Groupe de travail Réseau
Request for Comments : 1180
Traduction Claude Brière de L'Isle

T. Socolofsky & C. Kale
Spider Systems Limited
janvier 1991

Guide pour TCP/IP

Statut de ce mémoire
La présente RFC est un guide de la suite de protocoles TCP/IP qui se focalisant en particulier sur les étapes de la transmission d'un datagramme IP de l'hôte de source à l'hôte de destination en passant par un routeur. Elle ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Table des matières

1. Introduction

Ce guide ne contient qu'une vue des points saillants de TCP/IP, ce n'est donc que le "squelette" de la technologie TCP/IP. Il omet l'historique du développement et des fondements, l'utilisation commerciale, et son avenir par rapport à l'OSI de l'ISO. Bien sûr, une grande partie des informations techniques est aussi omise. Ce qui reste est le minimum des informations qui doivent être comprises par les professionnels qui travaillent dans un environnement TCP/IP. Ces professionnels sont les administrateurs de systèmes, les programmeurs de systèmes et les gestionnaires de réseau.

Ce guide utilise des exemples tirés de l'environnement TCP/IP UNIX , mais les principaux points s'appliquent sur toutes les mises en œuvre de TCP/IP.

Noter que l'objet du présent mémoire est l'explication, et non la définition. Si des questions se posent quand à la spécification correcte d'un protocole, on est prié de se référer aux RFC qui définissent réellement les normes.

La section qui suit donne une vue d'ensemble de TCP/IP. Elle est suivie des descriptions détaillées des composants individuels.

2. Vue d'ensemble de TCP/IP

Le terme générique de "TCP/IP" signifie habituellement tout ce qui se rapporte aux protocoles spécifiques de TCP et IP. Il peut inclure d'autres protocoles, applications, et même le support réseau. Un échantillon de ces protocoles est UDP, ARP, et ICMP. Un échantillon de ces applications est TELNET, FTP, et RCP. Un terme plus précis est "technologie internet". Un réseau qui utilise la technologie Internet est appelé un "internet".

2.1 Structure de base

Pour comprendre cette technologie, on doit d'abord comprendre la structure logique suivante :

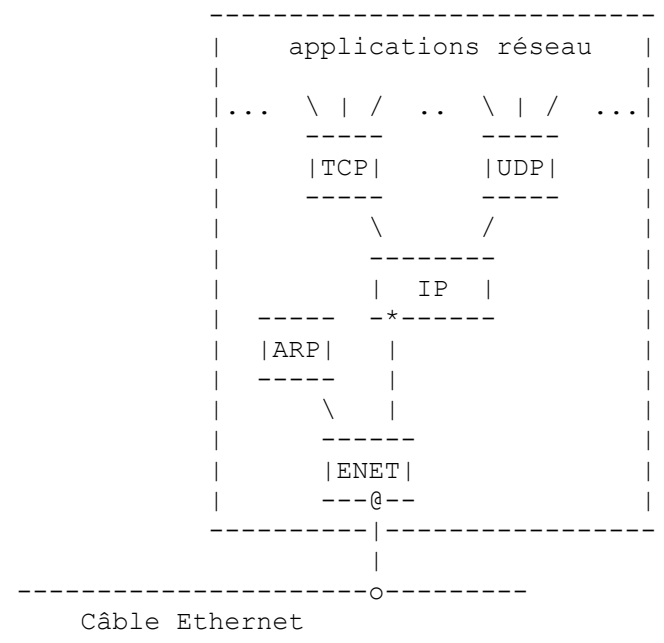

Figure 1 : Nœud réseau TCP/IP de base

Ceci est la structure logique des couches de protocoles à l'intérieur d'un ordinateur sur un internet. Chaque ordinateur qui peut communiquer en utilisant la technologie internet a une telle structure logique. C'est cette structure logique qui détermine le comportement de l'ordinateur sur l'internet. Les boîtes représentent le traitement des données lorsque elles passent à travers l'ordinateur, et les lignes qui connectent les boîtes montrent le chemin des données. La ligne horizontale du bas représente le câble Ethernet ; le "o" est l'émetteur-récepteur. Le signe "*" est l'adresse IP et le signe "@" est l'adresse Ethernet. Il est essentiel de comprendre cette structure logique pour comprendre la technologie internet ; on s'y réfère tout au long de ce guide.

2.2 Terminologie

Le nom d'une unité de données qui s'écoule à travers un internet dépend de son existence dans la pile de protocoles. En résumé, si elle est sur un Ethernet, on l'appelle une trame Ethernet ; si elle est entre le pilote Ethernet et le module IP, on l'appelle un paquet IP ; si elle est entre le module IP et le module UDP, on l'appelle un datagramme UDP ; si elle est entre le module IP et le module TCP, on l'appelle un segment TCP (et plus généralement, un message de transport) et si elle est dans une application réseau, on l'appelle un message d'application.

Ces définitions sont imparfaites. Les définitions réelles varient d'une publication à l'autre. Des définitions plus spécifiques se trouvent dans la RFC1122, au paragraphe 1.3.3.

Un pilote est un logiciel qui communique directement avec le matériel d'interface réseau. Un module est un logiciel qui communique avec un pilote, avec les applications réseau, ou avec un autre module.

Les termes pilote, module, trame Ethernet, paquet IP, datagramme UDP, message TCP, et message d'application sont utilisés lorsque approprié tout au long de ce guide.

2.3 Flux de données

Suivons le flux des données lorsque il s'écoule à travers la pile de protocoles de la Figure 1. Pour une application qui utilise TCP (*Protocole de contrôle de transmission*) les données passent entre l'application et le module TCP. Pour les applications qui utilisent UDP (*Protocole de datagramme d'utilisateur*) les données passent entre l'application et le module UDP. FTP (*Protocole de transfert de fichiers*) est une application typique qui utilise TCP. Sa pile de protocoles dans cet exemple est FTP/TCP/IP/ENET. SNMP (*Protocole simple de gestion de réseau*) est une application qui utilise UDP. Sa pile de protocoles dans cet exemple est SNMP/UDP/IP/ENET.

Le module TCP, le module UDP, et le pilote Ethernet sont des multiplexeurs de n à 1. Comme multiplexeurs, ils passent de nombreuses entrées sur une sortie. Ils sont aussi des démultiplexeurs de 1 à n. Comme démultiplexeurs, ils passent une entrée sur plusieurs sorties conformément au champ Type de l'en-tête de protocole.

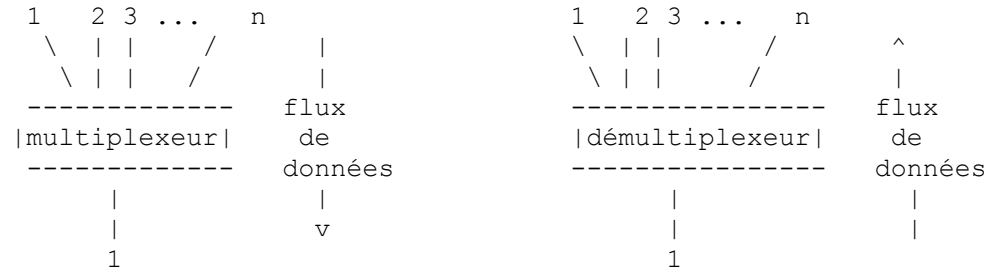

Figure 2 : Multiplexeur de 1 à n et démultiplexeur de n à 1

Si une trame Ethernet arrive du réseau dans le pilote Ethernet, le paquet peut être passé vers le haut au module ARP (*Protocole de résolution d'adresse*) ou au module IP (*Protocole Internet*). La valeur du champ Type dans la trame Ethernet détermine si la trame Ethernet est passée au module ARP ou IP.

Si un paquet IP arrive dans IP, l'unité de données est passée à TCP ou UDP, comme déterminé par la valeur du champ Protocole dans l'en-tête IP.

