3

Aperçu général des protocoles TCP/IP

Points clés du chapitre

- La différence entre un réseau général et un réseau IP ; la différence entre un réseau IP quelconque et l'internet (le réseau internet mondial).
- L'architecture standard des protocoles TCP/IP, les RFC associés et l'architecture hybride TCP/IP-OSI.
- Les relations entre les différentes couches et leurs processus respectifs, tant au niveau des hôtes que des routeurs.
- Les modalités de sécurité des protocoles TCP/IP.
- Le protocole IP et les problèmes de sécurité associés.
- Le protocole TCP et les problèmes de sécurité associés.
- Le protocole UDP et les problèmes de sécurité associés.
- Le protocole ICMP et les problèmes de sécurité associés.

Cet ouvrage s'adresse à un public qui connaît déjà les notions de base des réseaux d'ordinateurs, mais les violations de sécurité impliquent si souvent l'internet et les réseaux d'entreprises fondés sur TCP/IP que nous avons jugé bon de décrire dans ce chapitre les protocoles les plus importants et les principes majeurs.

Outre la présentation de TCP/IP, ce chapitre recense également les problèmes de sécurité soulevés par ces différents protocoles, information servant de base au contenu des deux chapitres suivants.

3.1 Réseaux généraux et réseaux IP

Au chapitre 2, nous nous sommes intéressés à divers réseaux. Ici, nous nous concentrons sur les réseaux IP, qui fonctionnent sous les protocoles TCP/IP et qui sont formés par l'interconnexion de divers réseaux au moyen de routeurs.

La figure 3.1 présente les différents éléments d'un réseau IP constitué de l'assemblage de trois réseaux quelconques ; un client mobile connecté en tant qu'hôte au réseau 1 se connecte au serveur B sur le réseau 3 en passant par le réseau 2.

Le réseau IP le plus connu est bien sûr l'internet mondial (appelé communément **l'internet**), constitué de plusieurs centaines de millions d'ordinateurs et de dizaines de milliers de réseaux. On appelle **hôtes** tous les ordinateurs connectés à l'internet, des serveurs les plus puissants aux simples ordinateurs de bureau et assistants personnels.

L'internet et les **intranets** (qui sont des réseaux IP privés d'entreprise) ont tous recours aux protocoles TCP/IP. Étant donné le nombre d'attaques perpétrées depuis l'internet, la compréhension de ces protocoles s'avère cruciale.

3.2 Protocoles TCP/IP

3.2.1 Historique

Entre la fin des années 1960 et le début des années 1970, l'Agence fédérale américaine DARPA (*Defense Advanced Research Projects Agency*) a financé la création du premier réseau étendu à commutation de paquets : **ARPANET**. Ce réseau, réparti sur tout le pays, reliait les principaux centres de recherche collaborant avec le ministère de la Défense américain.

Les années 1970 ont vu l'émergence de nombreux autres réseaux à commutation de paquets, toujours au service de la communauté scientifique, tels que CSNET (entre informaticiens), BITNET (entre professeurs d'économie et de science du comportement) et une myriade de petits réseaux de recherche situés dans d'autres pays[1]. Un certain Vinton Cerf a formulé un jour l'idée de les relier entre eux afin de constituer un vaste réseau mondial. La DARPA s'en est chargé en se fondant sur l'architecture d'ARPANET.

Pour des raisons expliquées plus loin, les standards sur lesquels reposait ce réseau internet naissant ont été rassemblés sous l'appellation suite de protocoles TCP/IP. Mis au point par l'IETF (*Internet Engineering Task Force*), ces protocoles constituaient la base du fonctionnement d'ARPANET.

1. Des réseaux à commutation de paquets destinés aux entreprises voient également le jour : par exemple, en France, Transpac (aujourd'hui réseau de France Télécom), qui n'est pas fondé sur TCP/IP, mais sur une norme de l'UIT, à savoir la norme X.25.

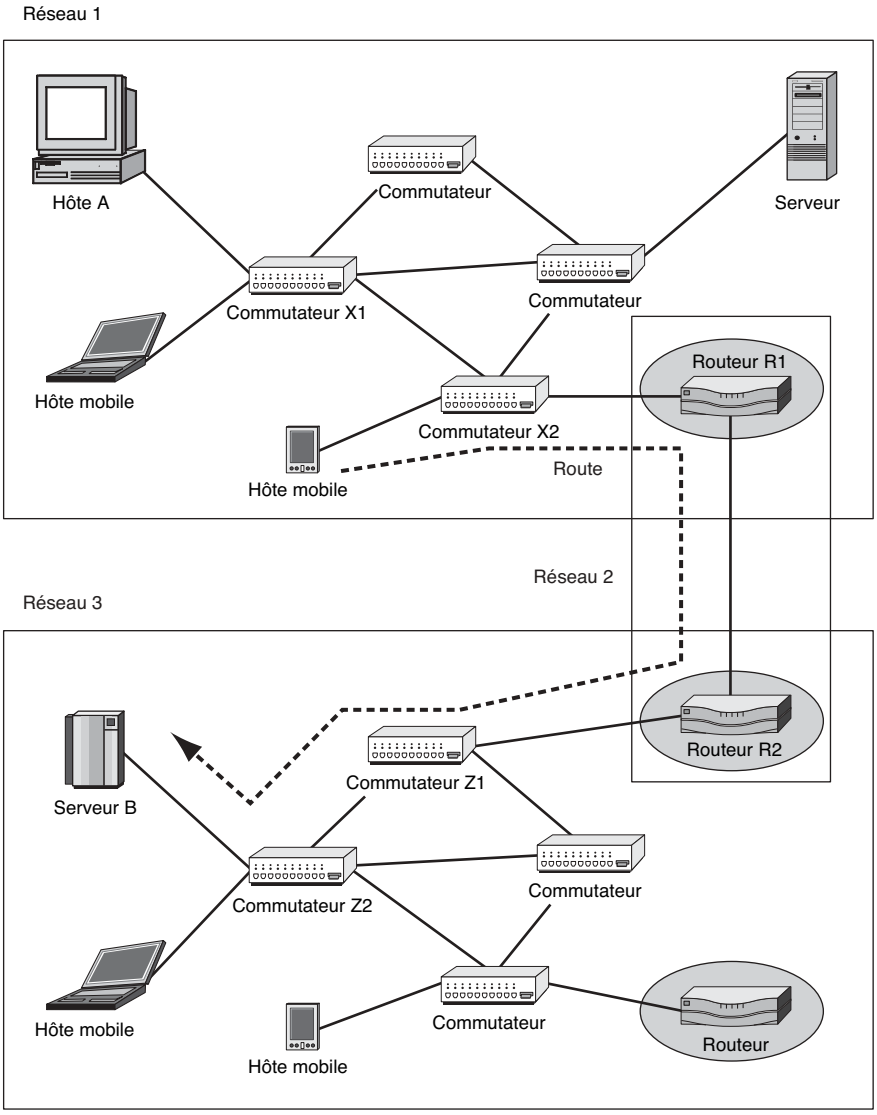


Figure 3.1 • Un réseau IP.

Les documents décrivant les divers standards produits par l'IETF sont connus sous le nom de **RFC** (*Request For Comments*). Par exemple, le protocole IP est spécifié dans le RFC 791. Les RFC ne spécifient pas uniquement des protocoles. Pour faciliter la consultation, l'IETF publie régulièrement un RFC recensant tous les protocoles de l'internet.

Encadré 3.1 : Mise en perspective de TCP/IP

Historique
Agence fédérale DARPA et réseau ARPANET
L'internet assure l'interconnexion des différents réseaux.
Groupe de travail IETF
La plupart des publications de l'IETF sont des RFC.
Protocoles de l'internet : liste de RFC officiellement reconnus comme protocoles standard

Architecture TCP/IP-OSI (voir tableau 3.1)
Associe les protocoles TCP/IP au niveau des couches 3-5 avec les protocoles OSI au niveau des couches 1-2.

Protocoles de divers types de réseaux (voir figure 3.2)
Ligne physique
Liaison de données

Trames et paquets (voir figure 3.3)
Une trame est un message empruntant une liaison de données.
Un paquet est un message circulant dans un internet.
Les paquets sont véhiculés par des trames (on dit qu'ils sont encapsulés).
Un seul paquet est transmis entre l'hôte source et l'hôte de destination.
Le paquet est encapsulé dans une trame différente à l'entrée de chaque nouveau réseau.

Couches Internet et Transport (voir figure 3.4)
Fonctions
- IP est un protocole de couche Internet dit de « bond-par-bond ».
- La couche Transport offre un service de bout-en-bout impliquant uniquement les deux hôtes interlocuteurs.

Protocole IP
- Le protocole IP est non fiable, c'est-à-dire qu'il ne corrige pas les erreurs.
- Cela est un atout : le travail des routeurs situés sur le chemin (la route) entre la source et la destination s'en trouve réduit.
- Le protocole TCP peut corriger les erreurs non détectées par IP.

Protocole TCP
- Service fiable et orienté connexion de couche Transport
- Corrige les erreurs que le protocole IP ne parvient pas à détecter.

Protocole UDP
Service non fiable et sans connexion de couche Transport
Protocole léger, utilisé lorsque la détection d'erreurs n'est pas importante

Couche Applications (voir figure 3.5)
Dirige les communications entre différentes applications, souvent d'origines différentes.

Transfert de documents et standards de format de documents
HTTP/HTML pour le Web
SMTP/RFC 822 (ou RFC 2822) pour le courrier électronique
Il existe de nombreux protocoles applicatifs en raison du grand nombre d'applications disponibles sur le marché.

3.2.2 Architecture hybride TCP/IP-OSI

Les protocoles sont le plus souvent développés dans un cadre commun, connu sous le nom d'«architecture de protocoles». Le tableau 3.1 montre qu'une architecture de protocoles est une pile (ou suite) de protocoles relatifs à un ensemble de couches fonctionnelles fournissant chacune des services spécifiques. Les services d'une couche sont offerts à la couche directement supérieure. Ils s'appuient eux-mêmes sur les services offerts par la couche immédiatement inférieure (à l'exception de la couche Physique, la plus basse).

Tableau 3.1 : Architecture des protocoles TCP/IP et OSI.

TCP/IP	OSI	Architecture hybride[a] TCP/IP-OSI
Applications	Applications	Applications
	Présentation	
	Session	
Transport	Transport	Transport
Internet	Réseau	Internet
Protocoles propres au réseau sous-jacent	Liaison de données	Liaison de données
	Physique	Physique

a. L'internet et la plupart des réseaux intranets d'entreprise ont recours à une architecture hybride TCP/IP-OSI.

Le tableau 3.1 compare l'architecture de protocoles à quatre couches de TCP/IP et l'architecture à sept couches du modèle OSI[2]. Comme les protocoles TCP/IP ne

2. Ce modèle de référence et de base pour l'interconnexion des systèmes ouverts est normalisé par l'ISO (*International Standardization Organization*, Organisation internationale de normalisation).

concernent pas les infrastructures de réseaux de type LAN ou autres, tels que les réseaux Ethernet ou Wi-Fi, on a communément recours aux couches basses de l'architecture OSI pour les spécifier.

Par conséquent, l'internet et la plupart des réseaux d'entreprise ont une architecture hybride de type TCP/IP-OSI, qui utilise des protocoles OSI au niveau des couches basses et des protocoles TCP/IP au niveau des couches supérieures[3] : Internet, Transport et Applications.

3.2.3 Protocoles des réseaux

La figure 3.2 présente divers types de liens associant des protocoles des trois couches basses des architectures réseaux : la couche Physique, la couche Liaison de données et la couche Internet. Alors que les deux premières assurent la communication au sein de l'infrastructure du réseau, la troisième est responsable des communications sur l'internet.

Couche Physique. Dans un réseau, les protocoles de couche Physique commandent et gèrent les liens physiques qui se trouvent entre des hôtes et des commutateurs (ou routeurs), et entre des commutateurs (ou routeurs). À la figure 3.2, au niveau du réseau X, une couche Physique s'inscrit entre l'hôte A et le commutateur X1, entre les commutateurs X1 et X2, et entre le commutateur X2 et le routeur R1. Jusqu'au serveur B, on distingue quatre couches Physique supplémentaires. Les protocoles de couche Physique gèrent les connecteurs mécaniques et les échanges de signaux de type électriques, optiques ou radio sur les supports de transmission.

