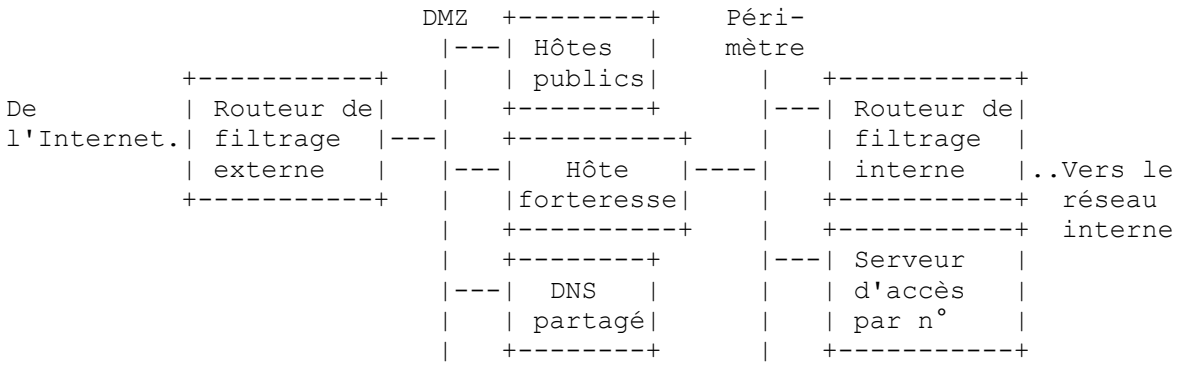
Lors d'un dénumérotage, l'argument d'adresse doit évidemment changer. Cela peut être plus subtil si la longueur du préfixe change, parce que la spécification de longueur dans la règle doit changer elle aussi. La nécessité d'un tel changement peut être difficile à identifier parce qu'elle s'applique à des gammes d'adresses qui peuvent être à un niveau d'agrégation plus élevé que l'opération explicite de dénumérotage.

La [RFC1812] exige que le filtrage fondé sur l'adresse permette des longueurs de préfixe arbitraires, mais certains hôtes et routeurs pourraient ne permettre que des préfixes de classes.

9.2 Considérations particulières sur les pare-feu

Les routeurs sont des composants critiques des systèmes de pare-feu. Du point de vue de l'architecture, deux fonctions de routeur sont décrites dans les modèles de pare-feu, le routeur de filtrage externe entre l'extérieur et la "zone démilitarisée (DMZ)" et le routeur de filtrage interne entre l'intérieur et le "périmètre de réseau". Entre ces deux réseaux se trouve l'hôte forteresse, dans lequel résident diverses fonctions d'isolation non liées à l'acheminement et l'authentification, qui sortent du domaine d'application du présent document.

Un aspect pertinent de l'hôte forteresse est cependant qu'il peut faire de la traduction d'adresse ou des transpositions de couche supérieure entre différents espaces d'adresses. Si l'espace d'adresses "extérieur" (c'est-à-dire, visible de l'Internet) change, cela va signifier que le routeur de filtrage externe aura besoin de changements de configuration. Comme le routeur de filtrage externe peut être sous le contrôle du FAI plutôt que sous celui de l'entreprise, une coordination administrative sera nécessaire.



Le routeur de filtrage externe a normalement des listes d'accès entrants qui bloquent le trafic non autorisé provenant de l'Internet, et des listes d'accès sortant qui permettent seulement l'accès aux serveurs de la DMZ et à l'hôte forteresse. Les filtres entrants bloquent normalement l'espace d'adresses privé, ainsi que l'espace d'adresses du réseau interne de l'entreprise. Si l'adresse réseau interne change, les filtres entrants doivent évidemment être changés.

Si les adresses d'hôte de la DMZ changent, les filtres sortants correspondants de l'hôte de filtrage externe devront aussi changer. Les routeurs de filtrage interne permettent l'accès en provenance du réseau interne aux serveurs sélectionnés sur le périmètre de réseau, ainsi qu'à l'hôte forteresse lui-même. Si l'entreprise utilise en interne un espace d'adresses privé, le dénumérotage peut ne pas affecter ce routeur.

Un autre composant d'un système de pare-feu est le serveur "DNS partagé", qui fait la transposition des adresses en relation avec les parties visibles de l'Internet mondial.