Si le datagramme UDP arrive dans UDP, le message d'application est monté à l'application réseau sur la base de la valeur du champ Accès dans l'en-tête UDP. Si le message TCP arrive dans TCP, le message d'application est monté à l'application réseau sur la base de la valeur du champ Accès dans l'en-tête TCP.

Le multiplexage en redescendant est simple à effectuer parce que de chaque point de départ il y a seulement un chemin de descente ; chaque module de protocole ajoute ses informations d'en-tête afin que le paquet puisse être démultiplexé à l'ordinateur de destination.

Les données qui passent des applications à TCP ou UDP convergent sur le module IP et sont envoyées à travers le pilote d'interface réseau inférieur.

Bien que la technologie internet prenne en charge de nombreux supports de réseau différents, Ethernet est utilisé pour tous les exemples de ce guide parce qu'il est le réseau physique le plus courant utilisé sous IP. L'ordinateur de la Figure 1 a une seule connexion Ethernet. L'adresse Ethernet de six octets est unique pour chaque interface d'un Ethernet et elle est localisée à l'interface inférieure du pilote Ethernet.

L'ordinateur a aussi une adresse IP de quatre octets. Cette adresse est localisée à l'interface inférieure au module IP. L'adresse IP doit être unique pour un internet.

Un ordinateur en fonctionnement connaît toujours sa propre adresse IP et sa propre adresse Ethernet.

2.4 Deux interfaces réseau

Si un ordinateur est connecté à deux Ethernets distincts comme dans la Figure 3.

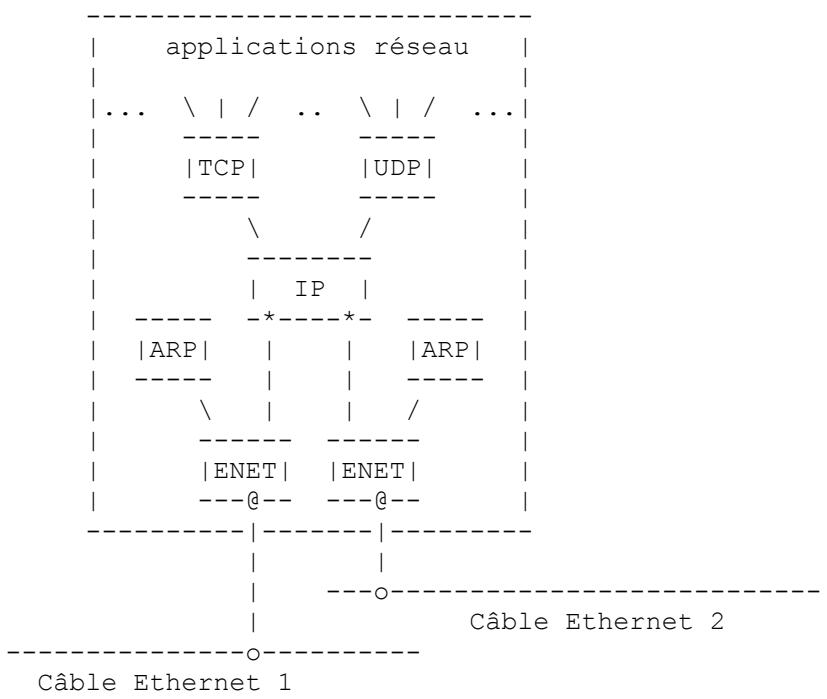

Figure 3 : Nœud réseau TCP/IP sur deux Ethernets

Prière de noter que cet ordinateur a deux adresses Ethernet et deux adresses IP.

On voit d'après cette structure que pour les ordinateurs avec plus d'une interface réseau physique, le module IP est à la fois un multiplexeur de n à m et un démultiplexeur de m à n.

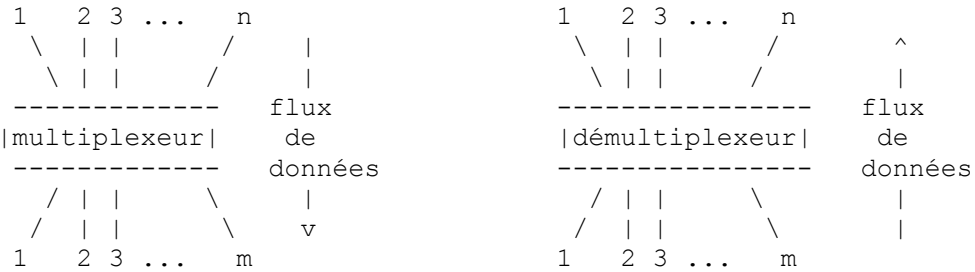

Figure 4 : Multiplexeur de n à m et démultiplexeur de m à n

Il effectue ce multiplexage dans l'une et l'autre direction pour traiter les données entrantes et sortantes. Un module IP avec plus d'une interface réseau est plus complexe que dans notre exemple d'origine car il peut transmettre des données sur le prochain réseau. Les données peuvent arriver sur toute interface réseau et être envoyées en sortie sur n'importe quel autre.

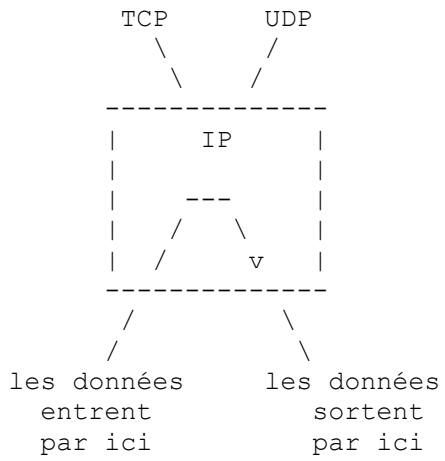

Figure 5 : Exemple de la transmission d'un paquet IP par IP

Le processus d'envoi d'un paquet IP vers un autre réseau est appelé "transmission" d'un paquet IP. Un ordinateur qui a été dédié à la tâche de transmettre des paquets IP est appelé un "routeur IP".

Comme on peut le voir d'après la figure, le paquet IP transmis ne touche jamais les modules TCP et UDP sur le routeur IP. Certaines mises en œuvre de routeur n'ont pas de module TCP ou UDP.

2.5 IP crée un seul réseau logique

Le module IP est au cœur du succès de la technologie internet. Chaque module ou pilote ajoute son propre en-tête au message à mesure qu'il descend le long de la pile de protocoles. Chaque module ou pilote retire l'en-tête correspondant du message à mesure que celui-ci monte la pile de protocoles vers l'application. L'en-tête IP contient l'adresse IP, qui construit un seul réseau logique à partir de plusieurs réseaux physiques. Cette interconnexion de réseaux physiques est à l'origine du nom "internet" *(inter réseaux)*. Un ensemble de réseaux physiques interconnectés qui délimitent la portée d'un paquet IP est appelé un "internet".

2.6 Indépendance du réseau physique

IP cache le matériel de réseau sous-jacent aux applications réseau. Si vous inventez un nouveau réseau physique, vous pouvez le mettre en service en mettant en œuvre un nouveau pilote qui connecte à l'internet en dessous de IP. Donc les applications réseau restent intactes et ne sont pas vulnérables aux changements des technologies du matériel.

2.7 Interopérabilité

Si deux ordinateurs sur un internet peuvent communiquer, ont dit qu'ils "interopèrent" ; si une mise en œuvre de technologie internet est bonne, on dit qu'elle a "l'interopérabilité". Les utilisateurs d'ordinateurs génériques bénéficient de l'installation d'un internet à cause de l'interopérabilité des ordinateurs qui sont sur le marché. Généralement, lorsque vous achetez un ordinateur, il va interopérer. Si l'ordinateur n'a pas l'interopérabilité, et si celle-ci ne peut pas être ajoutée, il occupe une niche rare et très particulière du marché.