Couche Liaison de données. Dans un réseau, les liens logiques qui le traversent de proche en proche sont appelés «liaisons de données». Les protocoles de couche Liaison de données déterminent la manière dont les hôtes, les commutateurs et les routeurs se transmettent les messages, appelés **trames**.

Dans le réseau X de la figure 3.2, une liaison de données intervient entre l'hôte A et le routeur R1. Le réseau Y compte, quant à lui, une liaison de données entre les routeurs R1 et R2. Enfin, dans le réseau Z, une liaison de données relie le routeur R2 au serveur B.

Couche Internet. Pour connecter plusieurs réseaux entre eux (trois dans la configuration présentée à la figure 3.2), l'IETF a défini un nouveau type de lien, appelé **route** ou **chemin**. Une route est un lien virtuel de bout-en-bout entre un hôte source et un hôte (ou serveur) de destination au travers d'un ou de plusieurs réseaux. À la figure 3.2, une route relie l'hôte A au serveur B. La couche Internet définit le mode d'acheminement des messages entre les routeurs. Ces messages sont appelés **paquets** (ou **datagrammes**).

3. L'IETF a toutefois développé des protocoles de couche basse, tel que PPP, qui agit au niveau de la couche Liaison de données (couche 2). Ceux-ci s'inscrivent tout naturellement au sein des couches basses de l'architecture OSI.

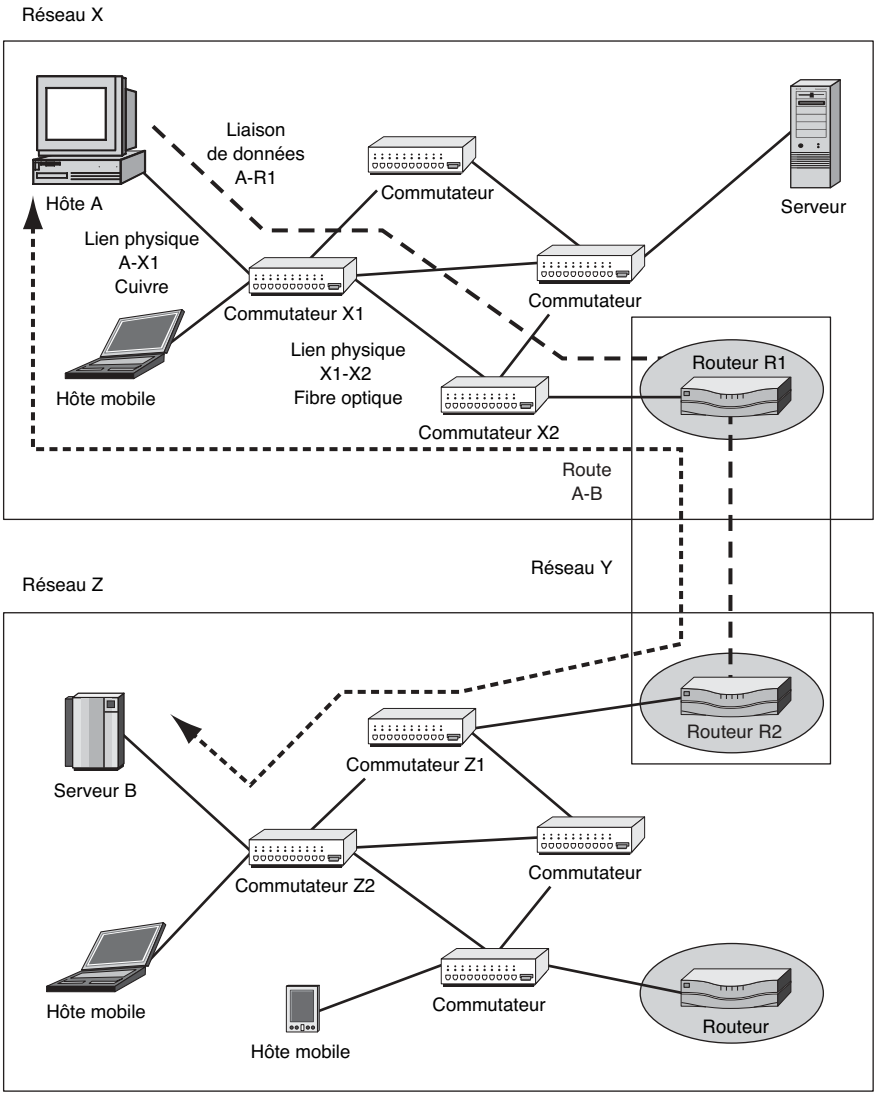


Figure 3.2 • Lien physique, liaison de données et route.

3.2.4 Trames et paquets

Les messages envoyés sur une liaison de données (logique) sont appelés «trames» et les messages envoyés dans un réseau IP sont appelés «paquets» ou datagrammes.

Paquets. Les paquets sont des messages de la couche Internet envoyés par un hôte source et reçus par un hôte de destination. Le tableau 3.2 illustre la structure type d'un paquet ou datagramme IP représenté en groupe de mots de 32 bits (les adresses IP font 32 bits). Le champ d'adresse IP source contient l'adresse IP de l'expéditeur ; le

champ d'adresse IP de destination est dédié à l'adresse IP du destinataire, utilisée par les routeurs pour acheminer le paquet jusqu'à sa destination finale.

Tableau 3.2 : Structure d'un paquet ou datagramme IP.

<table>
<tr><td colspan="4">Bit 0 Bit 31</td></tr>
<tr><td>Version (4 bits)</td><td>Longueur d'en-tête (4 bits) en mots de 32 bits</td><td>Type de service (8 bits)</td><td>Longueur totale (16 bits)
Longueur du paquet entier en octets</td></tr>
<tr><td colspan="3">Identification (16 bits)
Identifie les fragments d'un même paquet (valeur propre à chaque paquet)</td><td>Bits indicateurs (3 bits)
Décalage de fragment (13 bits) Indique le décalage du premier octet du fragment par rapport au paquet complet</td></tr>
<tr><td>Durée de vie (8 bits)</td><td colspan="2">Protocole (8 bits)
1 = ICMP, 6 = TCP, 17 = UDP</td><td>Somme de contrôle d'en-tête (16 bits)</td></tr>
<tr><td colspan="4">Adresse IP source (32 bits)</td></tr>
<tr><td colspan="4">Adresse IP de destination (32 bits)</td></tr>
<tr><td colspan="3">Options éventuelles</td><td>Bourrage</td></tr>
<tr><td colspan="4">Champ de données (douzaines, centaines ou milliers de bits)</td></tr>
</table>

Notes :

Les bits 0-3 renseignent sur le numéro de version.

Les bits 4-7 renseignent sur la longueur de l'en-tête.

Les bits 8-15 renseignent sur le type de service.

Les bits 16-31 renseignent sur la longueur totale.

Les bits 32-47 renseignent sur la valeur d'identification.

Trames. Les trames sont des messages circulant sur une liaison de données. Elles disposent, elles aussi, d'une adresse de destination permettant aux commutateurs (ou routeurs) de les envoyer à leur destinataire, hôte, commutateur ou routeur. Par exemple, au sein d'un réseau local de type Ethernet ou 802.11, ces adresses sont codées sur 48 bits. Elles sont appelées **adresses MAC** (*Media Access Control*).

Différence entre trames et paquets. La figure 3.3 illustre la différence entre les trames et les paquets.

- *Génération d'un paquet et transmission au sein d'une trame.* À la figure 3.3, un hôte génère un paquet à l'intention d'un serveur, qu'il place dans le champ de données d'une trame adaptée au réseau auquel il est connecté (réseau 1). Puis il envoie la trame au routeur A au travers d'une série de commutateurs (un seul est représenté).
- *Encapsulation.* L'encapsulation consiste à placer un message dans le champ de données d'un autre message. Il s'agit d'une procédure aussi courante que capitale.

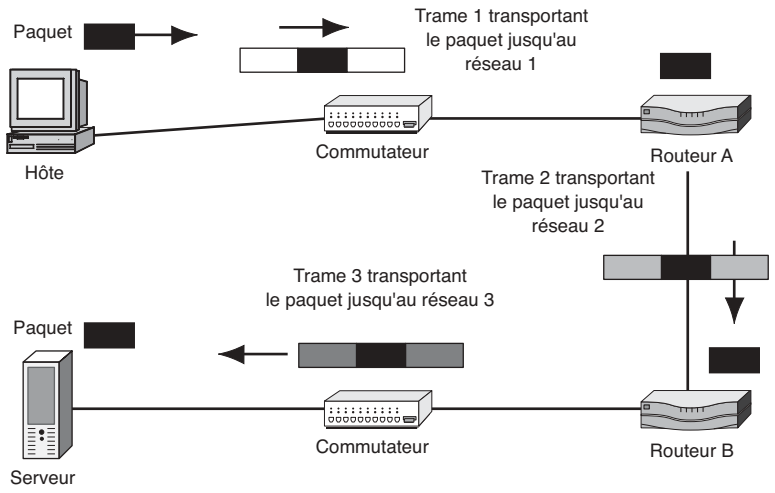


Figure 3.3 • Trames et paquets.

- *Au niveau du premier routeur : extraction et réencapsulation.* Le premier routeur (A) extrait le paquet de la trame 1 et se débarrasse de la trame en question. En fonction des informations contenues dans l'en-tête du paquet, il décide de ce qu'il doit en faire et l'envoie au second routeur en le plaçant dans une nouvelle trame (2), adaptée au réseau 2.
- *Au niveau du second routeur.* Le second routeur effectue la même opération : il extrait le paquet de la trame 2 et l'encapsule dans une troisième trame (3), adaptée au réseau 3.
- *De nombreuses trames pour un seul paquet.* En d'autres termes, le transfert d'un paquet au travers d'un réseau IP implique la génération d'une nouvelle trame à chaque changement de réseau.

3.2.5 Couches Internet et Transport

Les couches Internet et Transport œuvrent de concert pour le transfert des messages (voir figure 3.4).

IP et la couche Internet. La couche Internet a recours au **protocole IP** (***Internet Protocol***). Ce protocole détermine le devenir des paquets à chaque bond entre deux routeurs et entre les routeurs les plus proches des hôtes source et de destination sur un chemin donné. Un paquet traversant trois routeurs sur son chemin effectue ainsi quatre bonds.

IP est un protocole simple, qui ne corrige pas les erreurs pouvant être introduites au cours du transfert des paquets. Cela fait d'IP un **protocole non fiable**.

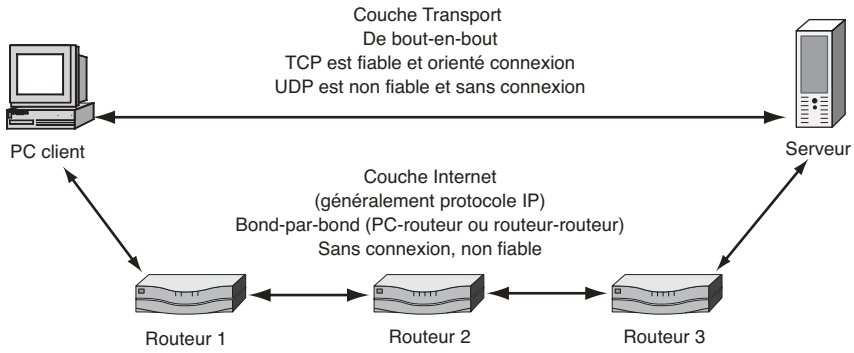


Figure 3.4 • Couches Internet et Transport.

Processus très intensif, la correction d'erreurs donnerait beaucoup de travail aux routeurs. L'absence de ce traitement permet ainsi d'utiliser des dispositifs plus simples, donc moins coûteux (il en est de même pour les commutateurs). Le protocole IP ne garantit même pas l'ordre d'arrivée des paquets et n'offre aucun moyen aux routeurs ou à l'hôte de destination de les remettre en ordre.

Protocole TCP (*Transmission Control Protocol*). Pour pallier les problèmes suscités par le manque de fiabilité du protocole IP, un **protocole fiable**, appelé TCP, a été défini au niveau de la couche Transport. Nous examinerons plus loin la correction d'erreurs opérée par TCP.

TCP ne corrige les erreurs qu'au niveau des hôtes, et non au cours du transfert des paquets. Cette correction de bout-en-bout se traduit, certes, par du travail supplémentaire pour les hôtes, mais la charge est nettement moindre que si la correction devait se réaliser à chaque bond entre les routeurs.

TCP et IP collaborent étroitement au transfert fiable et efficace des messages de leur source à leur destination.