9.3 Mécanismes de contrôle d'accès dynamique

Certains services de contrôle d'accès, tels que RADIUS et TACACS+, peuvent insérer des règles d'accès allouées de façon dynamique dans les configurations de routeurs. Par exemple, une base de données RADIUS "contient une liste d'exigences qui doivent être satisfaites pour permettre l'accès à l'usager. Cela comporte toujours la vérification du mot de passe, mais peut aussi spécifier le ou les clients ou le ou les accès auxquels il est permis à l'usager d'accéder." [RFC2058].

Les informations de configuration communiquées de façon dynamique au routeur peuvent être sous la forme de règles de filtrage. Effectivement, cette base de données d'authentification devient une extension de la base de données de configuration du routeur. Ces deux bases de données peuvent devoir être modifiées au titre de l'effort de dénumérotation.

Un autre problème de configuration dynamique survient lorsque on utilise "l'examen des paquets à état plein" sur les hôtes forteresse ou les routeurs pour apporter la sécurité pour les services fondés sur UDP, ou simplement pour IP. Dans de tels services, lorsque un paquet autorisé quitte l'environnement local pour aller dans un espace d'adresse qui n'est pas de confiance, une règle temporaire de filtrage est établie sur l'interface sur laquelle est attendue la réponse à ce paquet. La règle a normalement la durée de vie d'une seule réponse de paquet. Si ces règles sont définies dans une base de données en dehors du routeur, la base de données de règles est là encore une extension de la configuration de routeur qui doit faire partie de l'effort de dénumérotage.

10. Acheminement intérieur

La présente section traite de l'acheminement à l'intérieur d'une entreprise, qui suit généralement les règles ci-après, en ignorant les chemins par défaut :

1. Si il existe un seul chemin potentiel pour une destination, le suivre.
2. Si il y a plus d'un chemin potentiel pour une destination, utiliser celui qui a la plus faible métrique de bout en bout.
3. Si il y a plusieurs chemin d'égal plus faible coût pour la destination, envisager l'équilibrage de charge.

La plupart des entreprises ne participent pas directement aux mécanismes d'acheminement de l'Internet mondial, dont les détails sont laissés aux soins de leurs fournisseurs de services. La section suivante traite de ces plus complexes mécanismes extérieurs.

10.1 Chemins statiques

Durant un dénumérotage, l'adresse de destination et/ou de prochain bond des chemins statiques peut devoir changer. Il peut être nécessaire de redémarrer les routeurs ou de supprimer explicitement une entrée de tableau d'acheminement pour forcer la prise d'effet d'un changement de chemin statique.

10.2 RIP (Version 1 sauf mention contraire)

Le protocole d'informations d'acheminement (RIP, *Routing Information Protocol*) a longtemps été pour nous un des premiers protocoles d'acheminement intérieur. Il fait encore ce travail dans de petits réseaux, et a aussi été utilisé pour des fonctions associées qui ne font pas strictement partie de l'acheminement intérieur. Dans cet exposé, nous allons d'abord traiter des pures applications d'acheminement intérieur.

Dans un effort de dénumérotation qui implique de l'adressage sans classes, RIPv1 peut n'être pas capable de traiter le nouveau schéma d'adressage. Officiellement, ce protocole est historique et devrait être évité dans les nouveaux plans d'acheminement. Lorsque des exigences de supports traditionnels imposent qu'il soit retenu, il est préférable d'essayer de limiter RIPv1 aux parties de "bout" du réseau. Des mécanismes spécifiques de fabricants peuvent être disponibles pour interfacer RIPv1 dans un environnement sans classes.

Au titre de la planification d'une dénumérotation, on devrait réellement considérer l'intérêt de passer à RIPv2, OSPF, ou autres protocoles d'acheminement sans classes comme principaux moyens d'acheminement intérieur. Le faire ne va cependant pas supprimer le besoin de faire fonctionner RIP dans certaines parties de l'entreprise.

RIP est largement mis en œuvre sur les hôtes, où il peut être utilisé comme une méthode de découverte de routeur, ou pour l'équilibrage de charge et la tolérance aux fautes lorsque plusieurs routeurs sont sur un sous-réseau. Dans ces applications, RIP n'a pas besoin d'être le seul protocole d'acheminement dans le domaine ; RIP peut n'être présent que sur les sous-réseaux de bout. Les informations de destinations provenant de protocoles d'acheminement disposant de capacités plus importantes peuvent être traduites dans des mise à jour RIP. Bien qu'il soit généralement raisonnable de minimiser ou supprimer RIP au titre d'un effort de dénumérotage, il faut faire attention à ne pas supprimer aux hôtes la capacité à localiser les routeurs.