2.8 Après les généralités

Avec l'ensemble des fondements, nous allons répondre aux questions suivantes :

Lors de l'envoi d'un paquet IP, comment l'adresse de destination Ethernet est-elle déterminée ?
Comment IP sait-il quelles interfaces réseau inférieures utiliser lors de l'envoi d'un paquet IP ?
Comment un client sur un ordinateur atteint-il le serveur sur un autre ordinateur ?
Pourquoi TCP et UDP existent-ils tous deux, au lieu de juste l'un ou l'autre ?
Pourquoi les applications réseau sont elles disponibles ?

On y répondra tout à tour, après un rappel sur Ethernet.

3. Ethernet

Cette section fait un bref rappel de la technologie Ethernet.

Une trame Ethernet contient l'adresse de destination, l'adresse de source, le champ Type, et les données.

Une adresse Ethernet fait six octets. Chaque appareil a sa propre adresse Ethernet et est à l'écoute des trames Ethernet qui ont cette adresse de destination. Tous les appareils sont aussi à l'écoute des trames Ethernet qui ont une adresse de destination à caractère générique de "FF-FF-FF-FF-FF-FF" (en hexadécimal), appelée une adresse de "diffusion".

Ethernet utilise l'accès multiple avec surveillance de signal et détection de collision (CSMA/CD, *Carrier Sense and Multiple Access with Collision Detection*). CSMA/CD signifie que tous les appareils communiquent sur un seul support, qu'un seul peut transmettre à la fois, et qu'ils peuvent tous recevoir simultanément. Si deux appareils essayent d'émettre au même instant, la collision de transmission est détectée, et les deux appareils attendent pendant une période aléatoire (mais brève) avant d'essayer de recommencer à émettre.

3.1 Analogie avec l'homme

Une bonne analogie de la technologie Ethernet serait celle d'un groupe de personne qui parlent dans une petite pièce, complètement noire. Dans cette analogie, le support de réseau physique est les ondes sonores dans l'air de la pièce au lieu des signaux électriques d'un câble coaxial.

Chaque personne peut entendre les mots prononcés par une autre personne (détection de la porteuse). Chacun dans la pièce a une capacité égale à parler (accès multiple) mais aucun d'entre eux ne fait de longs discours parce qu'ils sont polis. Si une personne est impolie, on lui demande de quitter la pièce (c'est-à-dire qu'elle est sortie du réseau).

Personne ne parle pendant qu'un autre est en train de parler. Mais si deux personnes commencent à parler au même instant, chacune d'elles le sait parce que chacune entends quelque chose qu'elle n'a pas dit (détection de collision). Lorsque ces deux personnes remarquent cette condition, elles attendent un petit moment puis l'une d'elles commence à parler. L'autre entend parler et attend que le premier ait fini de parler avant de délivrer son propre discours.

Chaque personne a un nom unique (adresse Ethernet unique) pour éviter la confusion. Chaque fois que l'une d'elles parle, elle préface le message du nom de la personne à qui elle parle et de son propre nom (adresse Ethernet de destination et de source, respectivement) c'est-à-dire, "Hello Jeanne, c'est Jacques, ..blah blah blah...". Si l'envoyeur veut parler à tout le monde, il pourrait dire "à tous" (adresse de diffusion) c'est-à-dire, "Hello tous, c'est Jacques, ..blah blah blah...".

4. ARP

Lors de l'envoi d'un paquet IP, comment l'adresse de destination Ethernet est-elle déterminée ?

Le protocole de résolution d'adresse (ARP, *Address Resolution Protocol*) est utilisée pour traduire les adresses IP en adresses Ethernet. La traduction n'est faite que pour les paquets IP sortants, parce que c'est alors que l'en-tête IP et l'en-tête Ethernet sont créés.

4.1 Tableau ARP pour la traduction d'adresse

La traduction est effectuée avec une recherche sur un tableau. Celui-ci, qui est appelé un tableau ARP, est conservé en mémoire et contient une rangée pour chaque ordinateur. Il y a une colonne pour les adresses IP et une colonne pour les adresses Ethernet. Quand on traduit une adresse IP en adresse Ethernet, le tableau est parcouru pour chercher une adresse IP correspondante. Ce qui suit est un tableau ARP simplifié :

Adresse IP	Adresse Ethernet
223.1.2.1	08-00-39-00-2F-C3
223.1.2.3	08-00-5A-21-A7-22
223.1.2.4	08-00-10-99-AC-54

Tableau 1 : Exemple de tableau ARP

La convention humaine pour écrire l'adresse IP de quatre octets est que chaque octet est en décimal et est séparé par un point. Quand on écrit les six octets de l'adresse Ethernet, les conventions sont que chaque octet est en hexadécimal et est séparé par un signe moins ou par deux points.

Le tableau ARP est nécessaire parce que l'adresse IP et l'adresse Ethernet sont sélectionnées indépendamment ; on ne peut pas utiliser un algorithme pour traduire une adresse IP en adresse Ethernet. L'adresse IP est choisie par le gestionnaire de réseau sur la base de la localisation de l'ordinateur sur l'internet. Lorsque l'ordinateur est déplacé dans une partie différente d'un internet, son adresse IP doit être changée. L'adresse Ethernet est choisie par le fabricant sur la base de l'espace d'adresses Ethernet accordé par le fabricant. Lorsque le tableau de l'interface du matériel Ethernet est déplacée, l'adresse Ethernet change.

4.2 Scénario de traduction normal

En fonctionnement normal, une application réseau, telle que TELNET, envoie un message d'application à TCP, puis TCP envoie le message TCP correspondant au module IP. L'adresse IP de destination est connue par l'application, par le module TCP, et par le module IP. À ce point, le paquet IP a été construit et est prêt à être passé au pilote Ethernet, mais d'abord, on doit déterminer l'adresse de destination Ethernet.

Le tableau ARP est utilisé pour chercher l'adresse de destination Ethernet.

4.3 Paire demande/réponse ARP

Mais comment le tableau ARP est-il rempli pour la première fois ? La réponse est qu'il est rempli automatiquement par ARP en fonction des besoins.

Deux choses se passent quand le tableau ARP ne peut pas être utilisé pour traduire une adresse :

1. un paquet de demande ARP avec une adresse Ethernet de diffusion est envoyé sur le réseau à chaque ordinateur,
2. le paquet IP sortant est mis en file d'attente.

Chaque interface Ethernet d'ordinateur reçoit la trame Ethernet en diffusion. Chaque pilote Ethernet examine le champ Type dans la trame Ethernet et passe le paquet ARP au module ARP. Le paquet de demande ARP dit "Si votre adresse IP correspond à cette adresse IP cible, dites moi alors votre adresse Ethernet". Un paquet de demande ARP ressemble à quelque chose comme :

Adresse IP de l'envoyeur 223.1.2.1 Adresse Enet de l'envoyeur 08-00-39-00-2F-C3
Adresse IP cible 223.1.2.2 Adresse Enet cible <blanc>

Tableau 2 : Exemple de demande ARP

Chaque module ARP examine l'adresse IP et si l'adresse IP cible correspond à sa propre adresse IP, il envoie une réponse directement à l'adresse Ethernet de source. Le paquet de réponse ARP dit "Oui, cette adresse IP cible est la mienne, laissez moi vous donner mon adresse Ethernet". Un paquet de réponse ARP a le contenu du champ envoyeur/cible échangé par rapport à ceux de la demande. Il ressemble à quelque chose comme ceci :

Adresse IP de l'envoyeur 223.1.2.2 Adresse Enet de l'envoyeur 08-00-28-00-38-A9
Adresse IP cible 223.1.2.1 Adresse Enet cible 08-00-39-00-2F-C3

Tableau 3 : Exemple de réponse ARP

La réponse est reçue par l'ordinateur d'envoi d'origine. Le pilote Ethernet regarde le champ Type dans la trame Ethernet puis passe le paquet ARP au module ARP. Le module ARP examine le paquet ARP et ajoute les adresses IP et Ethernet de l'envoyeur à son tableau ARP.