UDP (*User Datagram Protocol*). Certaines applications, telles celles en temps réel (comme la voix ou la téléphonie sur IP), n'ont pas besoin d'un service de transfert fiable. En revanche, pour ces applications, le moindre retard dans la transmission des messages est à proscrire.

Les logiciels d'administration de réseau, qui vérifient constamment le statut des différents éléments du réseau, se satisfont également d'un service non fiable, qui permet de réduire le trafic réseau et le temps de traitement des paquets de contrôle (du fait de l'absence d'accusés de réception).

Pour ces applications ayant de préférence recours à un service non fiable, un second protocole de couche Transport, appelé UDP, a été défini par l'IETF.

3.2.6 Couche Applications

Les quatre couches basses d'un réseau assurent les relations entre les applications opérant sur les hôtes sources et les applications correspondantes sur les hôtes de destination.

La couche Applications repose sur des protocoles assurant la régulation des communications entre applications, notamment lorsque celles-ci proviennent de fabricants différents. Le standard HTTP (*HyperText Transfer Protocol*) permet par exemple au navigateur Internet Explorer de Microsoft d'un PC client d'effectuer des requêtes auprès d'un logiciel serveur SUN ONE.

Standards de format de documents. La plupart des standards applicatifs se présentent sous forme de paires, un membre de la paire détermine le format des fichiers en cours de transfert. Le langage HTML (*HyperText Markup Language*) définit ainsi le format des pages Web (voir figure 3.5). Dans le cas du courrier électronique, le format des messages textuels a été défini dans le RFC 822, remplacé depuis par le RFC 2822. D'autres applications reposent sur d'autres standards de format de documents.

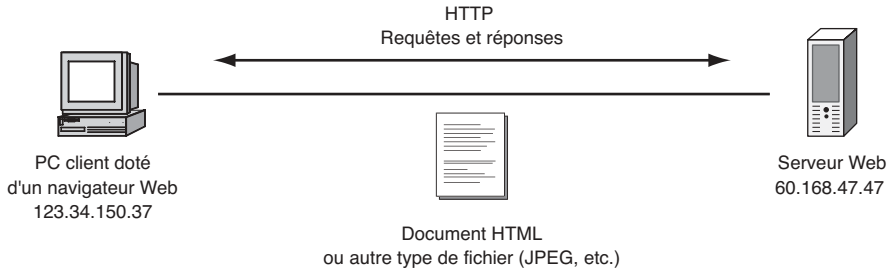


Figure 3.5 • HTML et HTTP.

Standards de transfert de documents. Si HTML définit le format des pages Web, ce langage ne spécifie pas la manière dont les hôtes clients les sollicitent auprès des serveurs, ni comment ces derniers accèdent aux requêtes de leurs clients. Cela est la tâche d'un autre type de standard, présentant une grande similarité avec les standard de format de documents. Dans notre exemple, il s'agit du protocole HTTP (*HyperText Transfer Protocol*). En ce qui concerne le courrier électronique, le protocole responsable du transfert des messages est SMTP (*Simple Mail Transfer Protocol*). Le protocole de transfert permettant la consultation du courrier électronique est le protocole POP (*Post Office Protocol*). Chaque application dispose de son propre standard de transfert de documents.

Protocoles applicatifs. Si la couche Internet est dominée par le protocole IP et la couche Transport par deux protocoles, TCP et UDP, la couche Applications a, quant à elle, recours à autant de protocoles qu'il existe d'applications. La grande majorité de la suite des protocoles TCP/IP sont donc des protocoles applicatifs.

3.3 Coopération intercouche

Bien qu'indépendants les uns des autres, les processus correspondant à chaque couche doivent collaborer tout au long du parcours des messages au travers du réseau, aussi bien au niveau des hôtes source et de destination qu'au niveau des routeurs.

3.3.1 Au niveau de l'hôte source

Au niveau de l'hôte source, les processus de couches adjacentes collaborent en transférant les messages d'une couche à l'autre (voir figure 3.6). Chaque couche génère un nouveau paquet contenant dans son champ de données le message fourni par la couche immédiatement inférieure.

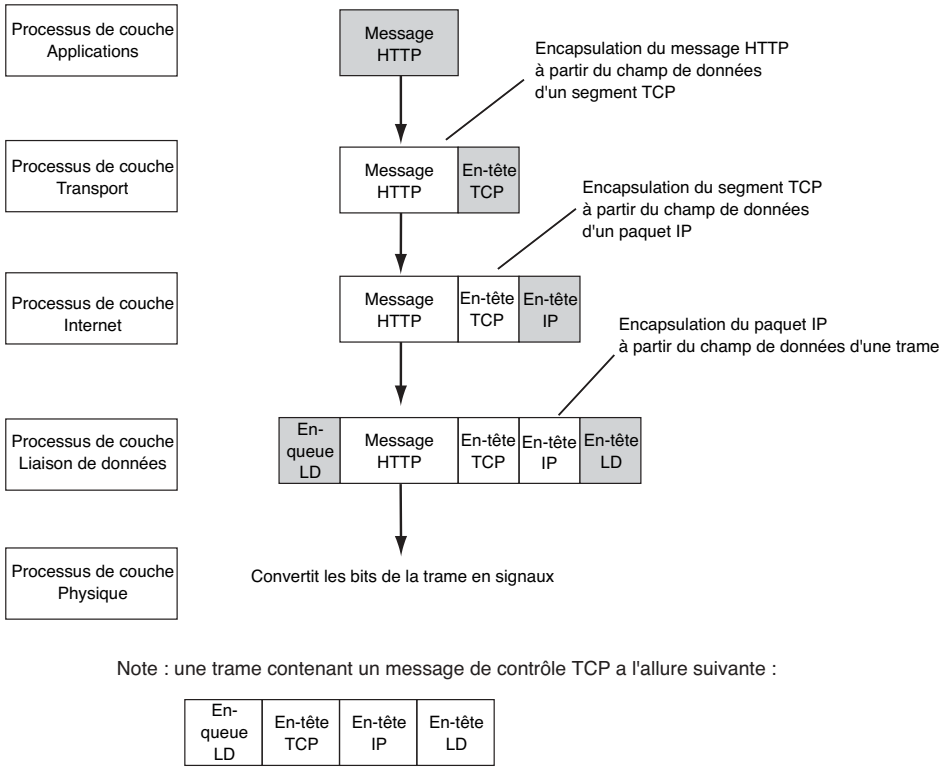


Figure 3.6 • Coopération intercouche par encapsulation de paquets au niveau de l'hôte source.

Encapsulation. Le message HTTP de la figure 3.6 est tout d'abord encapsulé dans un **segment**[4] TCP. Le processus de couche Transport utilise le message HTTP comme le champ de données d'un segment et lui ajoute un en-tête TCP. Le segment est ensuite encapsulé dans un paquet IP (par l'ajout d'un en-tête IP), puis le paquet IP est encapsulé dans une trame de liaison de données, en général entre un en-tête et un en-queue de couche Liaison de données (LD). Certains protocoles n'ont pas recours aux en-queues.

Couche Physique. En transportant des bits plutôt que des messages, la couche Physique se distingue nettement des autres couches. Lorsque la trame passe du processus de couche Liaison de données au processus de couche Physique, les bits sont convertis en signaux et transmis au niveau suivant.

Trame. La trame livrée à la couche Physique (voir figure 3.6) se compose d'un en-tête LD, d'un en-tête IP, d'un en-tête TCP, du message HTTP et d'un en-queue LD. La couche Physique convertit les bits de la trame en signaux physiques, électriques, optiques ou radio.

Autres types de trames. La figure 3.6 illustre le transfert d'un message HTTP émanant de la couche Applications. Tous les messages ne partent pas de cette couche : par exemple, les processus TCP de deux hôtes interlocuteurs communiquent souvent directement entre eux, même en l'absence de tout message applicatif. Le message de contrôle TCP figurant au bas de la figure ne véhicule aucun message applicatif. Il contient uniquement des informations de contrôle au sein de l'en-tête TCP.

3.3.2 Au niveau de l'hôte de destination

Au niveau de l'hôte de destination, les opérations précédentes se répètent en sens inverse (voir figure 3.7). La couche Physique reçoit des signaux, les convertit en bits et les remet au processus de couche Liaison de données, et ainsi de suite. Chaque couche extrait le message avant de le transmettre à la couche supérieure.

3.3.3 Au niveau des routeurs

La figure 3.8 présente les opérations effectuées par les routeurs, et plus particulièrement par le routeur R1 de la figure 3.1.

Réception. Le routeur reçoit tout d'abord une trame en provenance du commutateur X2. Le processus de couche Liaison de données du port de réception (port 1) extrait le paquet IP contenu dans la trame et le remet au processus de couche Internet du routeur R1.

Transmission. Le processus de couche Internet de R1 décide d'envoyer le paquet au port 4. Il le remet donc au processus de couche Liaison de données de ce port, qui l'encapsule dans une nouvelle trame (trame PPP) et le transmet au routeur R2.

4. Le terme « segment » désigne officiellement un message TCP.

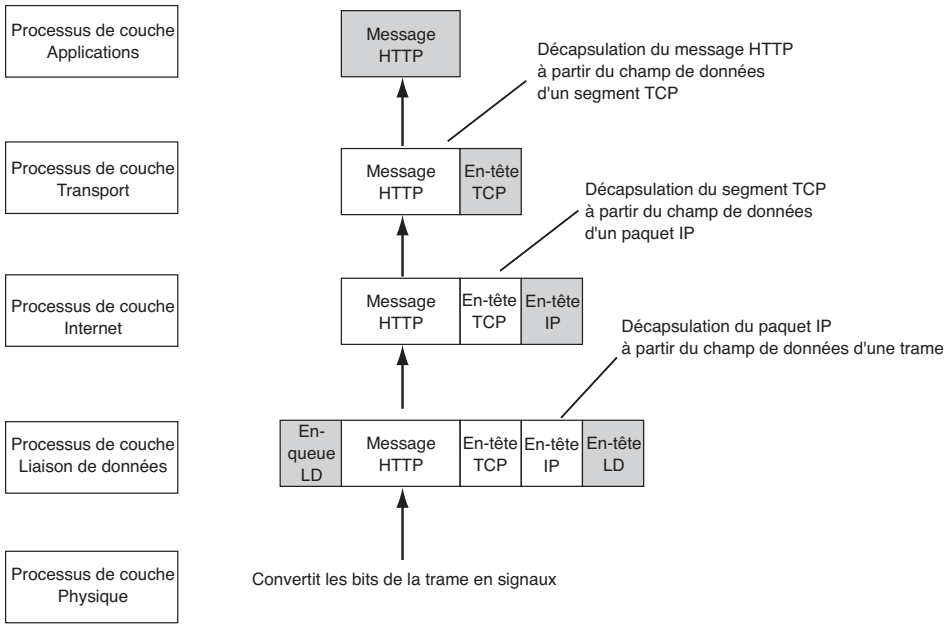
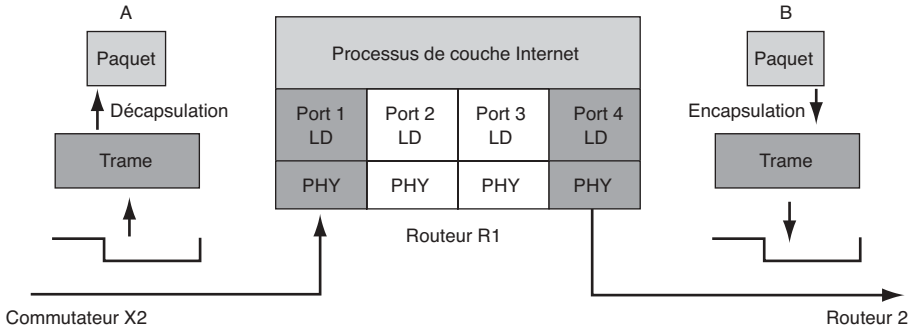


Figure 3.7 • Coopération intercouche par extraction (ou décapsulation) de paquets au niveau de l'hôte de destination.



Notes :

A. Le routeur R1 reçoit une trame en provenance du commutateur X2 sur le port 1.
Le processus du port 1 LD extrait le paquet.
Le processus du port 1 LD remet le paquet au processus de couche Internet.

B. Le processus de couche Internet envoie le paquet au port 4.
Le processus LD du port 4 encapsule le paquet dans une trame PPP.
Le processus LD remet la trame au port 4 PHY.