RIP est aussi utilisé comme un mécanisme d'acheminement quasi extérieur entre certains abonnés et leur FAI, comme un moyen plus simple que BGP pour que l'abonné annonce les chemins au fournisseur.

10.3 OSPF

OSPF a plusieurs sensibilités au dénumérotage qui vont au delà de celles de protocoles d'acheminement plus simples. Si les identifiants de routeur sont alloués de façon à faire partie de l'espace d'adresses enregistré, il est possible qu'on doive les changer au titre de l'effort de dénumérotage. Il peut être approprié d'utiliser l'espace d'adresses privé de la [RFC1918] pour les identifiants de routeurs, pour autant que ceux-ci puissent faire l'objet d'une recherche dans un serveur DNS au sein du domaine.

Les règles de résumé seront vraisemblablement affectées par le dénumérotage, en particulier si les frontières de zone changent.

Des techniques d'adressage particulières, telles que des interfaces non numérotées et des interfaces physiques avec des adresses IP dans plusieurs sous-réseaux, peuvent n'être pas transparentes à OSPF. Leur utilisation doit se faire avec prudence, et devrait être strictement limitée à l'intra zone.

Si le dénumérotage est partiellement motivé par l'introduction de services NBMA, cela peut avoir de nombreux impacts sur OSPF. Généralement, la meilleure façon de minimiser cet impact est d'utiliser des sous-réseaux séparés pour chaque VC. En faisant ainsi, des coûts OSPF différents peuvent être affectés aux différents VC, la configuration d'un routeur désigné n'est pas nécessaire, etc.

10.4 IS-IS

Les préfixes IP sont généralement associés à des définitions de zone IS-IS *(système intermédiaire à système intermédiaire)*. Si les préfixes IP changent, il peut y avoir un changement correspondant dans les définitions de zone.

10.5 IGRP et IGRP amélioré

Lorsque un passage de IGRP à IGRP amélioré *(EIGRP)* fait partie d'un effort de dénumérotage, il faut prendre en considération le besoin de désactiver le résumé automatique de chemin de IGRP. Ceci est probable si l'adressage sans classes est mis en œuvre.

Il faut aussi être conscient des nuances de la redistribution automatique entre IGRP et EIGRP. Le "numéro de système autonome" qui n'a pas besoin d'être un vrai numéro d'AS mais simplement d'identifier un ensemble de routeurs coopérants, doit être le même sur les processus d'IGRP et d'EIGRP pour que la redistribution automatique survienne.

11. Acheminement extérieur

Les chemins extérieurs peuvent être définis de façon statique. Si l'acheminement dynamique est impliqué, de tels chemins sont appris principalement de BGP. L'utilisation de RIP n'est pas rare pour permettre aux FAI d'apprendre de façon dynamique les chemins des nouveaux abonnés, bien qu'il y ait des soucis de sécurité dans une telle approche. IGRP et EIGRP peuvent être utilisés pour annoncer les chemins externes.

Un dénumérotage qui affecte les routeurs qui parlent BGP peut être complexe, parce qu'il peut exiger des changements non seulement dans les routeurs BGP du système autonome local, mais exiger aussi des changements dans les routeurs d'autres AS et chez les registraires dans l'acheminement. Cela va exiger une coordination administrative attentive.

Pour les seules raisons de la documentation, on considèrera la possibilité d'utiliser la notation de politique d'acheminement de [RIPE-181++] [RFC2280] pour décrire les politiques d'acheminement extérieur.

11.1 Registres/bases de données d'acheminement

Les organisations qui participent à l'acheminement extérieur auront normalement des informations d'acheminement non seulement dans leurs routeurs, mais aussi dans des bases de données qui fonctionnent sous le contrôle des registraires ou de fournisseurs de service de niveau supérieur (par exemple, l'arbitre de l'acheminement).

Si un FAI dont le précédent espace d'adresses venait d'un fournisseur différent subit un dénumérotage dans l'espace d'adresses d'un fournisseur différent, ou obtient pour lui-même un bloc reconnu, il peut y avoir des exigences administratives que les adresses précédemment allouées soient restituées. Cela inclut des changements dans la délégation IN-ADDR.ARPA, dans les bases de données SWIP, etc., et doit être coordonné avec les registraires et fournisseurs spécifiques impliqués. Tous les registraires et fournisseurs n'ont pas la même politique.