Le tableau mis à jour ressemble maintenant à ceci :

Adresse IP	Adresse Ethernet
223.1.2.1	08-00-39-00-2F-C3
223.1.2.2	08-00-28-00-38-A9
223.1.2.3	08-00-5A-21-A7-22
223.1.2.4	08-00-10-99-AC-54

Tableau 4 : Tableau ARP après la réponse

4.4 Suite des scénarios

La nouvelle traduction a maintenant été installée automatiquement dans le tableau, juste quelques millisecondes après qu'elle a été nécessaire. Comme vous vous en souvenez de l'étape 2 ci-dessus, le paquet IP sortant a été mis en file d'attente. Ensuite, la traduction d'adresse IP en adresse Ethernet est effectuée par une recherche dans le tableau ARP puis la trame Ethernet est transmise sur l'Ethernet. Donc, avec les nouvelles étapes 3, 4, et 5, le scénario pour l'ordinateur envoyeur est :

1. Un paquet de demande ARP avec une adresse de diffusion Ethernet est envoyé sur le réseau à chaque ordinateur.
2. Le paquet IP sortant est mis en file d'attente.
3. La réponse ARP arrive avec la traduction d'adresse d'IP en Ethernet pour le tableau ARP.
4. Pour le paquet IP mis en file d'attente, le tableau ARP est utilisé pour traduire l'adresse IP en adresse Ethernet.
5. La trame Ethernet est transmise sur l'Ethernet.

En résumé, quand la traduction manque dans le tableau ARP, un paquet IP est mis en file d'attente. Les données de traduction sont rapidement remplies avec la demande/réponse ARP et le paquet IP en file d'attente est transmis.

Chaque ordinateur a un tableau ARP distinct pour chacune de ses interfaces Ethernet. Si l'ordinateur cible n'existe pas, il n'y aura pas de réponse ARP et pas d'entrée dans le tableau ARP. IP va éliminer les paquets IP sortants envoyés à cette adresse. Les protocoles de couche supérieure peuvent faire la différence entre un Ethernet en panne et l'absence d'un ordinateur avec l'adresse IP cible.

Certaines mises en œuvre de IP et d'ARP ne mettent pas le paquet IP en file d'attente en attendant la réponse ARP. Le paquet IP est plutôt éliminé et la récupération de la perte du paquet IP est laissée aux soins du module TCP ou à l'application réseau UDP. Cette récupération est effectuée par une fin de temporisation et retransmission. Le message retransmis est envoyé avec succès sur le réseau parce que la première copie du message a déjà causé le remplissage du tableau ARP.

5. Protocole Internet

Le module IP est au cœur de la technologie internet et l'essence de IP est son tableau d'acheminement. IP utilise ce tableau en mémoire pour prendre toutes les décisions sur l'acheminement d'un paquet IP. Le contenu du tableau d'acheminement est défini par l'administrateur de réseau. Les fautes bloquent la communication.

Comprendre comment un tableau d'acheminement est utilisé c'est comprendre l'inter réseautage. Cette compréhension est nécessaire pour la bonne administration et maintenance d'un réseau IP.

Le tableau d'acheminement sera mieux compris en ayant d'abord une idée de l'acheminement, puis en regardant les adresses réseau IP, puis en examinant les détails.

5.1 Acheminement direct

La figure ci-dessous est un petit internet avec 3 ordinateurs : A, B, et C. Chaque ordinateur a la même pile de protocoles TCP/IP que dans la Figure 1. L'interface Ethernet de chaque ordinateur a sa propre adresse Ethernet. Chaque ordinateur a une adresse IP allouée à l'interface IP par le gestionnaire de réseau, qui a aussi alloué un numéro de réseau IP à l'Ethernet.

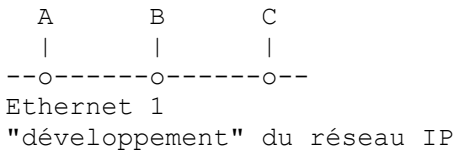

Figure 6. Un réseau IP

Lorsque A envoie un paquet IP à B, l'en-tête IP contient l'adresse IP de A comme adresse IP de source, et l'en-tête Ethernet contient l'adresse Ethernet de A comme adresse Ethernet de source. Aussi, l'en-tête IP contient l'adresse IP de B comme adresse IP de destination et l'en-tête Ethernet contient l'adresse Ethernet de B comme adresse Ethernet de destination.

adresse	source	destination
En-tête IP	A	B
En-tête Ethernet	A	B

Tableau 5 : Adresses dans une trame Ethernet pour un paquet IP de A à B

Pour ce simple cas, IP est redondant parce que IP ajoute peu au service offert par Ethernet. Cependant, IP ajoute du coût : le traitement de CPU supplémentaire et la bande passante du réseau pour générer, transmettre, et analyser l'en-tête IP.

Lorsque le module IP de B reçoit le paquet IP de A, il vérifie l'adresse IP de destination par rapport à la sienne, cherchant une correspondance, puis il passe le datagramme au protocole de niveau supérieur.

Cette communication entre A et B utilise l'acheminement direct.

5.2 Acheminement indirect

La figure ci-dessous est une vue plus réaliste d'un internet. Il est composé de 3 Ethernets et de 3 réseaux IP connectés par un routeur IP appelé ordinateur D. Chaque réseau IP a 4 ordinateurs ; chaque ordinateur a sa propre adresse IP et Ethernet.

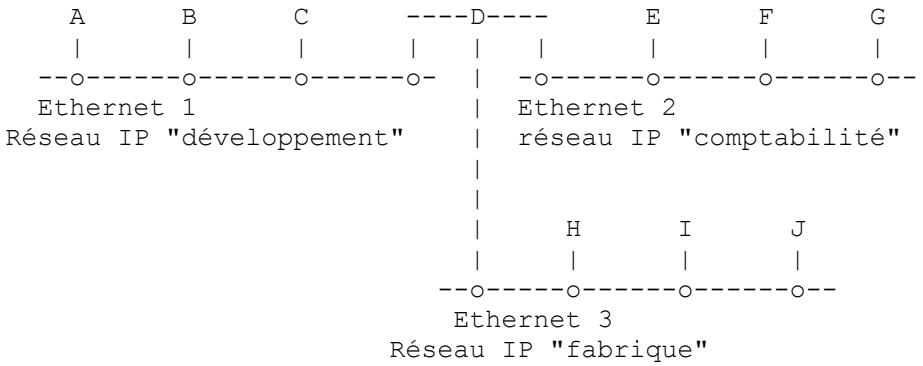

Figure 7. Trois réseaux IP; un internet

Sauf pour l'ordinateur D, chaque ordinateur a une pile de protocole TCP/IP comme celle de la Figure 1. L'ordinateur D est le routeur IP ; il est connecté aux trois réseaux et a donc trois adresses IP et trois adresses Ethernet. L'ordinateur D a une pile de protocoles TCP/IP similaire à celle de la Figure 3, sauf qu'il a trois modules ARP et trois pilotes Ethernet au lieu de deux. Noter que l'ordinateur D a seulement un module IP.

Le gestionnaire de réseau a alloué un numéro univoque, appelé un numéro de réseau IP, à chacun des Ethernets. Les numéros de réseau IP ne sont pas montrés sur ce diagramme, qui a juste les noms des réseaux.

Lorsque l'ordinateur A envoie un paquet IP à l'ordinateur B, le processus est identique à celui de l'exemple du réseau unique précédent. Toute communication entre les ordinateurs localisés sur un seul réseau IP correspondent à l'acheminement direct dont l'exemple a été discuté précédemment.