Figure 3.8 • Communication verticale au niveau d'un routeur.

3.3.4 TCP/IP et sécurité de site

La figure 3.9 présente la configuration type adoptée par la plupart des entreprises, c'est-à-dire le positionnement de pare-feux frontières à l'interface entre leur réseau et l'internet. Les pare-feux sont généralement placés à l'extrémité de la liaison de données reliant leurs locaux à leur fournisseur d'accès à internet. Il s'agit souvent d'une ligne point à point ayant recours au protocole PPP au niveau de la couche Liaison de données.

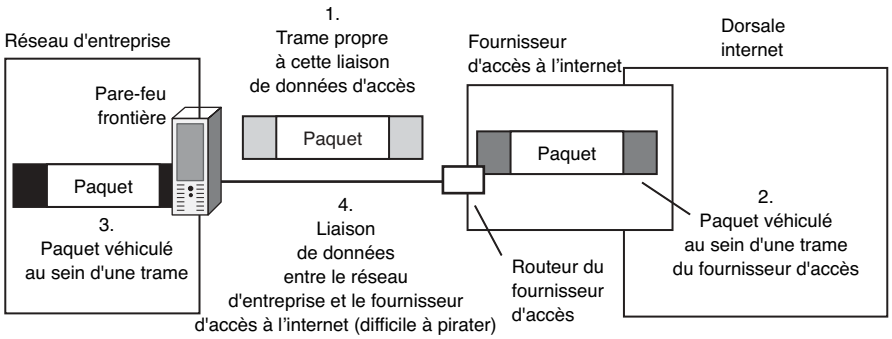


Figure 3.9 • Connexion d'une entreprise à son fournisseur d'accès à internet.

Ce type de connexion étant très difficile à pirater, la surveillance des pare-feux se concentre en général sur les paquets en provenance des couches Internet, Transport et Applications. Ils ignorent les en-tête et en-queue de couche Liaison de données. En simplifiant l'opération de filtrage, on réduit le temps de traitement et le coût des pare-feux.

Cependant, les liaisons de données et les connexions physiques à l'intérieur des réseaux d'entreprise sont vulnérables aux attaques des pirates (voir chapitre 2), si bien que des mesures de sécurité doivent également être prises en interne.

3.4 Protocole IP (Internet Protocol)

3.4.1 Propriétés générales

Lors de la conception du protocole IP, il était impossible de prévoir quels types de réseaux, au-delà du parc existant, l'utiliseraient un jour, de sorte que l'IETF a opté pour la simplicité, garante de la compatibilité. Comme l'a souvent répété Vinton Cerf, l'un des créateurs de l'internet : « IP avant tout » !

3.4.2 Service orienté connexion et service sans connexion

On distingue deux grands types de services réseau :

- Les conversations téléphoniques sont des sessions de communication structurées, qui partent par exemple du principe que les différents interlocuteurs sont en mesure de communiquer librement. Les conversations se concluent généralement par un accord mutuel entre les différents participants, et non par une décision unilatérale. Cette propriété est à la base de la notion de « service orienté connexion ».
- L'envoi d'une lettre par la poste n'implique, en revanche, aucune relation préalable entre l'expéditeur et le destinataire. Il est possible de poster un courrier à toute heure, sans se préoccuper de savoir si le destinataire est connecté à ce moment-là. On parle dans ce cas de « service sans connexion ».

3.4.3 IP est sans connexion

IP est sans doute l'archétype du service sans connexion sur l'internet. À la figure 3.10, le processus internet expéditeur transmet les paquets IP qui lui sont soumis au moment où il le souhaite, sans attendre l'établissement d'une connexion avec le processus destinataire.

3.4.4 IP est non fiable

Le protocole IP assure un service non fiable. À la figure 3.10, la réception du paquet IP ne génère pas d'accusé de réception. L'expéditeur n'a aucun moyen de savoir si son paquet est arrivé à bon port ou s'il doit le renvoyer. Cette absence de correction d'erreurs à chaque bond permet de réduire le prix des routeurs.

Encadré 3.2 : Synthèse du protocole IP

Propriétés générales

Service orienté connexion et service sans connexion
Les services orientés connexion se caractérisent par une ouverture et une clôture de session explicites (exemple : une conversation téléphonique).

Les services sans connexion se contentent d'envoyer des messages (exemple : le service postal).

IP est sans connexion.

IP est non fiable (vérifie la présence d'éventuelles erreurs mais ne les corrige pas).

Adresses IP hiérarchiques
Les adresses postales sont hiérarchiques (pays, commune, code postal, numéro et nom de la rue).

La plupart des centres de tri se contentent de vérifier le pays et la ville du destinataire.

Seuls les bureaux de poste et les facteurs s'intéressent au nom et au numéro de rue.

Les adresses IP de 32 bits sont hiérarchiques.

L'adresse réseau informe sur le réseau auquel appartient l'expéditeur.

L'adresse de sous-réseau informe sur le sous-réseau auquel appartient l'expéditeur à l'intérieur du réseau.

L'adresse hôte spécifie l'hôte expéditeur au sein du sous-réseau.

Les routeurs situés sur le chemin d'un paquet se contentent de consulter son adresse réseau et de sous-réseau, à l'exception du routeur chargé de remettre le paquet à son destinataire.

Toutes les adresses IP mesurent 32 bits, mais la taille relative de leurs différentes composantes peut varier.

Les masques de réseau renseignent sur la longueur de l'adresse réseau.

Les masques de sous-réseau renseignent sur la longueur (totale) de l'adresse réseau et de l'adresse de sous-réseau.

Adresses IP et sécurité

Usurpation d'adresse IP : envoi d'un message affichant une fausse adresse IP

Assure l'anonymat de l'expéditeur.

Peut exploiter les liens de confiance existant entre certains utilisateurs.

Attaque LAND : envoi d'un paquet à une victime affichant des adresses source et de destination ainsi que des numéros de port source et de destination identiques. En 1997, un grand nombre d'ordinateurs, de commutateurs, de routeurs et même d'imprimantes ont été mis en échec par des paquets de ce type.

Autres champs d'en-tête IP

Champ de protocole : indique la nature du contenu du champ de données IP.

Les pare-feux ont besoin de cette information pour savoir comment traiter le champ de données des paquets qu'ils reçoivent.

Champ de durée de vie

Chaque routeur réduit de 1 la valeur de durée de vie.

Le routeur qui, après soustraction, obtient une valeur de 0 élimine le paquet.

Ce même routeur envoie un message d'erreur à l'expéditeur.

Le paquet contenant ce message révèle l'adresse IP du routeur à l'attaquant.

Le logiciel Traceroute repose sur le principe de durée de vie pour identifier le chemin conduisant à un hôte donné.

Tracert est l'équivalent de Traceroute sous environnement Windows.

Champ de longueur d'en-tête et d'options

Les options présentent des risques.

Fragmentation

Les routeurs peuvent fragmenter les paquets (plus précisément, les champs de données des paquets) au cours de leur acheminement.

Chaque fragment a un numéro d'identification placé dans un champ spécifique.

Les valeurs de décalage des fragments permettent de les remettre dans le bon ordre.

Le bit de fragment suivant est nul dans le cas du dernier fragment.

Inspection des paquets suspects : en-tête TCP, etc., effectuée uniquement sur le premier paquet d'une série

Ne peut pas filtrer les paquets suivants (à partir de l'en-tête TCP, etc.).

Attaque Teardrop : paquet d'attaque défragmenté ne signifiant rien une fois les fragments assemblés

Certains pare-feux rejettent tous les paquets fragmentés (devenus rares à l'heure actuelle).

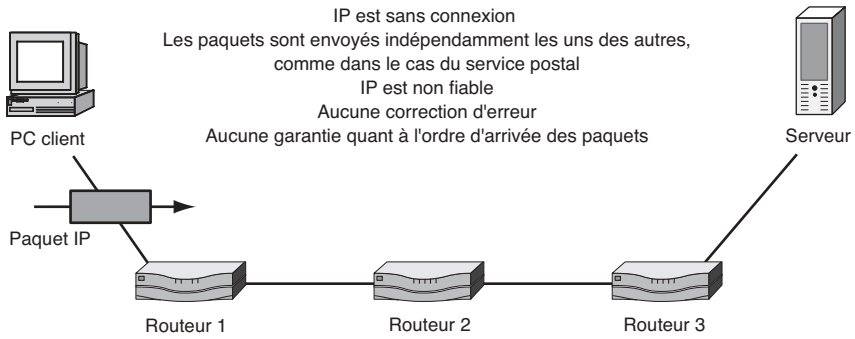


Figure 3.10 • Service IP sans connexion.

3.4.5 Adresses IP

Adresses postales hiérarchiques. Les adresses postales sont dites hiérarchiques dans le sens où leur contenu vient dans un certain ordre, de l'information la plus précise à la plus générale : numéro et nom de la rue, commune, code postal et pays.

Cette forme d'adressage simplifie le travail des centres de tri postal en leur permettant de classer le courrier par ville ou par pays. Une fois le pli arrivé au bureau de poste local, c'est le nom de la rue qui est pris en compte en tant qu'information d'adressage, le facteur s'intéressant lui au numéro de la rue en question pour trouver la bonne boîte aux lettres. Ce type d'organisation permet une forte réduction du coût du tri postal par rapport à un système d'adressage anarchique.

Adresses IP hiérarchiques. Les adresses IP suivent également une structure hiérarchique (voir figure 3.11).

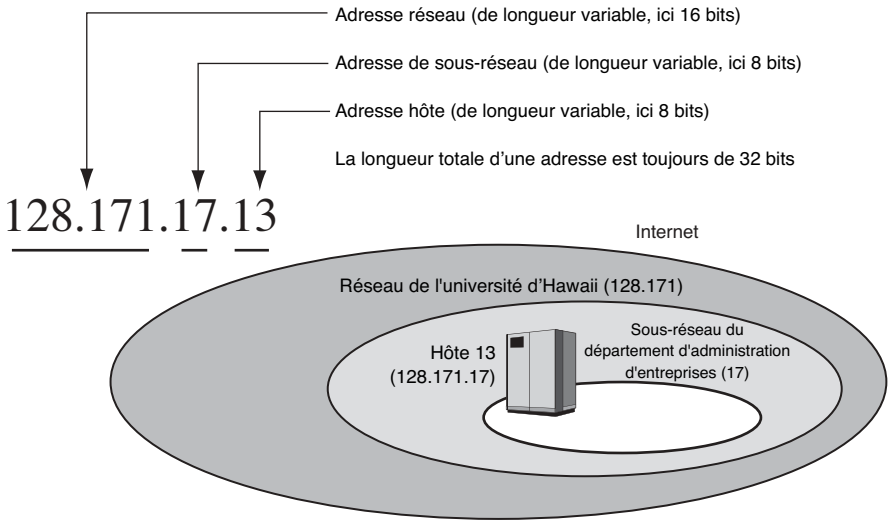


Figure 3.11 • Adresse IP hiérarchique.

- *Adresses réseau.* L'adresse IP 128.171.17.13 (voir figure 3.11) commence par 128.171, cette composante correspondant au réseau auquel est connecté l'expéditeur. Ces 16 bits indiquent que le message provient d'un hôte du réseau de l'université d'Hawaii. L'adresse IP de tous les hôtes connectés à ce réseau débute par 128.171.
- *Adresses de sous-réseau.* Le numéro 17 correspond au sous-réseau, en l'occurrence au département d'administration d'entreprises de l'université. L'adresse de tous les hôtes connectés à ce sous-réseau débute donc par 128.171.17.
- *Adresses hôte.* Enfin, le numéro 13 correspond à un hôte particulier. Ce numéro de 8 bits indique donc l'un des hôtes du département d'administration d'entreprises de l'université d'Hawaii.

Adresses IP hiérarchiques et tables de routage simplifiées. Les opérations de routage sur l'internet reposent sur la nature hiérarchique des adresses IP. Pour prendre leurs décisions d'acheminement, les différents routeurs placés sur le chemin d'un paquet considèrent surtout son adresse réseau, et parfois également l'adresse de sous-réseau.

Bien que l'internet se compose de plusieurs millions d'hôtes, les routeurs ne disposent généralement que de quelques centaines de milliers de règles d'acheminement concernant les paquets qu'ils doivent traiter. Ces règles reposent soit uniquement sur l'adresse réseau, soit sur une combinaison des adresses réseau et de sous-réseau, et permettent d'envoyer par le même chemin tous les paquets à destination d'adresses apparentées.