Si l'entreprise est un système autonome enregistré et qu'elle se dénumérote dans un espace d'adresses différent, les objets de chemins avec les anciens préfixes dans les registres d'acheminement devront être supprimés et les objets de chemin avec les nouveaux préfixes devront être ajoutés.

11.2 BGP – Organisation propre

Les informations d'adressage IP peuvent être incorporées dans plusieurs aspects d'un locuteur BGP. Cela inclut :

1. L'identifiant de routeur.
2. Les adresses IP du routeur homologue.
3. Les listes de préfixes annoncés.
4. Les règles de filtrage des chemins.

Certains outils existent (RtConfig) pour générer la partie configuration de politique des déclarations de configuration de routeur BGP à partir des politiques spécifiées dans RIPE-181 ou RPSL.

11.3 BGP -- autre AS

D'autres systèmes autonomes, y compris non adjacents, peuvent contenir des références directes ou indirectes (par exemple, agrégées) aux informations d'acheminement mentionnées ci-dessus. Des outils existent pour faire une vérification préliminaire de la connexité avec certaines destinations externes (RADB).

12. Gestion de réseau

Cette section est destinée à traiter des parties de la gestion de réseau qui sont intimement associées aux routeurs, plutôt qu'un exposé général sur la dénumérotation et la gestion de réseau.

Les méthodes utilisées pour gérer les routeurs incluent les telnets à des accès de console virtuelle, SNMP, et TFTP. Les scripts de gestion de réseau peuvent contenir des références incorporées aux adresses IP qui prennent en charge ces services. En général, il faut essayer de convertir les références de script à des adresses IP en noms du DNS.

Un problème critique et complexe sera de convertir les bases de données SNMP, qui sont normalement organisées par adresse IP.

12.1 Gestion de configuration

Les noms et adresses des serveurs qui participent à la gestion de configuration peuvent devoir être changés, ainsi que le contenu des configurations qu'ils fournissent. Les serveurs TFTP sont couramment utilisés pour cela, comme peuvent l'être les gestionnaires SNMP.

12.2 Services de résolution/répertoire de nom

Durant un dénumérotage, il va probablement être utile d'allouer des noms du DNS aux interfaces, aux interfaces virtuelles, et des identifiants de routeur aux routeurs. On se souvient qu'il est parfaitement acceptable d'identifier les interfaces internes avec les adresses privées des [RFC1597] [RFC1918], tant que les pare-feu et autres filtres empêchent ces adresses d'être propagées en-dehors de l'entreprise.

Si on utilise l'adressage dynamique, on devrait envisager le DNS dynamique. Comme c'est encore en développement, il peut être approprié d'envisager des moyens non normalisés pour apprendre quelles adresses ont été allouées de façon dynamique, de façon à pouvoir faire un ping ou autre moyen de gestion.

Se souvenir aussi que de la résolution de noms peut être faite par des tableaux statiques qui font partie des configurations de routeur. Changer les entrées du DNS, et même redémarrer les routeurs, ne va pas les changer.

12.3 Gestion des fautes

Les indications de conditions anormales peuvent être envoyées à plusieurs endroits qui peuvent être des adresses IP incorporées, tels que les serveurs pièges SNMP, les serveurs syslogd, etc.

On devrait se souvenir que de grosses salves d'erreurs transitoires peuvent être causées au titre de la conversion d'adresses dans le dénumérotage. Il faut avoir conscience que ces salves peuvent submerger la capacité des fichiers d'enregistrement, et éventuellement causer la perte des informations d'audit. On peut envisager d'augmenter la capacité des fichiers ou de trouver d'autres moyens de les protéger durant la conversion.

12.4 Gestion des performances

Les informations sur les performances peuvent être enregistrées dans les routeurs eux-mêmes, et restituées par des scripts de gestion de réseau. D'autres informations de performances peuvent être envoyée à syslogd, ou conservées dans les bases de données SNMP.

Les scripts générateurs de charge utilisés pour les essais de performances peuvent contenir des adresses IP incorporées. Examiner attentivement les scripts qui contiennent du code exécutable pour générer des gammes d'adresses d'essai. De tels scripts peuvent, à première vue, paraître ne contenir aucune adresse IP explicite. Ils peuvent, par exemple, contenir un "germe" d'adresse utilisé avec une boucle d'incrémentation.