Lorsque les ordinateurs D et A communiquent, c'est une communication directe. Lorsque les ordinateurs D et E communiquent, c'est une communication directe. Lorsque les ordinateurs D et H communiquent, c'est une communication directe. C'est comme cela parce que chacune de ces paires d'ordinateurs est sur le même réseau IP.

Cependant, lorsque l'ordinateur A communique avec un ordinateur qui est sur l'autre côté du routeur IP, la communication n'est plus directe. A doit utiliser D pour transmettre le paquet IP au prochain réseau IP. Cette communication est appelée "indirecte".

Cet acheminement des paquets IP est fait par les modules IP et se fait de façon transparente pour TCP, UDP, et les applications réseau.

Si A envoie un paquet IP à E, l'adresse IP de source et l'adresse Ethernet de source sont celles de A. L'adresse IP de destination est celle de E, mais parce que le module IP de A envoie les paquets IP à D pour les transmettre, l'adresse Ethernet de destination est celle de D.

adresse	source	destination
En-tête IP	A	E
En-tête Ethernet	A	D

Tableau 6. Adresses dans une trame Ethernet pour un paquet IP de A pour E (avant D)

Le module IP de D reçoit le paquet IP et en examinant l'adresse IP de destination, il dit "Ceci n'est pas mon adresse IP", et

il envoie le paquet IP directement à E.

adresse	source	destination
En-tête IP	A	E
En-tête Ethernet	D	E

Tableau 7. Adresses dans une trame Ethernet pour un paquet IP de A pour E (après D)

En résumé, pour les communications directes, l'adresse IP de source et l'adresse Ethernet de source sont toutes deux celle de l'envoyeur, et l'adresse IP de destination et l'adresse Ethernet de destination sont celle du receveur. Pour la communication indirecte, l'adresse IP et les adresses Ethernet ne s'apparient pas de cette façon.

Cet exemple d'internet est très simple. Les réseaux réels sont souvent compliqués par de nombreux facteurs, résultant en plusieurs routeurs IP et plusieurs types de réseaux physiques. Cet exemple d'internet pourrait voir le jour parce que le gestionnaire du réseau veut partager un grand Ethernet afin d'isoler le trafic de diffusion Ethernet.

5.3 Règles d'acheminement du module IP

Ce survol de l'acheminement a montré ce qui arrive, mais pas comment cela arrive. Examinons maintenant les règles, ou les algorithmes, utilisés par le module IP.

Pour un paquet IP sortant, qui entre dans IP en venant d'une couche supérieure, IP doit décider si il envoie le paquet IP directement ou indirectement, et IP doit choisir une interface réseau inférieure. Ces choix sont faits en consultant le tableau d'acheminement.

Pour un paquet IP entrant, qui entre dans IP en provenant d'une interface inférieure, IP doit décider si il transmet le paquet IP ou si il le passe à une couche supérieure. Si le paquet IP est transmis, il est traité comme un paquet IP sortant.

Lorsque un paquet IP entrant arrive, il n'est jamais retransmis sur la même interface réseau.

Ces décisions sont prises avant que le paquet IP ne soit passé à l'interface inférieure et avant que ne soit consulté le tableau ARP.

5.4 Adresse IP

Le gestionnaire de réseau alloue les adresses IP aux ordinateurs conformément au réseau IP auquel l'ordinateur est rattaché. Une partie des quatre octets de l'adresse IP est le numéro de réseau IP, l'autre partie est le numéro IP de l'ordinateur (ou numéro d'hôte). Pour l'ordinateur dans le tableau 1, avec une adresse IP de 223.1.2.1, le numéro de réseau est 223.1.2 et le numéro d'hôte est 1.

La portion de l'adresse qui est utilisée pour le numéro de réseau et pour le numéro d'hôte est définie par les bits de poids fort dans les quatre octets de l'adresse. Tous les exemples d'adresses IP de ce guide sont du type classe C, ce qui signifie que les trois premiers bits indiquent que 21 bits font le numéro de réseau et 8 bits sont le numéro d'hôte. Cela permet 2 097 152 réseaux de classe C avec jusqu'à 254 hôtes sur chaque réseau.

L'espace d'adresse IP est administré par le NIC (Centre d'informations réseau). Tous les internets qui sont connectés à l'Internet mondial doivent utiliser des numéros de réseau alloués par le NIC. Si vous construisez votre propre internet et si vous n'avez pas l'intention de le connecter à l'Internet, vous devrez quand même obtenir votre numéro de réseau auprès du NIC. Si vous vous attribuez votre propre numéro, vous courrez le risque de confusion et de chaos dans l'éventualité où votre internet se connecterait à un autre internet.

5.5 Noms

Les gens se réfèrent aux ordinateurs avec des noms, et pas avec des numéros. Un ordinateur appelé alpha peut avoir l'adresse IP 223.1.2.1. Pour les petits réseaux, ces données de traduction de nom en adresse sont souvent conservées dans chaque ordinateur dans le fichier "hôtes". Pour les plus grands réseaux, ce fichier de données de traduction est mémorisé sur un serveur et l'accès se fait par le réseau en cas de besoin. Quelques lignes de ce fichier pourraient ressembler à ceci :

```
223.1.2.1   alpha
223.1.2.2   beta
223.1.2.3   gamma
223.1.2.4   delta
223.1.3.2   epsilon
223.1.4.2   iota
```

L'adresse IP est la première colonne et le nom de l'ordinateur est dans la seconde colonne.

Dans la plupart des cas, vous pouvez installer des fichiers "hôtes" identiques sur tous les ordinateurs. Vous remarquerez que "delta" a seulement une entrée dans ce fichier bien qu'il ait trois adresses IP. Delta peut être atteint par n'importe laquelle de ses adresses IP ; celle qui est utilisée importe peu. Quand delta reçoit un paquet IP et regarde l'adresse de destination, il va reconnaître toutes ses propres adresses IP.

Les réseaux IP ont aussi reçu des noms. Si vous avez trois réseaux IP, votre fichier "réseaux" pour récapituler ces noms pourrait ressembler à ceci :

```
223.1.2     développement
223.1.3     comptabilité
223.1.4     fabrique
```

Le numéro de réseau IP est dans la première colonne et son nom est dans la seconde colonne.

D'après cet exemple, on peut voir que alpha est le numéro d'ordinateur 1 sur le réseau développement, que beta est l'ordinateur numéro 2 sur le réseau développement, et ainsi de suite. On peut dire aussi que alpha est développement.1, que beta est développement.2, et ainsi de suite.

Les fichiers d'hôtes ci-dessus sont adéquats pour les usagers, mais le gestionnaire de réseau va probablement remplacer la ligne pour delta par :

```
223.1.2.4   devnetrouter   delta
223.1.3.1   facnetrouter
223.1.4.1   accnetrouter
```

Ces trois nouvelles lignes pour les fichiers d'hôtes donnent à chacune des adresses IP de delta un nom significatif. En fait, La première adresse IP sur la liste a deux noms ; "delta" et "devnetrouter" sont synonymes. En pratique "delta" est le nom d'utilisation générale de l'ordinateur et les trois autres noms ne sont utilisés que pour l'administration du tableau d'acheminement IP.

Ces fichiers sont utilisés par les commandes d'administration du réseau et les applications réseau pour fournir des noms significatifs. Ils ne sont pas nécessaires pour le fonctionnement d'un internet, mais il le rendent plus facile pour nous.

5.6 Tableau d'acheminement IP

Comment IP sait-il quelle interface réseau utiliser lors de l'envoi d'un paquet IP ? IP regarde dans le tableau d'acheminement en utilisant une clé de recherche du numéro de réseau IP extraite de l'adresse de destination IP.

Le tableau d'acheminement contient une rangée pour chaque chemin. Les principales colonnes dans le tableau d'acheminement sont le numéro de réseau IP, le fanion direct/indirect, l'adresse IP du routeur, et le numéro d'interface. IP se réfère à ce tableau pour chaque paquet IP sortant.