Si, par exemple, une règle ordonne d'envoyer tous les paquets à destination du réseau 60 vers le routeur de premier bond 123.17.22.101 au travers du port 3, tous les paquets devant rejoindre ce réseau emprunteront ce même chemin.

L'adresse hôte n'intéresse ainsi que le dernier routeur sur le chemin d'un paquet vers sa destination.

Masque d'adresses IP. Toutes les adresses IP mesurent 32 bits, mais la taille de leurs différentes composantes est variable. L'adresse IP de la figure 3.11 a, par exemple, une adresse réseau de 16 bits, et une adresse de sous-réseau ainsi qu'une adresse hôte de 8 bits chacune, mais toutes les combinaisons de multiples de 8 sont possibles. En plus d'une adresse IP, les paquets sont également porteurs d'un masque informant les routeurs sur la longueur de l'adresse réseau et, le cas échéant, de l'adresse de sous-réseau.

Masque de réseau. Un masque est un nombre de 32 bits. Les masques de réseau sont composés de 1 dans l'adresse réseau et de 0 dans l'adresse de sous-réseau et l'adresse hôte. Le masque de réseau de l'adresse IP de la figure 3.11 est 255.255.0.0 (en notation décimale, 11111111 correspond à 255 et 00000000 à 0).

- *Application du masque de réseau 255.255.0.0 à l'adresse IP 128.171.17.13.* Le tableau 3.3 illustre l'utilisation des masques de réseau IP, c'est-à-dire la façon dont les routeurs déterminent que l'adresse réseau dans l'adresse IP 128.171.17.13, par exemple, est 128.171, codée sur 16 bits.

  Le masque de réseau correspondant à l'adresse 128.171.17.13 est 255.255.0.0. Quel que soit le masque appliqué à une adresse IP, les 1 « donnent » les bits de l'adresse et les 0 « donnent » des 0. Ainsi, l'application du masque 255.255.0.0 à l'adresse 128.171.17.13 donne 128.171.0.0. L'adresse réseau de 16 bits est bien 128.171.

Tableau 3.3 : Masquage d'adresse IP avec des masques de réseau et de sous-réseau.

	Masquage de réseau	**Masquage de sous-réseau**
Le masque	Renseigne sur la longueur de l'adresse réseau	Renseigne sur la longueur de la somme de l'adresse réseau et de l'adresse de sous-réseau
11111111 donne la valeur décimale	255	255
00000000 donne la valeur décimale.	0	0
Le masquage donne	Le bit d'adresse IP lorsque sa valeur est 1 ; 0 lorsque sa valeur est nulle	Le bit d'adresse IP lorsque sa valeur est 1 ; 0 lorsque sa valeur est nulle
Exemple 1		
Adresse IP	128.171.17.13	128.171.17.13
Masque	255.255.0. 0	255.255.255.0

Tableau 3.3 : Masquage d'adresse IP avec des masques de réseau et de sous-réseau. *(Suite)*

Résultat	128.171.0.0	128.171.17.0
Signification	L'adresse réseau de 16 bits est 128.171	Le couple adresse réseau et adresse de sous-réseau (d'une longueur totale de 24 bits) est 128.171.17
Exemple 2		
Adresse IP	60.47.123.7	60.47.123.7
Masque	255.0.0.0	255.255.0.0
Résultat	60.0.0.0	60.47.0.0
Signification	L'adresse réseau de 8 bits est 60	Le couple adresse réseau et adresse de sous-réseau (d'une longueur totale de 16 bits) est 60.47

- *Application du masque de réseau 255.0.0.0 à l'adresse IP 60.47.123.7.* L'application du masque réseau de 8 bits 255.0.0.0 à l'adresse IP 60.47.123.7 donne 60.0.0.0. L'adresse réseau est donc 60.

Masque de sous-réseau. Le masque de sous-réseau se compose de 1 à la fois dans la partie réseau et dans la partie sous-réseau. Il renseigne sur la longueur de la somme des parties réseau et sous-réseau d'une adresse IP, et non sur la taille respective de ces deux composantes. Il permet de créer des règles d'acheminement s'appliquant à tous les paquets destinés au même sous-réseau d'un réseau donné.

- *Application du masque de sous-réseau 255.255.255.0 à l'adresse IP 128.171.17.13.* Le masque de sous-réseau correspondant à l'adresse IP de la figure 3.11 est 255.255.255.0. L'application de ce masque à l'adresse 127.171.17.13 donne 128.171.17, c'est-à-dire une combinaison de 24 bits composée de l'adresse réseau (16 bits) et de l'adresse de sous-réseau (8 bits). Il n'est pas précisé quels bits correspondent à l'adresse réseau ou à l'adresse de sous-réseau.
- *Application du masque de sous-réseau 255.255.0.0 à l'adresse IP 60.47.123.7.* Le masque de sous-réseau 255.255.0.0 appliqué à l'adresse IP 60.47.123.7 donne 60.47.0.0. Ici, la longueur de la somme de l'adresse réseau et de l'adresse de sous-réseau n'est que de 16 bits.

3.4.6 Adressage IP et sécurité

Usurpation d'adresses IP. L'usurpation d'adresse IP consiste à remplacer l'adresse IP de l'expéditeur d'un paquet par une autre. Cette pratique, à la portée des hackers les moins expérimentés, permet essentiellement de protéger leur anonymat et d'abuser de la confiance de leurs cibles.

- *Anonymat de l'expéditeur.* Les attaquants attachent de l'importance à leur anonymat. L'utilisation d'une fausse adresse IP empêche l'identification du véritable expéditeur d'un paquet. À la figure 3.12, le destinataire pense avoir reçu un message de l'hôte 60.168.4.6, et non de l'hôte1.34.150.37.

- *Abus de confiance.* Les attaquants peuvent exploiter les liens de confiance existant entre certaines personnes pour s'assurer de la prise en charge de leurs paquets d'attaque. À la figure 3.12, l'utilisateur de l'hôte 60.168.47.47 se fie à l'utilisateur de l'hôte 60.168.4.6 ; il accepte tous les messages de sa part sans effectuer de vérification préalable. Il suffit donc *a priori* à un hacker d'usurper l'identité du second utilisateur (en usurpant son adresse IP) pour faire accepter ses paquets d'attaque sur le poste 60.168.47.47.

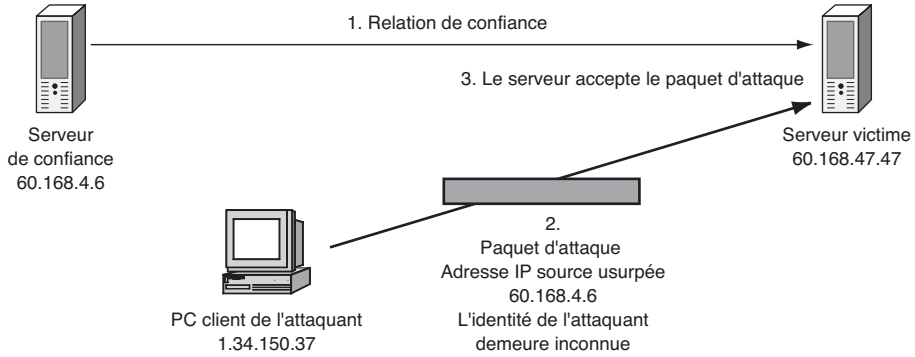


Figure 3.12 • Usurpation d'adresse IP.

Attaque LAND. L'une des principales attaques fondées sur l'usurpation d'adresse IP est l'attaque LAND (voir figure 3.13), qui consiste à envoyer un paquet contenant la même adresse IP dans les champs d'adresse IP source et de destination et le même numéro de port dans les deux champs correspondants.

Un message ainsi adressé constitue un non-sens qui tend à dérouter les hôtes tentant de le lire. Lors de la première attaque LAND en 1997, tous les clients et serveurs Windows ciblés, ainsi qu'un grand nombre de serveurs UNIX, de commutateurs, de routeurs, voire d'imprimantes ont été mis en échec. Les fabricants ont depuis développé des systèmes de protection contre ce type d'attaque, tenant compte du fait que des combinaisons de paramètres inattendues peuvent poser de sérieux problèmes.

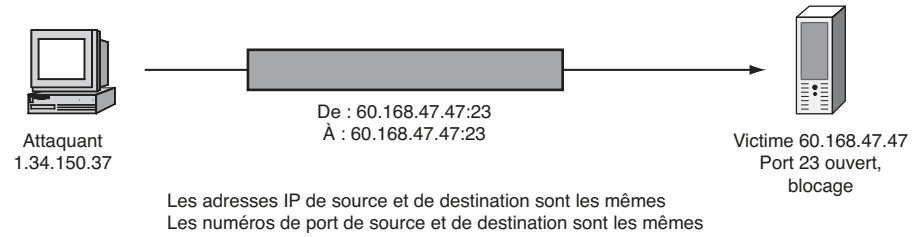


Figure 3.13 • Attaque LAND reposant sur l'usurpation d'adresse IP.

3.4.7 Autres champs d'en-tête IP

Les paquets IP sont constitués de deux parties : l'**en-tête**, qui se compose lui-même de plusieurs sous-parties appelées « champs d'en-tête », et le **champ de données**, qui contient généralement un segment TCP encapsulé, un datagramme UDP ou un message de contrôle ICMP.

Champ Protocole. Le champ Protocole de 8 bits informe sur la nature du message contenu dans le champ de données. Un 1 signifie par exemple qu'il s'agit d'un message ICMP, un 6 qu'il s'agit d'un segment TCP et un 17 que le message encapsulé est un datagramme UDP. Les pare-feux ont recours à ce champ pour savoir de quelle manière filtrer l'en-tête du paquet à traiter.

Champ Durée de vie. Le champ Durée de vie de 8 bits sert à supprimer les paquets présentant des en-têtes erronés, pour éviter qu'ils errent sans fin sur l'internet à la recherche de leur destinataire. Cette valeur, définie par l'expéditeur, peut aller jusqu'à 65 535 ; chaque routeur sur le chemin du paquet la réduit d'une unité[5]. Le routeur qui, après la soustraction, obtient une valeur de 0 est chargé d'éliminer le paquet.

Le champ de durée de vie peut malheureusement s'avérer très utile aux attaquants, en particulier en révélant d'importantes informations sur la nature des réseaux qu'ils cherchent à infiltrer. L'usage hostile le plus courant de ce champ consiste à envoyer plusieurs paquets d'une durée de vie d'une seule unité. Réduisant cette valeur à zéro, les premiers routeurs rencontrés suppriment ces paquets et renvoient à l'attaquant un message d'erreur contenant leur adresse IP. De nouvelles salves de paquets sont ensuite lancées, cette fois avec des paquets d'une durée de vie de deux unités, puis trois, puis quatre, etc. La série de messages d'erreurs renvoyés permet ainsi progressivement de cartographier le réseau sondé.

Le logiciel UNIX Traceroute a recours à une approche semblable pour identifier les routeurs situés sur le chemin emprunté par les paquets. Traceroute est ainsi à la fois un bon outil d'administration de réseau et un puissant outil d'attaque pour les pirates. L'équivalent de Traceroute sous Windows s'appelle Tracert.

La figure 3.14 présente un rapport Tracert concernant l'URL **www.hawaii.edu**. Tracert informe également sur le temps de transmission et parfois sur les noms des hôtes aux premiers routeurs rencontrés. Lorsque cette information n'apparaît pas, on peut supposer que les routeurs sont dotés de pare-feux ou programmés pour refuser de répondre à ce logiciel.

5. La durée de vie devait initialement être exprimée en secondes ; or la valeur contenue dans le champ de durée de vie correspond finalement au nombre maximal de bonds permis entre routeurs.

Figure 3.14 • Logiciel Tracert sous Windows.

Champs Longueur d'en-tête et Options. Le champ Longueur d'en-tête informe sur la longueur de l'en-tête IP : il suffit de multiplier la valeur de ce champ par 4 pour obtenir le nombre d'octets de l'en-tête. La valeur normale est 5, signifiant que l'en-tête ne contient pas de champ d'options et qu'il mesure 20 octets. En présence d'options, cette valeur est plus importante. Les pare-feux de certains réseaux d'entreprise sont conçus pour rejeter tous les paquets contenant des options (relativement rares) car celles-ci peuvent être le vecteur de différents types d'attaques[6].