12.5 Gestion de comptabilité

Les enregistrements de comptabilité peuvent être envoyés périodiquement à syslogd ou comme des pièges SNMP. Autrement, le gestionnaire SNMP ou d'autres applications de gestion peuvent périodiquement interroger les informations de comptabilité dans les routeurs, et donc contenir des adresses IP incorporées.

12.6 Gestion de la sécurité

La gestion de la sécurité inclut l'enregistrement des journaux d'événement *(logging)*, l'authentification, le filtrage, et le contrôle d'accès. Les routeurs peuvent avoir des références incorporées aux serveurs pour toutes ces fonctions.

De plus, les routeurs vont couramment contenir des filtres qui contiennent des règles qui se rapportent à la sécurité. Ces règles sont vouées à un recodage explicite car elles tendent à fonctionner au niveau binaire.

Certains serveurs d'authentification et mécanismes de filtrage peuvent mettre à jour de façon dynamique les filtres de routeurs.

12.7 Service de l'heure

Les références incorporées aux serveurs NTP devraient être changées en noms DNS lorsque possible, et dénumérotées autrement.

13. IP et encapsulation de protocole

Les paquets IP peuvent être acheminés pour fournir la connexité pour des protocoles non IP, ou pour du trafic IP avec des adresses non cohérentes avec l'environnement d'acheminement actif. De telles fonctions d'encapsulation ont normalement un modèle de tunnelage, où une connexion de bout en bout entre deux adresses de protocole "passager" est transposée en une paire d'adresses IP de points d'extrémité. L'encapsulation de chemin générique *(GRE, Generic Route Encapsulation)* est un moyen représentatif de ce genre de tunnelage [RFC1701], [RFC1702].

13.1 À présent

La dénumérotation de l'environnement IP principal ne signifie pas souvent que les adresses du protocole passager doivent changer. En fait, une telle encapsulation de protocole pour le trafic IP peut être une méthode très viable pour le traitement

de systèmes traditionnels qui ne peuvent pas être facilement dénumérotés. Pour ce cas des réseaux traditionnels, les adresses IP traditionnelles peuvent être tunnelées sur l'environnement d'acheminement renuméroté.

Noter aussi que IP peut être un protocole passager sur des systèmes non IP qui utilisent IPX, AppleTalk, etc.

13.2 À l'avenir

Les mécanismes de tunnelage sont fondamentaux pour la transition prévue de IPv4 à IPv6. Au titre de l'effort de dénumérotage de IPv4, il peut valoir la peine de réserver une partie de l'espace d'adresses pour les futurs tunnels IPv6.

Bien qu'il y ait un besoin clair et immédiat de dénumérotation IPv4, il peut y avoir des cas où la dénumérotation IPv4 peut être différée de quelques mois ou années. Si l'effort est différé, il peut être prudent à ce moment de considérer si les mises en œuvre IPv6 disponibles ou les mécanismes de tunnelage forment des solutions de remplacement viables à la dénumérotation IPv4. Il peut être approprié de dénuméroter certaines parties de l'espace IPv4 existant directement dans l'espace IPv6. Les outils pour cet objet sont en cours d'expérimentation au moment de la rédaction du présent document.

14. Considérations pour la sécurité

Les routeurs sont des parties critique des pare-feu, et sont par ailleurs utilisés pour la mise en application de la sécurité. Les erreurs de configuration commises durant le dénumérotage peuvent exposer les systèmes à des intrusions malveillantes, ou refuser le service à des utilisateurs autorisés. Le souci le plus critique est que les filtres soient configurés de façon appropriée pour les anciennes et les nouvelles adresses, mais d'autres numéros peuvent aussi impacter la sécurité, comme les pointeurs sur les serveurs d'authentification, de journaux d'événement, et du DNS.

Durant une opération de dénumérotage, il peut être approprié d'introduire des mécanismes d'authentification pour les mises à jour d'acheminement.

15. Programmation et mise en œuvre d'un dénumérotage

Une grande partie de l'effort de dénumérotage sera fait sur des plateformes autres que les routeurs. Néanmoins, les routeurs sont une partie clé de tout effort de dénumérotage.

Étape 1 – Inventaire de adresses et noms affectés.

