
RFC 1234: Tunneling de trafic IPX sur un réseau IP

Auteur: D. Provan, Novell Inc. 06/1991
Traduction : Franck "Linuxshell" Verrot 03/2002

Note du traducteur:

Ce document est une traduction non-officielle de la RFC 1234 sur le tunneling de trafic IPX à travers les réseaux IP.
L'auteur de cette traduction décline toute responsabilité sur l'utilisation de ce document et/ou su d'éventuelles erreurs de traduction.
Concernant les droits du traducteur: le traducteur renonce à ses droits sur la reproduction de ce document si l'ensemble de ces conditions est respecté: les reproductions doivent être complètes(contenant cette note), d'un seul tenant(un seul fichier ou un ensemble de pages physiquement reliées), sans aucune modification du contenu et réalisées à partir de la dernière version de ce document disponible ici ou bien en mailant le traducteur.
A noter, et l'information est importante, que les licenses sont traduites, procurez-vous la RFC officielle pour les version originales.

Statut de ce document:

Ce document descrit une méthode d'encapsulation de datagrammes IP à l'intérieur de paquets UPD avec que le trafic IPX puissent voyager à travers un réseau internet IP. Cette RFC spécifie une piste des standards du protocole IAB pour la communauté Internet, et recherche discussions et suggestions pour des améliorations. Veuillez vous référer à l'édition actuelle de l'"IAB Official Protocol Standards" pour l'état de standardisation et le statut de ce protocole.
La distribution de ce document est illimitée.

Introduction:

Le protocole d'échange de paquet sur Internet (Internet Packet eXchange ou IPX) est le protocole inter-réseau utilisé par la suite de protocole NetWare par Novell. Pour les sujets de ce document, IPX est équivalent fonctionnellement au protocole internet par datagrammes(IDP) par la suite de protocole Xerox Network Systems[1]. Ce document décrit une méthode d'encapsulation de datagrammes IPX à l'intérieur de paquets UDP[2] afin que le trafic UDP puissent voyager voyager à travers un réseau internet IP[3].

Cette RFC permet une implémentation IPX pour voir un internet IP comme un

simple réseau IPX. Une implémentatipn de ce mémo encapsulera des datagrammes IPX dans des paquets UDP de la même manière que toute implémentation en hardware encapsulerait des datagrammes IPX dans des armatures matérielles. Des réseaux d'IPX peuvent être reliés ensemble à travers les internets qui supportent uniquement le trafic IP.

Format de paquet:
==========

Chaque datagramme IPX est contenu dans la portion des données(data portion) d'un paquet UDP. Tous les champs IP et UDP sont initialisés normalement. Les ports source et destination dans le paquet UDP doivent tous deux être initialisés à la valeur du port UDP allouée par les autorités d'assignement de numéros internet (Internet Assigned Numbers Authority) pour l'implémentation de cette méthode d'encapsulation.

Comme avec toute application UDP, la partie qui transmet a l'option d'éviter la surcharge de checksum en mettant le checksum UDP à zéro. Comme les implémentations IPX n'utilisent jamais le checksum UDP afin de préserver les paquets IPX des dommages, un "checksumming" UDP est hautemment recommandée pour l'encapsulation IPX.

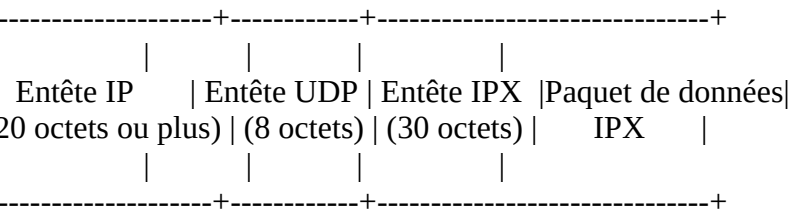

Figure 1: Un paquet IPX contenu en tant que donnée dans un paquet UDP.

Paquets réservés:
==========

Les deux premiers octets de l'entête IPX contiennent le checksum IPX. Les paquets IPX ne sont jamais envoyé avec un checksum, donc chaque entête IPX commence par deux octets de FF en héxadécimal. Les implémentations de ce schéma d'encapsulation doivent ignorer les paquets avec n'importe quelle autre valeur dans les deux premiers octets immédiatement consécutifs à l'entête UDP. Les autres valeurs sont réservées pour de futurs possibles améliorations de ce protocole d'encapsulation.