Champ Longueur totale. Le champ Longueur totale renseigne sur la longueur en octets du paquet IP tout entier. S'agissant d'un champ de 16 bits, la longueur totale du paquet ne peut dépasser les 65 535 octets. Une des premières attaques par saturation, baptisée **Ping de la mort**, avait recours à des paquets **Ping** d'une taille supérieure à cette limite (voir figure 3.15). Elle affectait la plupart des premières versions de TCP/IP. Aujourd'hui, la grande majorité des systèmes d'exploitation sont conçus pour rejeter automatiquement les paquets surdimensionnés.

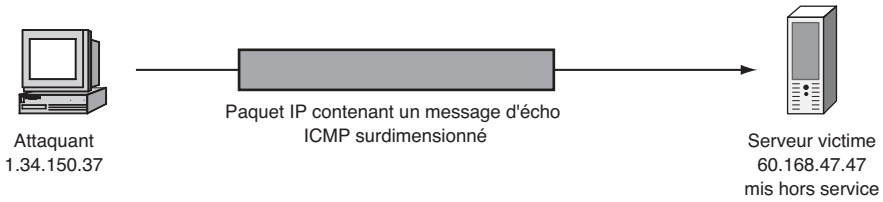


Figure 3.15 • Attaque Ping de la mort.

Champ Somme de contrôle (d'en-tête). Le champ Somme de contrôle contient une valeur permettant au processus internet du destinataire d'un message de vérifier les

6. Doté d'options d'acheminement par la source, le paquet peut par exemple décider lui-même du chemin à prendre pour rejoindre sa destination, propriété pouvant servir à la cartographie du réseau.

éventuelles erreurs contenues dans l'en-tête. La valeur de la somme de contrôle introduite par l'expéditeur d'un message se calcule à partir des valeurs des champs de l'en-tête IP. Le destinataire effectue le même calcul et compare son résultat à la valeur affichée par le paquet. Si les deux sont identiques, la transmission s'est probablement effectuée sans erreur.

Certaines personnes se méfient de cette méthode de contrôle en raison du manque de fiabilité du protocole IP, l'absence de correction d'erreurs empêchant la retransmission des paquets perdus ou défectueux. Ces derniers sont simplement supprimés en raison des dommages pouvant être causés par des en-têtes corrompus. Le nouveau standard IP (IPv6) est censé abandonner cette forme de protection, jugée superflue.

Fragmentation. Supposons qu'un paquet IP de grande taille se présente au niveau d'un routeur. Celui-ci identifie le sous-réseau de destination et constate avant la transmission que le paquet est trop volumineux pour l'infrastructure en place (les différentes technologies de réseau imposent des limites spécifiques à la taille des paquets entrants). Face à cette situation, le routeur est contraint de fragmenter le paquet IP, c'est-à-dire de diviser son champ de données en plusieurs morceaux et d'envoyer chacun de ces fragments au sein de paquets IP différents.

- *Assemblage des paquets.* Afin que l'hôte destinataire puisse reconstituer le message initial (par la mise bout à bout des champs de données des différents paquets), tous les fragments sont dotés d'un **numéro d'identification** (placé au sein d'un champ de même nom) identique à celui du paquet dont ils sont issus. Cela permet au destinataire de reconnaître tous les fragments d'un même paquet.

  Pour permettre au destinataire d'assembler tous les fragments dans le bon ordre, le routeur leur attribue par ailleurs une valeur de **décalage** (offset), qui est de 0 pour le premier fragment.

  Tous les fragments disposent également d'un bit «**fragment suivant**» mis à part le dernier, dont la valeur nulle dans le champ correspondant indique qu'il est le tout dernier de la série. Lorsque le destinataire le lit, il sait que l'assemblage du paquet original est achevé.

- *Attaque par saturation Teardrop.* L'une des premières attaques par saturation à exploiter la fragmentation des paquets IP a été l'attaque Teardrop, qui consistait en la génération d'une série de messages comparables aux fragments d'un paquet IP, à ceci près que les informations concernant leur longueur et leur décalage étaient incohérentes. La figure 3.16 montre que le champ de données reconstitué présente des vides et des chevauchements. Incapables d'interpréter les résultats de la reconstitution de ces paquets, de nombreux systèmes d'exploitation étaient vulnérables aux attaques Teardrop.

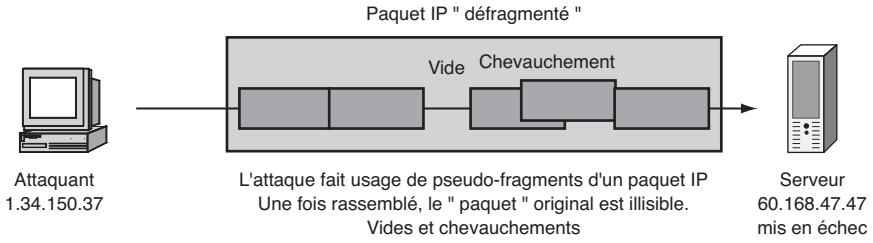


Figure 3.16 • Attaque par saturation Teardrop.

- *Paquets fragmentés et pare-feux.* La fragmentation de paquets induit elle aussi des risques car elle empêche les pare-feux d'examiner le contenu de chaque paquet entrant. En effet, seul le premier fragment d'une série porte les en-têtes TCP, UDP et ICMP (voir figure 3.17). S'il les juge dangereux, le pare-feu rejettera sans doute le premier fragment, mais pas obligatoirement les suivants, qui n'affichent pas de données d'en-tête prohibées. Du fait de ce risque et de la raréfaction croissante de la fragmentation de paquets, de nombreux pare-feux sont aujourd'hui conçus pour rejeter tous les paquets sans en-tête faisant suite à un paquet IP rejeté.

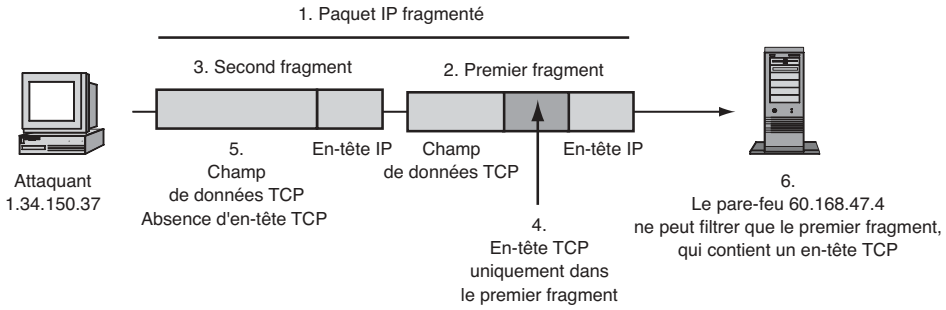


Figure 3.17 • L'en-tête TCP figure uniquement dans le premier fragment d'un paquet IP.

3.5 Protocole TCP (Transmission Control Protocol)

Les messages TCP, aussi appelés **segments TCP**, constituent sans doute la charge la plus courante des paquets IP. Le tableau 3.4 présente un tel segment à l'intérieur du champ de données d'un paquet IP.

Tableau 3.4 : Paquet IP portant un segment UDP dans son champ de données.

Bit 0 Bit 31

Version (4 bits)	Longueur d'en-tête (4 bits)	Type de service (8 bits)	Longueur totale (16 bits)	
Identification (16 bits)			Fanions	Décalage de fragment (13 bits)
Durée de vie (8 bits)		Protocole (8 bits)	Somme de contrôle d'en-tête (16 bits)	
Adresse IP source (32 bits)				
Adresse IP de destination (32 bits)				
Numéro de port source (16 bits)			Numéro de port de destination (16 bits)	
Numéro de séquence (32 bits)				
Numéro d'accusé de réception (32 bits)				
Longueur d'en-tête (4 bits)	Réservé (6 bits)	Champs de fanions (6 bits)	Taille de la fenêtre (16 bits)	
Somme de contrôle TCP (16 bits)			Pointeur urgent (16 bits)	
Options (éventuellement)				Bourrage
Champ de données				

Note : les champs de fanions sont de 1 bit ; ils peuvent inclure des bits SYN, ACK, FIN et RST.

3.5.1 Service fiable

La figure 3.18 schématise un échange de données entre deux processus de couche Transport au cours d'une session TCP. Tous les segments TCP conformes, reçus par ces processus, font l'objet d'un accusé de réception, connu sous le nom de segment ACK (pour « ACKnowledgement »). Un segment ACK n'est autre qu'un segment dont le bit ACK est activé.

Que se passe-t-il lorsqu'un segment ne fait pas l'objet d'un accusé de réception, comme le segment 8 de la figure 3.18 ? Le processus de couche Transport expéditeur considère qu'il s'agit d'un paquet perdu ou endommagé au cours de la transmission et procède à sa retransmission (segment 9).

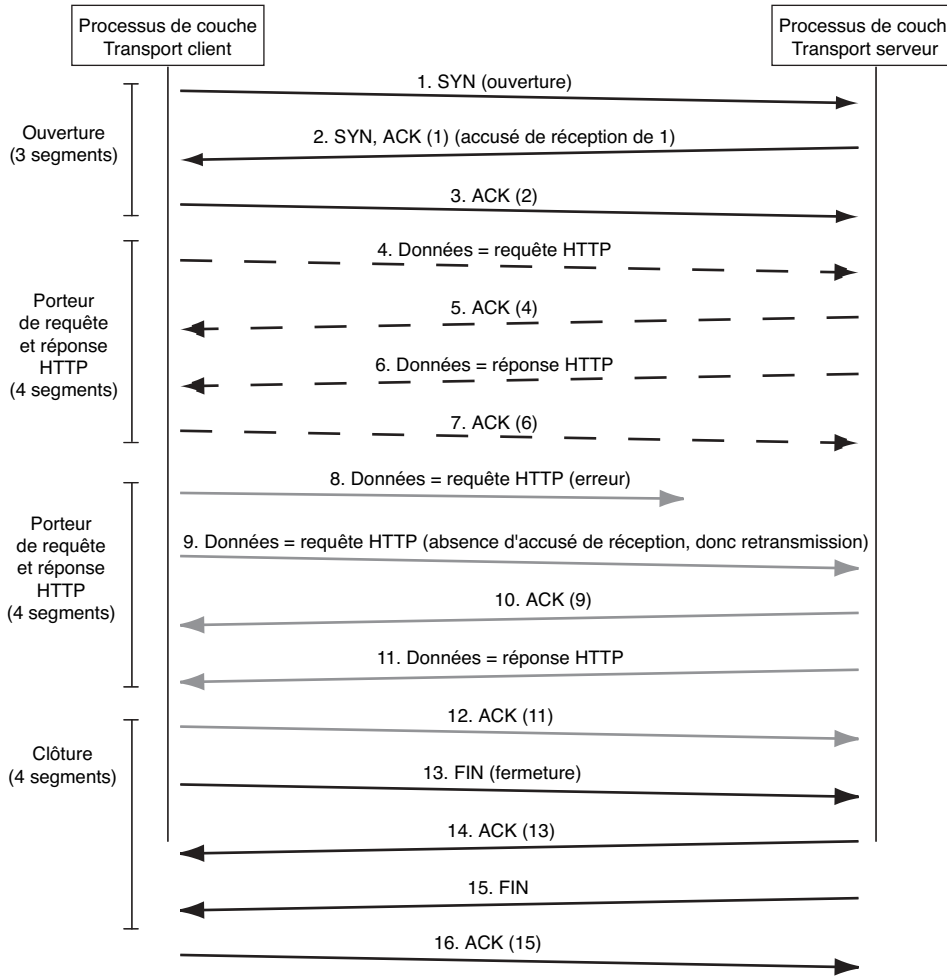


Figure 3.18 • Échanges au cours d'une session TCP normale.

3.5.2 Connexion TCP

Au contraire du protocole IP, TCP est un service orienté connexion dans la mesure où les connexions TCP passent par des étapes formelles d'ouverture et de clôture de session.

Ouverture en trois temps. L'établissement d'une session TCP nécessite l'échange de trois segments. On parle d'ouverture en trois temps.

Le processus de couche Transport désireux d'initier une connexion envoie tout d'abord un segment[7] TCP **SYN** (1), qui a par définition le bit SYN activé (c'est-à-dire fixé à 1), au processus Transport de son interlocuteur.

Si ce dernier accepte la connexion, il répond par un segment SYN/ACK (2), aux bits SYN et ACK activés, pour indiquer que la connexion est acceptée et pour accuser réception du segment SYN original.