Étape 2 – Désigner tous les changements topologiques nécessaires. Si un espace d'adresses temporaire, des traducteurs d'adresse réseau, etc., sont nécessaires, les obtenir.

Étape 3 –Installer et tester les changements pour rendre le réseau plus accessible à la dénumérotation. Cela inclut de faire un usage maximal des chemins par défaut et des résumés, tout en minimisant les références aux serveurs fondées sur les adresses.

Étape 4 – Planifier le dénumérotage réel. Doit il être graduel ou total ? Peut il être fait par une série de dénumérotages de réseaux de bout, éventuellement avec des adresses secondaires sur les routeurs centraux ? La NAT est-elle appropriée ? Si oui, comment doit-elle être utilisée ?
Quel est le plan de repli si des problèmes majeurs surviennent ? Faire une distinction entre des problèmes dans le système d'acheminement et des problèmes imprévus chez les hôtes affectés par la dénumérotation.

Étape 5 – Prendre les sauvegardes finales.

Étape 6 – Convertir les adresses et les noms, ou commencer la coexistence.

- Faire les changements nécessaires pour le DNS et les pare-feu.
- Redémarrer comme nécessaire les routeurs et les serveurs.
- Nettoyer les antémémoires comme approprié.
- Se souvenir que les définitions de noms statiques dans les routeurs peuvent n'être pas affectées par les changements du DNS.
- Coordonner les changements avec les organisations externes affectées (par exemple, FAI, partenaires commerciaux, registraires d'acheminement)

Étape 7 – Documenter ce qui ne l'est pas déjà. Faire des notes pour aider la personne qui devra faire le prochain

dénumérotage. Partager l'expérience avec le groupe de travail PIER ou d'autres organisations appropriées.

15.1 Application des changements

Les changements liés à un dénumérotage devraient être introduits avec précaution dans les réseaux opérationnels. Pour que les changements prennent effet, il est vraisemblable qu'au moins les interfaces, et probablement les routeurs, devront être redémarrés. La séquence selon laquelle les changements sont appliqués doit être pensée avec soin, pour éviter la perte de la connexité, les boucles d'acheminement, etc., lorsque le dénumérotage est en cours.

On pourra se reporter aux études de cas présentées au groupe de travail PIER pour des exemples de fonctionnement d'expériences de dénumérotage. Les organisations qui ont subi un dénumérotage ont dû porter une attention particulière à l'information des usagers sur les pannes possibles, à la coordination des changements sur plusieurs sites, etc. C'est une décision qui appartient à l'organisation de savoir si le dénumérotage d'un routeur peut être effectué de façon incrémentaire ou doit être fait par une conversion majeure au "jour J".

Avant de faire des changements significatifs, FAITES D'ABORD DES SAUVEGARDES de tous les fichiers de configuration de routeur, des fichiers de zone du DNS, et des autres informations qui documentent votre environnement présent.

15.2 Contrôle de la configuration

Du point de vue du fonctionnement, une part importante du dénumérotage et de la suite de la maintenance du dénumérotage ne va pas reposer sur les interfaces du routeur local, que se soit pour l'interpréteur du langage de commande, fondé sur un menu, ou par des commandes graphiques, pour les aspects plus sophistiqués de la configuration, mais de faire la configuration (et ses changements) principale sur une station de travail appropriée. Sur une station de travail ou autre ordinateur à vocation générale, on peut éditer, répertorier, traiter les fichiers de configuration avec des macro processeurs et autres outils, etc. Les outils de contrôle de code source peuvent être utilisés sur les fichiers de configuration du routeur.

Une fois que le fichier de configuration est défini pour un routeur, les mécanismes pour le charger varient selon la mise en œuvre spécifique du routeur. En général, cela va inclure un transfert de fichier utilisant FTP ou TFTP dans un fichier de configuration sur le routeur, des commandes SNMP SET, ou se connecter sur le routeur comme une console distante en utilisant un émulateur de terminal pour télécharger la nouvelle configuration dans le mode de configuration interactive du routeur. L'acquisition originale des fichiers de configuration traditionnels est le processus inverse.

15.3 Éviter l'instabilité

Les processus d'acheminement tendent à l'instabilité lorsque ils doivent soudainement traiter un très grand nombre de mises à jour, comme cela peut survenir si une conversion "au jour J" n'est pas planifiée avec grand soin. Une ligne directrice générale est de ne faire de changements que dans une seule partie d'une hiérarchie d'acheminement à la fois.