Tracés d'adresse Unicast:
==========

Les adresses IPX sont formées d'un numéro réseau de 4 octets et un numéro d'hôte de 6 octets. IPX utilise un numéro de réseau afin de router chaque paquet à travers l'internet IPX au réseau de destination. Un fois que le paquet arrive au réseau de destination, IPX utilise un numéro d'hôte de 6 octets comme

adresse hardware sur ce réseau.

Les numéros d'hôte sont également échangés dans les entêtes IPX des paquets du protocole de routage d'information IPX("IPX Routing Information Protocol" ou également RIP). Cela requiert des noeuds de fin et des routeurs en accord avec l'information sur l'adresse hardware requise pour transmettre les paquets à travers des réseaux intermédiaires sur le chemin allant au réseaux de destination.

Pour l'implémentation de ce document, les deux premiers octets du numéro d'hôte seront toujours mis à zéro et les quatre derniers octets seront toujours les quatres octets de l'adresse IP du noeud. Cela fait un tracé d'adresse trivial pour des transmissions unicast: les deux premiers numéros d'hôte sont abandonnés, laissant place à une adresse IP normale de quatre octets. Le code d'encapsulation doit utiliser cette adresse IP comme adresse de destination du tunnel de paquet UPD/IP.

Emissions entre des serveurs Clients:
==========

IPX requiert des facilités d'émission de sorte que les serveurs NetWare et les routeurs IPX partageant un réseau puissent se retrouver les uns les autres. comme la large émission d'IP d'internet n'est ni approprié ni disponible, d'autres mécanismes sont requis. Pour ce document, chaque serveur et routeur doit mainteanit une liste d'adresses IP des autres serveur IPX et routeurs sur l'internet IP. Je réferai à cette liste en tant que "liste client"("peer list"), à des membres individuels comme "client", et à tous les autres clients pris ensemble, incluant le noeud local, comme le "groupe de client". Quand IPX demande une émission, l'implémentation de l'encapsulation simule l'émission en transmettant un paquet unicast séparé à chaque client dans la liste client.

Du fait que chaque liste client soit construite à la main, différents groupes de clients peuvent partager la même IP internet sans en connaître une autre. Cela diffère d'un réseau IPX normal où tous les clients se retrouveront les uns les autres automatiquement en utlisant les facilités d'émission du hardware.

La liste de clients à chaque noeud doit contenir les autres clients dans le groupe de client. Dans la plupart des cas, la connectivité souffera si les émissions d'un client en recherche d'un autre client faillissent constamment dans le groupe.

La liste de client peut être implémentées en utilisant l'IP multicast*[4], mais comme les facilités du multicast ne sont pas largement disponibles en ces temps, aucune adresse multicast bien connue n'a été assignée et aucune implémentation utilisant le multicast n'existe. Comme l'IP multicast est déployée dans les implémentations IP, il peut être utilisé en incluant simplement dans la liste client une adresse IP multicast pour les serveurs IPX et les routeurs. L'adresse IP multicast devra remplacer les adresses IP de tous les clients qui recevront les paquets IP multicast envoyés depuis ce client. (* = multi-émissions).

Emissions par clients:

Typiquement, les noeuds client NetWare n'ont pas besoin de recevoir d'émissions, dont normalemment un noeud client NetWare sur un internet IP ne nécessitera pas d'être inclut dans les listes client sur les serveurs.

D'un autre côté, les clients d'un réseau IPX ont besoin d'envoyer des émissions de manière à localiser les serveurs et découvrir des routes. Une implémentation client d'encapsulation UDP peut gérer cela en ayant une liste configurée d'adresses IP de tous les serveurs et routeurs dans le groupe de client fonctionnant sur un inter-réseau IP. Comme avec la liste de client sur un serveur, l'implémentation client devra simuler une émission en envoyant une copie du paquet à chaque adresse IP dans sa liste de serveurs et routeurs IPX. Une des adresses IP dans la liste, peut-être la seule, peut être une adresse d'émission ou, si possible, une adresse multicast. Cela permet au client de communiquer avec les membres d'un groupe de client sans avoir à connaître leur adresses IP spécifiques.