Enfin, le processus initiateur envoie un segment ACK (3) accusant réception du segment SYN/ACK.

À ce niveau, les deux parties se sont déclarées favorables à la connexion et sont assurées de la disponibilité de leur interlocuteur. La connexion est désormais ouverte.

Clôture normale en quatre temps. La clôture (ou libération) d'une session TCP implique l'échange de quatre segments. Un premier segment **FIN** (13) de la part de l'un des deux interlocuteurs indique que toutes ses transmissions sont terminées (excepté les éventuelles transmissions de segments ACK). Un message accuse réception de ce segment (14), accompagné d'un segment FIN (15) indiquant que l'autre partie a également terminé de transmettre. Un dernier accusé de réception (16) informe que l'information est bien arrivée. La connexion est désormais fermée.

Encadré 3.3 : Synthèse du protocole TCP

Les messages sont des segments TCP (voir tableau 3.4)
Le champ de fanions contient plusieurs fanions de 1 bit : ACK, SYN, FIN, RST, etc.

Fiable (voir figure 3.18)
Le processus destinataire envoie un accusé de réception (ACK) au processus expéditeur pour les segments bien reçus.

Le bit ACK est activé.

Si le processus expéditeur ne reçoit pas de confirmation de la réception d'un segment donné, il procède à sa retransmission.

Connexion TCP (voir figure 3.18)
Procédures d'ouverture et de clôture formelles

Ouverture en trois temps : SYN, SYN/ACK, ACK

Clôture en quatre temps : FIN, ACK, FIN, ACK

Clôture brusque : RST

Un segment RST est envoyé au sein d'un paquet contenant l'adresse IP de l'expéditeur.

Utile pour les pirates dans la mesure où il permet d'identifier les adresses IP actives (voir figure 3.19).

Numéros de séquence et d'accusé de réception
Le numéro de séquence renseigne sur la position de chaque segment par rapport aux autres.

Le numéro d'accusé de réception permet de savoir à quel segment un accusé de réception fait référence.

7. Les numéros qui suivent les noms des segments renvoient aux numéros d'étapes mentionnés à la figure 3.18.

Numéro de port (voir figure 3.20)
Ports connus utilisés par les applications en mode root (ou administrateur) (1-1023)
HTTP = 80, Telnet = 23, FTP = 21 pour le contrôle, 20 pour le transfert de données, SMTP = 25
Ports disponibles pour n'importe quelle application (1024-49152)
Ports éphémères/dynamiques/privés utilisés par les clients (49153-65355, soit 16 384 au total)
Le format des interfaces de connexion (sockets) est le suivant : adresse IP : port ; par exemple : 128.171.17.13 :80
Désigne un logiciel spécifique sur un hôte donné
Usurpation de port (voir figure 3.21)
Application utilisant un port réservé sans autorisation
Souvent possible au travers des pare-feux, le port 80 étant le plus touché

Clôture brusque (RST). L'autre manière de libérer une session TCP est comparable au fait de « raccrocher au nez » de son interlocuteur. Il s'agit d'une clôture brusque.

Dans le cas d'une clôture brusque, un seul segment TCP, appelé RST (pour *ReSeT*), assure la clôture de la connexion. Celui-ci peut être envoyé à tout moment par l'un des deux interlocuteurs, ne laissant aucune équivoque quant au sort de la session.

- *Attaques par sonde SYN/ACK.* Soit un processus de couche Transport qui envoie un segment SYN/ACK au processus homologue d'un autre hôte n'ayant émis aucun segment SYN préalable (voir figure 3.19). Ce dernier, victime d'une attaque par sonde SYN/ACK, répond par un segment RST pour indiquer son refus.

  Le problème est que le paquet IP porteur du segment RST contient l'adresse IP de son expéditeur, information précieuse pour tout attaquant cherchant à identifier les adresses IP actives d'un réseau donné pour l'assaillir. L'envoi de paquets SYN/ACK à toutes les adresses d'un groupe d'adresses IP est un très bon moyen de planifier une attaque contre un réseau.

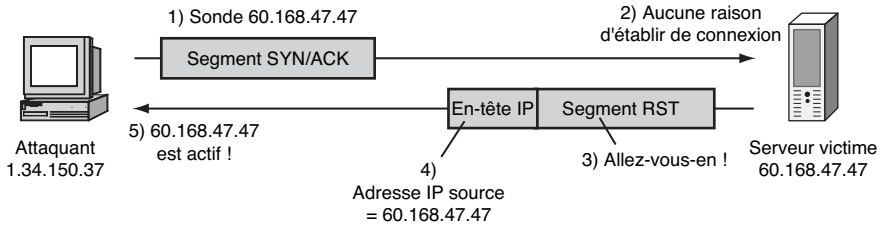


Figure 3.19 • Attaque par sonde SYN/ACK utilisant un segment RST.

3.5.3 Numéros de séquence et d'accusé de réception

Chaque segment TCP est doté d'un numéro de séquence renseignant sur son emplacement dans la chaîne de fragments en cours de transmission. Bien que les numéros

de séquence soient relativement complexes, ils suivent généralement un ordre croissant[8]. Au cours d'une connexion entre deux hôtes, chacun peut adopter son propre système de numérotation.

L'utilisation de numéros de séquence se justifie par la nature minimaliste du service IP, qui ne transmet pas forcément les paquets dans le bon ordre. Par ailleurs, un segment envoyé et reçu deux fois, à cause de la perte de l'accusé de réception correspondant, est facilement reconnu grâce à son numéro de séquence (identique sur les deux exemplaires) ; une version est donc immédiatement supprimée.

Le numéro d'accusé de réception permet, quant à lui, d'indiquer à l'expéditeur à quel paquet un accusé de réception donné fait référence.

Les numéros de séquence et d'accusé de réception ne sont pas les mêmes.

3.5.4 Numéros de port

Chaque segment TCP débute par un numéro de port source et un numéro de port de destination, longs de 16 bits chacun. Il en est de même pour les datagrammes UDP. Clients et serveurs exploitent ces champs de manière différente.

Serveurs et numéros de port réservés. Pour les serveurs, le numéro de port d'un segment TCP ou d'un datagramme UDP indique l'application à laquelle est destiné son champ de données (un même serveur propose souvent plusieurs services applicatifs).

Les applications les plus importantes disposent de plusieurs numéros de port réservés, compris entre 0 et 1023. Par exemple, l'un des numéros de port attitrés de HTTP est 80. FTP exploite le port 21 pour l'établissement des connexions et la transmission de messages de contrôle, et le port 20 pour le transfert de données. Le protocole SMTP (*Simple Mail Transfer Protocol*) utilise le port 25, tandis que l'application Telnet a recours au port 23.

À chaque fois qu'un client envoie un message de requête à un serveur, il place le numéro de port réservé de l'application qu'il souhaite exploiter (par exemple 80 pour un serveur Web et 25 pour un serveur SMTP) dans le champ relatif au numéro de port de destination (voir figure 3.20). La réponse du serveur contient, quant à elle, ce numéro de port dans son champ réservé au numéro de port source.

Numéros de port enregistrés. Les numéros de port réservés ne devraient être accessibles qu'aux applications privilégiées s'exécutant en mode root (ou administrateur), les autres services applicatifs pouvant opérer avec des privilèges moindres. Au lieu d'utiliser des numéros de port réservés, ceux-ci devraient avoir recours à des numéros de port enregistrés, compris entre 1 024 et 49 152.

8. La seule exception se présente lorsque le numéro de séquence atteint sa valeur maximale, auquel cas le décompte repart de 0 ou à un numéro de séquence peu élevé.

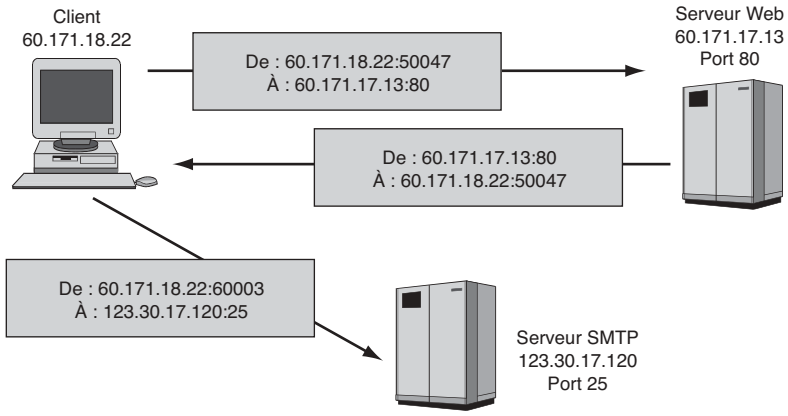


Figure 3.20 • Utilisation des numéros de port TCP et UDP.

Clients et numéros de port éphémères. Les clients procèdent d'une manière quelque peu différente. Tout client se connectant à un logiciel applicatif exécuté depuis un serveur génère un numéro de port éphémère (également dit **privé** ou **dynamique**), compris entre 49 153 et 65 535 (soit 16 382 numéros de port au total). Cette plage est recommandée par l'IETF. Cela dit, bien que tous les systèmes d'exploitation respectent la plage de numéro de ports connus (0-1 023), un grand nombre d'entre eux ont recours à des plages non standard de numéros de port éphémères.

Pour une transmission en direction d'un serveur Web, le numéro de port éphémère est 50 047. Pour une session avec un serveur de messagerie SMTP, c'est 60 003. Les paquets circulant dans la direction client-serveur contiennent tous ce numéro dans leur champ de numéro de port source, et les paquets renvoyés par le serveur dans leur champ de numéro de port de destination.

Socket ou interface de connexion. La figure 3.20 utilise la syntaxe «socket», à savoir une adresse IP et un numéro de port séparés d'un deux-points, par exemple : 60.171.18.22 :50047. Une socket est une application spécifique opérant sur un hôte particulier.

Usurpation de port. Le fait d'utiliser un numéro de port non autorisé, tel qu'un numéro de port réservé au lieu d'un numéro de port éphémère, est qualifié d'usurpation de port (voir figure 3.21).

Le problème est le suivant : en raison de l'important volume de trafic HTTP auquel elles font face, de nombreuses entreprises autorisent le passage des paquets destinés au port 80 sans aucun contrôle de pare-feu, ce qui constitue une voie d'accès privilégiée pour les pirates. Les applications usurpant le port 80 et d'autres ports peu contrôlés peuvent être détectées et bloquées par des pare-feux applicatifs (voir chapitre 5).

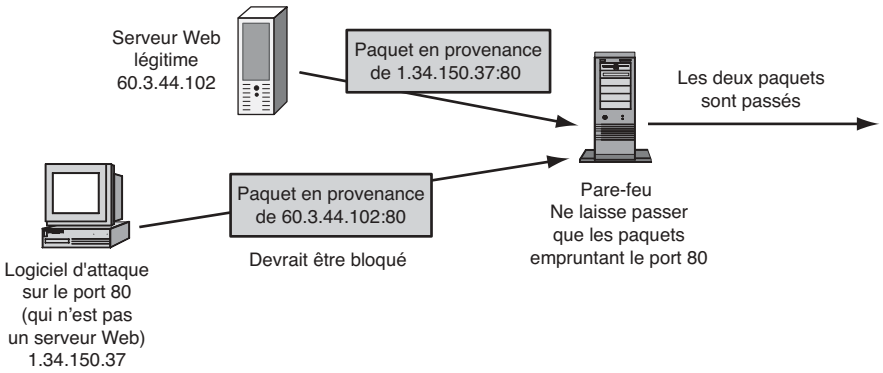


Figure 3.21 • Usurpation de port.

3.6 Protocole UDP (User Datagram Protocol)

3.6.1 Datagramme UDP

Le tableau 3.5 présente un paquet IP portant un datagramme UDP dans son champ de données. UDP étant un service sans connexion et non fiable, les datagrammes UDP sont beaucoup plus simples que les segments TCP ; par exemple, ils ne contiennent pas de champ d'accusé de réception, de numéro de séquence, de fanions, etc.

Un datagramme UDP est uniquement doté d'un numéro de port source et de destination, d'un champ de longueur UDP, indiquant la taille du datagramme, et d'un champ de somme de contrôle pour la vérification d'erreurs. À la moindre erreur rencontrée, le datagramme est rejeté, sans aucune demande de retransmission.