La conception d'un système d'acheminement devrait être hiérarchique jusqu'aux plus petits domaines. Bien que OSPF et IS-IS aient des modèles explicitement hiérarchisés sur la base de la zone, les principes hiérarchiques peuvent être utilisés avec la plupart des mises en œuvre des protocoles modernes d'acheminement. La hiérarchisation peut être imposée à un protocole tel que RIPv2 ou EIGRP par un usage judicieux de l'agrégation des chemins, le filtrage des annonces d'acheminement, etc.

Respecter un modèle hiérarchique durant le dénumérotage signifie des choses comme de dénuméroter la partie de "bout" d'un domaine d'acheminement et de laisser cette partie se stabiliser avant de changer les autres parties. Autrement, il peut être raisonnable d'ajouter de nouveaux numéros au cœur de réseau, en lui permettant de converger, de dénuméroter les bouts, et de supprimer ensuite les vieux numéros du cœur du réseau. Évidemment, ces lignes directrices sont plus praticables lorsque il y a des espaces d'adresses ancien et nouveau distincts, sans chevauchement. Si un bloc d'adresses doit simplement être réalloué, on peut s'attendre à quelques pertes de service.

16. Remerciements

Merci à Jim Bound, Paul Ferguson, Geert Jan de Groot, Roger Fajman, Matt Holdrege, Dorian Kim, Walt Lazear, Eliot Lear, Will Leland, et Bill Manning pour leurs conseils et leurs commentaires.

17. Références

[RFC1518] Y. Rekhter et T. Li, "Architecture pour l'allocation d'adresses IP avec CIDR", septembre 1993. *(Historique*

[RFC1631] K. Egevang, P. Francis, "Le traducteur d'adresse réseau (NAT) IP", juin 1994. *(Info., remplacé par 3022)*

[RFC1812] F. Baker, "Exigences pour les routeurs IP version 4", juin 1995. *(Mise à jour par la RFC 2644)*

[RFC1879] B. Manning, éd., "Résultats d'expérience de sous-réseau de classe A et recommandations", janvier 1996. *(Info)*

[RFC1897] R. Hinden, J. Postel, "Allocation d'adresses d'essai IPv6", janvier 1996. (*Obsolète, voir* RFC2471) *(Exp.)*

[RFC1900] B. Carpenter, Y. Rekhter, "Un dénumérotage représente du travail", février 1996. *(Information)*

[RFC1918] Y. Rekhter et autres, "Allocation d'adresse pour les internets privés", BCP 5, février 1996.

[RFC2050] K. Hubbard, M. Kosters, D. Conrad, D. Karrenberg, J. Postel, "Lignes directrices pour l'allocation des adresses IP par les registraires Internet", novembre 1996. *(Remplace* RFC1466) (BCP0012)

[RFC2058] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Service d'authentification distante d'utilisateur appelant (RADIUS)", janvier 1997. (*Obsolète, voir* RFC2138) *(P.S.)*

[RFC2071] P. Ferguson, H. Berkowitz, "Généralités sur la dénumérotation du réseau : pourquoi on la veut et ce qu'elle est", janvier 1997. *(Information)*

[RFC2280] C. Alaettinoglu, T. Bates, E. Gerich, D. Karrenberg, D. Meyer, M. Terpstra, C. Villamizar, "Langage de spécification des politiques d'acheminement (RPSL)", janvier 1998. (*Obsolète, voir* RFC2622) *(P.S.)*

[RFC2332] J. Luciani et autres, "Protocole de résolution du prochain bond NBMA (NHRP)", avril 1998. *(P.S.)*

[RFC2333] D. Cansever, "Déclaration d'applicabilité du protocole NHRP", avril 1998. *(P.S.)*

[Carpenter] Message à la liste de diffusion PIER, voir les archives du groupe de travail PIER

[Lear] Message à la liste de diffusion PIER, voir les archives du groupe de travail PIER

[deGroot] Message à la liste de diffusion PIER, voir les archives du groupe de travail PIER

[Wobus] "DHCP FAQ Memo", http://web.syr.edu/~jmwobus/comfaqs/dhcp.faq.html

18. Adresse de l'auteur

Howard C. Berkowitz
PSC International
1600 Spring Hill Road, Suite 310
Vienna VA 22182
USA