Sur la plupart des ordinateurs, le tableau d'acheminement peut être modifié avec la commande "route". Le contenu du tableau d'acheminement est défini par le gestionnaire de réseau, parce que c'est lui qui alloue les adresses IP aux ordinateurs.

5.7 Détails de l'acheminement direct

Pour expliquer comment il est utilisé, visitons en détails les situations d'acheminement que nous avons vues précédemment.

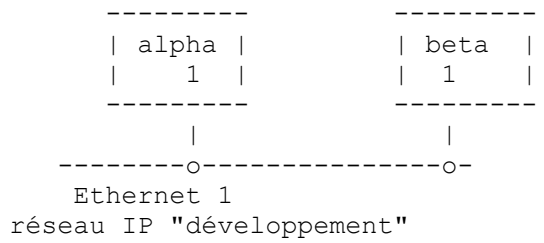

Figure 8. Vue en gros plan sur un réseau IP

Le tableau d'acheminement à l'intérieur de alpha ressemble à ceci :

réseau	fanion direct/indirect	routeur	numéro d'interface
développement	direct	<blanc>	1

Tableau 8. Exemple d'un tableau d'acheminement simple

On peut voir cela sur certains systèmes UNIX avec la commande "netstat -r". Avec ce réseau simple, tous les ordinateurs ont des tableaux d'acheminement identiques.

Pour l'exposé, le tableau est repris sans la traduction du numéro de réseau en nom de réseau.

réseau	fanion direct/indirect	routeur	numéro d'interface
223.1.2	direct	<blanc>	1

Tableau 9. Exemple de tableau d'acheminement simple avec les numéros

5.8 Scénario direct

Alpha envoie un paquet IP à beta. Le paquet IP est dans le module IP de alpha et l'adresse de destination est beta ou 223.1.2.2. IP extrait la portion réseau de cette adresse IP et examine la première colonne du tableau pour chercher une correspondance. Avec ce réseau, une correspondance est trouvée sur la première entrée.

Les autres informations de cette entrée indiquent que les ordinateurs sur ce réseau peuvent être atteints directement par l'interface numéro 1. Une traduction de tableau ARP est faite sur l'adresse IP de beta, puis la trame Ethernet est envoyée directement à beta via l'interface numéro 1.

Si une application essaye d'envoyer des données à une adresse IP qui n'est pas sur le réseau développement, IP va être incapable de trouver une correspondance dans le tableau d'acheminement. IP élimine alors le paquet IP. Certains ordinateurs fournissent un message d'erreur "Réseau injoignable".

5.9 Détails sur l'acheminement indirect

Regardons maintenant d'un peu plus près le scénario plus compliqué que nous avons vu précédemment.

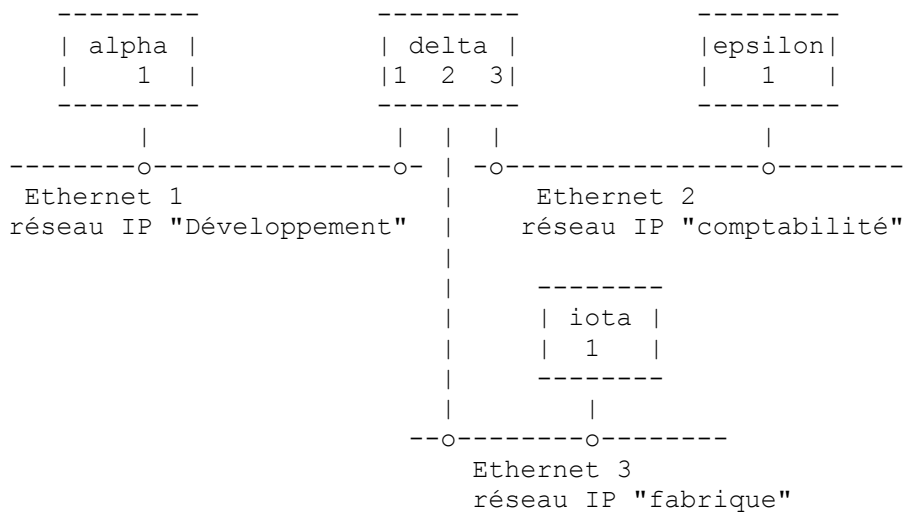

Figure 9. Vue en gros plan de trois réseaux IP

Le tableau d'acheminement au sein de alpha ressemble à ceci :

réseau	fanion direct/indirect	routeur	numéro d'interface
développement	direct	<blanc>	1
comptabilité	indirect	devnetrouter	1
fabrique	indirect	devnetrouter	1

Tableau 10. Tableau d'acheminement de Alpha

Pour les besoins de l'exposé, le tableau est repris en utilisant les numéros plutôt que les noms.

réseau	fanion direct/indirect	routeur	numéro d'interface
223.1.2	direct	<blanc>	1
223.1.3	indirect	223.1.2.4	1
223.1.4	indirect	223.1.2.4	1

Tableau 11. Tableau d'acheminement de Alpha avec les numéros

Le routeur dans le tableau d'acheminement de Alpha est l'adresse IP de la connexion de delta au réseau développement.

5.10 Scénario indirect

Alpha envoie un paquet IP à epsilon. Le paquet IP est dans le module IP de alpha et l'adresse de destination IP est epsilon (223.1.3.2). IP extrait la portion réseau de cette adresse IP (223.1.3) et examine la première colonne du tableau à la recherche d'une correspondance. Une correspondance est trouvée sur la seconde entrée.

Cette entrée indique que les ordinateurs sur le réseau 223.1.3 peuvent être atteints à travers le routeur IP devnetrouter. Le module IP de Alpha fait alors une traduction de tableau ARP pour l'adresse IP de devnetrouter et envoie le paquet IP directement à devnetrouter à travers l'interface numéro 1 de Alpha. Le paquet IP contient toujours l'adresse de destination de epsilon.

Le paquet IP arrive à l'interface du réseau développement de delta et est passé au module IP de delta. L'adresse de destination IP est examinée et comme elle ne correspond à aucune des propres adresses IP de delta, delta décide de transmettre le paquet IP.

Le module IP de Delta extrait la portion réseau de l'adresse IP de destination (223.1.3) et examine son tableau d'acheminement à la recherche d'un champ réseau correspondant. Le tableau d'acheminement de Delta ressemble à ceci :

réseau	fanion direct/indirect	routeur	numéro d'interface
développement	direct	<blanc>	1
fabrique	direct	<blanc>	3
comptabilité	direct	<blanc>	2

Tableau 12. Tableau d'acheminement de Delta

Ci-dessous figure le tableau de delta sans la traduction en noms .

réseau	fanion direct/indirect	routeur	numéro d'interface
223.1.2	direct	<blanc>	1
223.1.3	direct	<blanc>	3
223.1.4	direct	<blanc>	2

Tableau 13. Tableau d'acheminement de Delta avec les numéros

La correspondance est trouvée sur la seconde entrée. IP envoie alors le paquet IP directement à epsilon à travers l'interface numéro 3. Le paquet IP contient l'adresse IP de destination de epsilon et l'adresse Ethernet de destination de epsilon.

Le paquet IP arrive à epsilon et est passé au module IP de epsilon. L'adresse de destination IP est examinée et trouvée en correspondance avec l'adresse IP de epsilon, de sorte que le paquet IP est passé à la couche de protocole supérieure.

5.11 Résumé de l'acheminement

Lorsque un paquet IP voyage à travers un grand internet, il peut passer par de nombreux routeurs IP avant d'atteindre sa destination. Le chemin qu'il emprunte n'est pas déterminé par une source centrale mais c'est le résultat de la consultation de chacun des tableaux d'acheminement utilisés pendant le voyage. Chaque ordinateur définit seulement le prochain bond du voyage et se fie à cet ordinateur pour envoyer le paquet IP le long du chemin.