Il est important de réaliser que les paquets d'émission envoyés depuis un client IPX doivent être capable de trouver chaque serveur et routeurs dans le groupe de client du serveur. Contrairement à IP, qui a un mécanisme de redirection unicast, les systèmes finaux IPX sont responsables de la découverte des informations de routage en émettant une paquet demandant un routeur qui ne peut pas transmettre de paquet à la destination désirée.
Si de tel paquets ne tendent pas à rechercheentière du groupe de client du serveur, les ressources dans l'internet IPX peut être visible à un système final, à présent introuvable par celui-ci.

Unité de transmission maximale:

Bien que soient possibles des paquets IPX plus grands, l'unité standard maximale de transmission pour IPX est 576 octets. Par conséquent, 576 octets est l'unité standard de transmission par recommandée par défaut pour les paquets IPX destinés à être envoyés avec la technique d'encapsulation. Avec les huit octets de l'entête IDP et les vingt octets de l'entête IP, le paquet IP résultant fera ainsi 604 octets. A noter qu'il est plus grand, les 576 octets de la taille maximale de l'implémentation IP sont requis pour accepter. Toute implémentation IP supportant cette technique d'encapsulation doit être
capable de recevoir des paquets IP de 604 octets.

Comme les amélioration des protocoles et hardwares permettent des unité de transmission IP plus grands et non-fragmentés, les paquets de taille 576 octets maximaux peuvent devenir une responsabilité. Pour cette raison, il est recommandé que la taille des unités de transmission IPX maximale soit configurable dans les implémentations de ce document.

Points sur la de sécurité

==========

Utilisant une large zone, un réseau de manière générale tel un internet IP dans la position normale d'un cablage physique présente quelques problèmes de sécurité anormalement rencontrés dans des inter-réseaux IPX.
Le médias normaux sont typiquement protégés physiquement d'accès extérieur; les internets IP autorisent typiquement un accès extérieur.

Le résultat principal est que la sécurité de l'inter-réseau IPX est seulement aussi bon que la sécurité de l'internet IP entier à travers ses propres tunnels. Les classes d'attaque distribuées suivantes sont possibles:

1) Des clients IPX non-autorisés peuvent avoir accès à des ressources à travers des attaques d'accès normaux tel que le cassage de mot de passe.

2) Des gateways IPX non-autorisés peuvent diriger le traffix IPX sur des destinations inattendues.

3) Des agents non-autorisés peuvent monitorer et manipuler le flux du trafic IPX sur des médias physique utilisés par l'internet IP et sous le contrôle de l'agent.

Sur une grande étendue, ces risques de sécurité sont typiques des risques recontrés sur une autre application utilisant un internet IP. Ils sont ici mentionnés seulement parce que IPX n'est pas normalement suspicieux de ces médias. Les administrateurs d'un réseau IPX devront être consciens de ces risques de sécurité additionnels.

Numéros assignés

Les autorités d'assignement de numéros internet assignent des numéros de ports UDP bien-connus. Ils ont assignés le port numéro 213 en décimal à la technique d'encapsulation IPX décrite dans ce document [5].

Remerciements

Cette technique d'encapsulation a été developpé indépendamment par Schneider & Koch et par Novell. Je voudai remercier Thomas Ruf de Schneider & Koch pour avoir relu ce document pour l'accorder avec l'implémentation de Schneider & Koch et aussi pour ses autres suggestions utiles.

References

[1] Xerox, Corp., "Internet Transport Protocols", XSIS 028112, Xerox Corporation, December 1981.

[2] Postel, J., "User Datagram Protocol", RFC 768, USC/Information

Sciences Institute, August 1980.

[3] Postel, J., "Internet Protocol", RFC 791, DARPA, September 1981.

[4] Deering, S., "Host Extensions for IP Multicasting", RFC 1112, Stanford University, August 1989.

[5] Reynolds, J., and J. Postel, "Assigned Numbers", RFC-1060, USC/Information Sciences Institute, March 1990.

Adresse de l'auteur

Don Provan
Novell, Inc.
2180 Fortune Drive
San Jose, California, 95131

Téléphone: (408)473-8440

EMail: donp@Novell.Com