5.12 Gestion des chemins

La maintenance correcte des tableaux d'acheminement sur tous les ordinateurs dans un grand internet est une tâche difficile ; la configuration du réseau est constamment modifiée par les gestionnaires de réseau pour satisfaire des besoins

changeants. Des fautes dans les tableaux d'acheminement peuvent bloquer la communication de façons qui sont très difficiles à diagnostiquer.

Conserver une simple configuration de réseau est très loin de faire un internet fiable. Par exemple, la méthode la plus directe pour allouer des réseaux IP à Ethernet est d'allouer un seul numéro de réseau IP à chaque Ethernet.

On peut aussi obtenir de l'aide de certains protocoles et applications réseau. Le protocole de message de contrôle de l'Internet (ICMP, *Internet Control Message Protocol*) peut faire rapport de certains problèmes d'acheminement. Pour de petits réseaux, le tableau d'acheminement est rempli à la main sur chaque ordinateur par l'administrateur de réseau. Pour de plus grands réseaux, l'administrateur automatise cette opération manuelle avec un protocole d'acheminement pour répartir les routes sur tout un réseau.

Lorsque un ordinateur est déplacé d'un réseau IP à un autre, son adresse IP doit changer. Lorsque un ordinateur est retiré d'un réseau IP, son ancienne adresse devient invalide. Ces changements exigent de fréquentes mises à jour du fichier "hôtes". Ce fichier plat peut devenir difficile à entretenir même pour des réseaux de taille moyenne. Le système des noms de domaines aide à résoudre ces problèmes.

6. Protocole de datagramme d'utilisateur (UDP)

UDP est un des deux principaux protocoles qui réside par dessus IP. Il offre son service aux applications réseau de l'utilisateur. Des exemple d'applications réseau qui utilisent UDP sont le système de fichier réseau (NFS, *Network File System*) et le protocole simple de gestion de réseau (SNMP, *Simple Network Management Protocol*). Le service est un petit peu plus qu'une interface à IP.

UDP est un service de livraison de datagrammes sans connexion qui ne garantit pas la livraison. UDP ne conserve pas la connexion de bout en bout avec le module UDP distant ; il pousse simplement le datagramme hors du réseau et accepte les datagrammes entrant du réseau.

UDP ajoute deux valeurs à ce qui est fourni par IP. L'une est le multiplexage des informations entre les applications sur la base du numéro d'accès. L'autre est une somme de contrôle pour vérifier l'intégrité des données.

6.1 Accès

Comment un client sur un ordinateur atteint il le serveur sur un autre ?

Le chemin de communication entre une application et UDP se fait par des accès UDP. Ces accès sont numérotés, en commençant à zéro. Une application qui offre le service (le serveur) attend la venue des messages sur un accès spécifique dédié à ce service. Le serveur attend patiemment qu'un client quelconque demande le service.

Par exemple, le serveur SNMP, appelé un agent SNMP, attend toujours sur l'accès 161. Il ne peut y avoir qu'un seul agent SNMP par ordinateur parce qu'il n'y a qu'un seul accès UDP de numéro 161. Ce numéro d'accès est bien connu ; c'est un numéro fixé, un des numéros alloués de l'internet. Si un client SNMP veut le service, il envoie sa demande au numéro d'accès 161 de UDP sur l'ordinateur de destination.

Lorsque une application envoie des données à travers UDP, elles arrivent à l'extrémité distante comme une seule unité. Par exemple, si une application fait cinq écritures à l'accès UDP, l'application de l'extrémité distante va faire cinq lectures sur l'accès UDP. La taille de chaque écriture correspond aussi à la taille de chaque lecture.

UDP préserve la frontière de message définie par l'application. Il ne fusionne jamais deux messages d'application ensemble, ni ne divise un seul message d'application en plusieurs parties.

6.2 Somme de contrôle

Un paquet IP entrant avec un champ d'en-tête IP Type qui indique "UDP" est passé au module UDP par IP. Lorsque le module UDP reçoit le datagramme UDP de IP, il examine la somme de contrôle UDP. Si la somme de contrôle est zéro, cela signifie qu'il n'a pas été calculé de somme de contrôle par l'envoyeur et qu'elle peut être ignorée. Donc, le module UDP de l'ordinateur d'envoi peut ou non générer des sommes de contrôle. Si Ethernet est le seul réseau entre les deux modules UDP qui communiquent, on peut n'avoir pas besoin de faire de sommes de contrôle. Il est cependant recommandé de toujours activer la génération de sommes de contrôle parce que, à un moment quelconque à l'avenir, un changement du tableau d'acheminement peut envoyer les données à travers un support moins fiable.

Si la somme de contrôle est valide (ou zéro), le numéro d'accès de destination est examiné et si une application est liée à cet accès, un message d'application est mis en file d'attente pour que l'application le lise. Autrement, le datagramme UDP est éliminé. Si les datagrammes UDP entrants arrivent plus vite que ce que l'application peut lire et si la file d'attente a atteint sa valeur maximum, les datagrammes UDP sont éliminés par UDP. UDP va continuer d'éliminer les datagrammes UDP jusqu'à ce qu'il y ait de l'espace dans la file d'attente.

7. Protocole de contrôle de transmission (TCP)

TCP fournit un service différent de celui d'UDP. TCP offre un flux d'octets orienté connexion, au lieu d'un service de livraison de datagrammes sans connexion. TCP garantit la livraison, alors que UDP ne la garantit pas.

TCP est utilisé par les applications qui exigent la garantie de livraison et ne veulent pas être ennuyées avec des fins de temporisation et des retransmissions. Les deux applications réseau les plus typiques qui utilisent TCP sont le protocole de transfert de fichier (FTP, *File Transfer Protocol*) et TELNET. Les autres applications réseau populaires de TCP incluent le système X-Window, le protocole de copie à distance (RCP, *remote copy protocol*), et les commandes r-series. Les grandes capacités de TCP ne sont pas gratuites : il exige plus de CPU et de bande passante du réseau. Les entrailles du module TCP sont bien plus compliquées que celle d'un module UDP.

Similaires à UDP, les applications réseau connectent à des accès TCP. Des numéros d'accès bien définis sont dédiés à des applications spécifiques. Par exemple, le serveur TELNET utilise le numéro d'accès 23. Le client TELNET peut trouver le serveur simplement en se connectant à l'accès 23 de TCP sur l'ordinateur spécifié.

Lorsque l'application commence à utiliser TCP pour la première fois, le module TCP sur l'ordinateur du client et le module TCP sur l'ordinateur du serveur commencent à communiquer ensemble. Ceux deux modules de point d'extrémité TCP contiennent des informations d'état qui définissent un circuit virtuel. Ce circuit virtuel consomme des ressources dans les deux points d'extrémité TCP. Le circuit virtuel est bidirectionnel ; les données peuvent aller dans les deux directions simultanément. L'application écrit les données à l'accès TCP, les données traversent le réseau et sont lues par l'application à l'extrémité distante.

TCP met en paquets le flux d'octet à volonté ; il ne conserve pas les frontières entre les écritures. Par exemple, si une application fait cinq écritures à l'accès TCP, l'application à l'extrémité distante peut faire dix lectures pour obtenir toutes les données. Ou elle peut obtenir toutes les données en une seule lecture. Il n'y a pas de corrélation entre le nombre et la taille des écritures à une extrémité et le nombre et la taille des lectures à l'autre extrémité.

TCP est un protocole de fenêtre glissante avec des fins de temporisation et des retransmissions. Les données sortantes doivent être acquittées par le TCP de l'extrémité distante. Les accusés de réception peuvent être portés par les données. Les deux extrémités réceptrices peuvent contrôler le flux de l'extrémité distante, empêchant ainsi un débordement de mémoire tampon.

Comme avec tous les protocoles à fenêtre glissante, le protocole a une taille de fenêtre. La taille de fenêtre détermine la quantité de données qui peut être transmise avant d'exiger un accusé de réception. Pour TCP, cette quantité n'est pas un nombre de segments TCP mais un nombre d'octets.

8. Applications réseau

Pourquoi TCP et UDP existent ils tous deux, au lieu d'avoir simplement l'un ou l'autre ?

Ils fournissent des services différents. La plupart des applications sont mises en œuvre pour utiliser seulement l'un ou l'autre. Le programmeur va choisir le protocole qui satisfait au mieux les besoins. Si on a besoin d'un service fiable de livraison de flux, TCP pourrait être meilleur. Si on a besoin d'un service de datagrammes, UDP pourrait être le mieux. Si on a besoin d'efficacité sur des circuits à longue portée, TCP pourrait être meilleur. Si on a besoin d'efficacité sur des réseaux rapides avec faible latence, UDP pourrait être meilleur. Si les besoins ne rentrent pas parfaitement dans ces catégories, le "meilleur" choix n'est pas évident. Cependant, les applications peuvent s'appuyer sur les déficiences pour faire leur choix. Par exemple, si on choisit UDP et qu'on a besoin de fiabilité, l'application doit alors fournir de la fiabilité. Si on choisit TCP et qu'on a besoin d'un service centré sur l'enregistrement, l'application doit alors insérer des marqueurs dans le flux d'octets pour délimiter les enregistrements.

Quelles applications réseau sont disponibles ?

Il y en a bien trop pour en faire la liste. Leur nombre augmente continuellement. Certaines des applications existent depuis le début de la technologie internet : TELNET et FTP. D'autres sont relativement nouvelles : X-Windows et SNMP. Ce qui suit est une brève description des applications mentionnées dans ce guide.

8.1 TELNET

TELNET fournit une capacité de connexion à distance sur TCP. Son fonctionnement et son apparence sont similaires à la frappe des touches sur un commutateur téléphonique. Sur la ligne de commandes; l'usager tape "telnet delta" et reçoit une invite de connexion de la part de l'ordinateur appelé "delta".

TELNET fonctionne bien ; c'est une vieille application qui a une interopérabilité largement répandue. Les mises en œuvre de TELNET fonctionnent habituellement entre différents systèmes d'exploitation. Par exemple, un client TELNET peut être sur un VAX/VMS et le serveur sur un système UNIX V.

8.2 FTP

Le protocole de transfert de fichiers (FTP, *File Transfer Protocol*) aussi ancien que TELNET, utilise aussi TCP et a une interopérabilité largement répandue. Son fonctionnement et son apparence sont comme si un utilisait TELNET sur l'ordinateur distant. Mais au lieu de taper les commandes usuelles, on devra faire avec une courte liste de commandes pour des listes de répertoires et des choses de cette sorte. Les commandes FTP permettent de copier des fichiers entre des ordinateurs.

8.3 rsh

Coquille distante (rsh, *Remote Shell* ou remsh) fait partie d'une famille complète de commandes à distance de style UNIX. La commende UNIX copy, cp, devient rcp. La commande UNIX "qui est connecté", who, devient rwho. La liste continue et porte le nom collectif de "série de commandes 'r'" ou de commandes "r*" (r étoile).

Les commandes r* fonctionnent principalement entre des systèmes UNIX et elles sont conçues pour des interactions entre des hôtes de confiance. La sécurité est assez peu prise en considération, mais elles fournissent un environnement pratique à l'utilisateur.

Pour exécuter la commande "cc file.c" sur un ordinateur distant appelé delta, on tape "rsh delta cc file.c". Pour copier le fichier "file.c" sur delta, on tape "rcp file.c delta:". Pour se connecter à delta, on tape "rlogin delta", et si on administre les ordinateurs d'une certain façon, on ne sera pas confronté à une invite de mot de passe.

8.4 NFS

Le système de fichiers réseau (NFS, *Network File System*) d'abord développé par Sun Microsystems Inc, utilise UDP et est excellent pour monter des fichiers système UNIX sur plusieurs ordinateurs. Une station de travail sans disque dur peut accéder au disque dur de son serveur comme si le disque était en local sur la station. Une seule copie d'une base de données sur un grand système "alpha" peut aussi être utilisée par le système "beta" si le système de fichiers de la base de données est NFS monté sur "beta".

NFS ajoute une charge significative au réseau et a peu d'utilité sur les liaisons lentes, mais les bénéfices sont élevés. Le client NFS est mis en œuvre dans le noyau, ce qui permet à toutes les applications et commandes d'utiliser le disque monté avec NFS comme si c'était un disque local.

8.5 SNMP

Le protocole simple de gestion de réseau (SNMP, *Simple Network Management Protocol*) utilise UDP et est conçu pour être utilisé par les stations centrales de gestion de réseau. C'est un fait bien connu qu'avec suffisamment de données, un gestionnaire de réseau peut détecter et diagnostiquer les problèmes du réseau. La station centrale utilise SNMP pour collecter ces données des autres ordinateurs du réseau. SNMP définit le format des données ; il appartient à la station centrale ou au gestionnaire de réseau de les interpréter.

8.6 X-Window

Le système X Window utilise le protocole X Window sur TCP pour ouvrir des fenêtres d'affichage en format binaire sur une station de travail. X Window est beaucoup plus qu'un utilitaire pour des fenêtres de dessin ; c'est toute une philosophie de conception d'une interface d'utilisateur.

9. Autres informations

Beaucoup d'informations sur la technologie internet n'ont pas été incluses dans ce guide. Cette section fait la liste des informations qui sont considérées comme le niveau de détail suivant pour le lecteur qui souhaite en savoir plus.

- commandes d'administration : arp, route, et netstat
- ARP : entrée permanente, entrée publiée, entrée périmée, usurpation d'identité
- tableau d'acheminement IP, entrée d'hôte, passerelle par défaut, sous-réseaux
- IP : compteur de durée de vie, fragmentation, ICMP
- RIP, boucles d'acheminement
- Système des noms de domaine

10. Références

[1] Comer, D., "Internetworking with TCP/IP Principles, Protocols, and Architecture", Prentice Hall, Englewood Cliffs, New Jersey, U.S.A., 1988.

[2] Feinler, E., et al, "DDN Protocol Handbook", Volume 2 et 3, DDN Network Information Center, SRI International, 333 Ravenswood Avenue, Room EJ291, Menlow Park, California, U.S.A., 1985.

[3] Spider Systems, Ltd., "Packets and Protocols", Spider Systems Ltd., Stanwell Street, Edinburgh, U.K. EH6 5NG, 1990.

11. Relations aux autres RFC

Cette RFC est un guide qui ne met à jour ni ne rend obsolète aucune autre RFC.

12. Considérations pour la sécurité

La suite de protocoles TCP/IP pose des problèmes pour la sécurité. Pour certains, ces considérations sont des problèmes sérieux, pour d'autres elles ne le sont pas ; cela dépend des exigences de l'utilisateur.

Le présent guide ne discute pas de ces problèmes, mais si vous voulez en savoir plus vous devriez commencer par la question de l'usurpation d'ARP, puis utiliser la section de "Considérations pour la sécurité" de la RFC1122 pour conduire vos investigations.

13. Adresse des auteurs

Theodore John Socolofsky
Spider Systems Limited
Spider Park
Stanwell Street
Edinburgh EH6 5NG
United Kingdom
téléphone : + 031-554-9424
fax : + 031-554-0649
mél : TEDS@SPIDER.CO.UK

Claudia Jeanne Kale
12 Gosford Place
Edinburgh EH6 4BJ
United Kingdom
téléphone : + 031-554-7432
mél : CLAUDIAK@SPIDER.CO.UK