3.6.2 Usurpation de port UDP

En raison de sa simplicité, UDP offre moins de possibilités d'attaques aux pirates que TCP (ils profitent de la grande variété des champs d'en-tête des segments TCP pour tester l'effet de valeurs inhabituelles ou incohérentes). En revanche, à l'instar de TCP, UDP est vulnérable à l'usurpation de port.

3.6.3 Insertion de datagramme UDP

L'utilisation de numéros de séquence rend difficile l'insertion de faux segments au sein des échanges de paquets TCP. Pour que le segment intrus soit reconnu et accepté par le destinataire, le hacker doit lui attribuer le bon numéro de séquence ; or il s'agit là d'une opération très délicate. Avec UDP, par contre, l'insertion de datagrammes indésirables dans un flux de paquets ne pose pas de problème car le destinataire n'a aucun moyen de détecter la supercherie.

Encadré 3.4 : Synthèse du protocole UDP

Les datagrammes UDP sont simples (voir tableau 3.5)
Numéros de port source et de destination (16 bits chacun)
Longueur UDP (16 bits)
Somme de contrôle UDP (16 bits)

Usurpation de port possible

Insertion d'un datagramme UDP
Insertion d'un datagramme UDP dans un échange de paquets en cours
Difficile à détecter du fait qu'UDP n'utilise pas de numéros de séquence

Tableau 3.5 : Paquet IP portant un datagramme UDP dans son champ de données.

Bit 0 Bit 31

<table>
<tr><td colspan="2">Version (4 bits)</td><td>Longueur d'en-tête (4 bits)</td><td>Type de service (8 bits)</td><td colspan="2">Longueur totale (16 bits)</td></tr>
<tr><td colspan="4">Identification (16 bits)</td><td>Fanions</td><td>Décalage de fragment (13 bits)</td></tr>
<tr><td colspan="2">Durée de vie (8 bits)</td><td colspan="2">Protocole (8 bits)</td><td colspan="2">Somme de contrôle d'en-tête (16 bits)</td></tr>
<tr><td colspan="6">Adresse IP source (32 bits)</td></tr>
<tr><td colspan="6">Adresse IP de destination (32 bits)</td></tr>
<tr><td colspan="3">Numéro de port source (16 bits)</td><td colspan="3">Numéro de port de destination (16 bits)</td></tr>
<tr><td colspan="3">Longueur UDP (16 bits)</td><td colspan="3">Somme de contrôle UDP (16 bits)</td></tr>
<tr><td colspan="6">Champ de données</td></tr>
</table>

3.7 Protocole ICMP (Internet Control Message Protocol)

Le protocole IP n'assure que le transfert de messages, de la manière la plus simple qui soit. Les paquets transférés ne contiennent quasiment aucune information de contrôle (ou de commande). Pour pallier cette déficience et dans le dessein de normaliser les informations de contrôle de la couche Internet, les ingénieurs de l'IETF ont mis au point le protocole ICMP.

3.7.1 IP et ICMP

Les protocoles IP et ICMP entretiennent des liens très étroits décrits dans les RFC 791 et 792. Les messages ICMP sont véhiculés au sein de paquets IP (voir tableau 3.6). En outre, toutes les versions du protocole IP sont compatibles avec ICMP.

Tableau 3.6 : Paquet IP portant un message ICMP dans son champ de données.

Bit 0			Bit 31
Version (4 bits)	Longueur d'en-tête (4 bits)	Type de service (8 bits)	Longueur totale (16 bits)
Identification (16 bits)			Fanions / **Décalage de fragment (13 bits)**
Durée de vie (8 bits)		Protocole (8 bits)	Somme de contrôle d'en-tête (16 bits)
Adresse IP source (32 bits)			
Adresse IP de destination (32 bits)			
Type (8 bits)		Code (8 bits)	Dépend du type et du code
Dépend du type et du code			

3.7.2 Types de messages ICMP

ICMP reconnaît plusieurs types de messages, contenant chacun des informations de contrôle spécifiques. Ils se répartissent en trois catégories : les messages d'erreur, de contrôle et d'analyse de réseau. L'encadré 3.5 recense les types les plus courants.

Type et Code. Chaque type de message ICMP respecte une syntaxe particulière. Néanmoins, tous débutent par la même paire de champs de 8 bits : Type et Code. Le premier annonce la catégorie générale à laquelle le message en question appartient. Le second renseigne sur sa fonction précise ; il prend la valeur nulle quand le message ICMP n'a recours à aucun code.

Encadré 3.5 : Synthèse du protocole ICMP

ICMP gère les messages de contrôle (ou de commande) au niveau de la couche Internet.

ICMP et IP
Les messages ICMP sont encapsulés dans le champ de données des paquets IP.

Type et Code (voir tableau 3.6)
Type : catégorie à laquelle appartient un message de contrôle donné
Code : sous-catégorie du type (fixé à 0 en l'absence de code)

Messages d'analyse de réseau
L'écho (type 8, sans code) demande au destinataire s'il est opérationnel et disponible.
L'hôte visé renvoie une réponse écho (type 0, sans code).
Les logiciels Ping ont recours aux échos.
Les administrateurs réseau diagnostiquent les problèmes à partir des échos ne rencontrant pas de réponse.
Les pirates identifient des proies potentielles car une réponse à un écho est signe d'activité.

Messages d'erreur
Informent l'expéditeur d'une erreur, mais celle-ci n'est pas corrigée.
Destinataire inaccessible (type 3, codes multiples)
Un code est associé à chacune des raisons pouvant expliquer le silence de l'hôte visé.
Le message de réponse de l'hôte visé contient son adresse IP.
Temps écoulé (type 11, sans code)
Chaque routeur réduit la valeur du champ de durée de vie d'une unité.
Le routeur qui, après soustraction, obtient une valeur de durée de vie égale à 0 élimine le paquet et envoie un message de temps écoulé.
Ce message contient l'adresse IP du routeur.
En envoyant successivement des paquets d'une durée de vie à chaque fois supérieure d'une unité, il est possible d'explorer progressivement tout le réseau, jusqu'à obtenir sa représentation fidèle.

Code de contrôle
Réseau de contrôle
Ralentissement de la source (type=4, sans code)
Demande à l'hôte interlocuteur de réduire sa vitesse de transmission.
Usage légitime : contrôle de flux si l'hôte envoyant un message de demande de ralentissement est saturé
Les hackers peuvent lancer une attaque par saturation (déni de service)
Redirection (type 5, codes multiples).
Demande à l'hôte ou routeur d'envoyer le paquet par une voie différente de celle qu'il vient d'utiliser.
Les attaquants peuvent perturber les activités de réseau en envoyant, par exemple, les paquets dans des « trous noirs ».

De nombreuses autres catégories de messages ICMP sont définies.

Messages d'analyse de réseau. Dans la première catégorie de messages ICMP figurent les messages d'analyse de réseau, qui permettent à l'administrateur d'un réseau (et également aux pirates) de connaître le statut de ses différents éléments.

- *Écho et réponse d'écho (Ping).* Un administrateur réseau souhaitant vérifier si un hôte donné est toujours opérationnel peut lui envoyer un message d'écho (type 8,

sans code). Si l'hôte est actif, il lui renvoie une réponse d'écho (type 0, sans code). Le logiciel le plus courant pour l'envoi de messages d'écho et l'analyse des réponses s'appelle Ping (*Packet INternet Groper*). Écho et réponse d'écho sont tous deux des messages d'analyse de réseau ICMP.

Tout administrateur de réseau use sans compter de Ping. Lorsqu'un problème se présente, il « pingue » les différents routeurs et hôtes pour vérifier lesquels sont encore accessibles, le profil des réponses lui permettant bien souvent de localiser la panne.

Malheureusement, Ping donne aussi aux pirates la possibilité de connaître un réseau aussi bien que son administrateur. L'envoi d'un grand nombre de Ping en simultané peut même constituer une attaque par saturation du fait du temps pris par les hôtes ciblés pour répondre à chaque requête d'écho.

Messages d'erreur. Les messages d'erreur informent les hôtes ou leurs utilisateurs des problèmes se déclarant au cours de leurs envois. Étant donné que les messages perdus en cours de transfert ne sont pas retransmis, il ne s'agit pas d'une correction d'erreur, mais plutôt d'un système d'avertissement d'erreur.

- *Destination inaccessible.* La principale famille de messages d'erreur ICMP regroupe les messages de destination inaccessible (type 3), émis par les routeurs ne parvenant pas à transmettre les paquets qu'ils traitent à leurs destinataires. Les raisons de ces échecs sont symbolisées par différents codes. Par exemple, le code 1 indique que le destinataire est inaccessible, le code 2 que le port spécifié par l'expéditeur est inaccessible, etc.

  Exploitant ce système de renseignement, une forme d'attaque relativement courante consiste à envoyer des paquets délibérément erronés dans le but de générer des messages d'erreur et à vérifier ainsi que les hôtes visés sont bien « actifs ». Encore un moyen clandestin de cartographier un réseau ! Les pirates préfèrent cette méthode au simple envoi de messages Ping car la plupart des pare-feux sont conçus pour filtrer les Ping en provenance de l'extérieur, les seules requêtes Ping légitimes étant censées être générées en interne.

- *Temps écoulé.* Chaque routeur situé le long du chemin emprunté par un paquet vers sa destination réduit sa valeur de durée de vie d'une unité. Lorsque cette valeur arrive à 0, le paquet est éliminé et un message d'erreur ICMP de temps écoulé (type 11, sans code) est envoyé à l'expéditeur. Les pirates disposent, là encore, d'un autre moyen de cartographier un réseau.

Messages de contrôle. Les messages de contrôle ICMP ayant la capacité de modifier le fonctionnement d'un réseau, ils sont particulièrement dangereux lorsqu'ils sont envoyés par un hacker.

- *Ralentissement de la source.* Certains types de messages ICMP servent à altérer le fonctionnement des hôtes ou routeurs du réseau. Les messages de ralentissement de la source (type 4, sans code) servent ainsi au **contrôle de flux**, c'est-à-dire à gérer la vitesse à laquelle les hôtes envoient leurs paquets. Un hôte recevant ce type de message réduit normalement sa vitesse de transmission. Malheureuse-

ment, les pirates en profitent pour lancer des attaques par saturation en forçant les serveurs d'un réseau à réduire leur vitesse de transmission à un tel point qu'ils ne parviennent plus à satisfaire les requêtes de leurs utilisateurs.

- *Redirection.* Parmi les autres messages de contrôle ICMP, l'un des plus dangereux est le message de redirection (type 5, différents codes), qui informe les hôtes et routeurs de l'existence de chemins plus appropriés en direction des destinataires. Un hacker s'en servira par exemple pour demander aux routeurs de faire passer par un réseau pirate tous leurs messages dirigés vers l'extérieur ou de les envoyer dans un «trou noir» d'où ils ne ressortiront jamais.

Autres types de messages ICMP. De nombreux autres types de messages ICMP existent. Ils présentent quasiment tous un certain danger lorsqu'ils proviennent de l'extérieur. Vous en trouverez une liste complète sur le site Web de la IANA (*Internet Assigned Number Authority*), à l'adresse **www.iana.com**.

Conclusion

Ce chapitre passe en revue les différentes notions associées à TCP/IP, en partant du principe que le lecteur a déjà une certaine connaissance du fonctionnement général de ce standard de protocoles. Il aborde ensuite TCP/IP du point de vue de la sécurité, en s'intéressant notamment à ses nombreuses faiblesses et aux principales menaces qui pèsent sur lui.

Exercices

3.1. Pourquoi les attaques Ping de la mort, Teardrop, LAND et autres imposent-elles de nouvelles approches dans la vérification de logiciels, qui vont au-delà de la simple détection d'erreurs ?

3.2. Comment concevoir un réseau IP plus sûr ? Il s'agit d'une question très complexe.

3.3. Comment un attaquant peut-il envoyer des faux paquets à partir d'un simple PC ?

3.4. En quoi le fait de disposer d'une carte précise d'un réseau peut-il faciliter la tâche d'un attaquant ?

3.5. Dans un message d'écho ICMP, quelle est la valeur du champ de code ?

3.6. Dans le fichier journal d'un système de détection d'intrusion, un certain nombre de paquets ont leurs bits (TCP) FIN et SYN activés. Peut-il s'agir de paquets d'attaques ? Justifiez. Si oui, quelle est l'intention probable de l'attaquant ?

3.7. Dans le même fichier journal figure à présent de nombreux paquets en provenance du port 80 (HTTP), envoyés par des PC clients. Que peuvent-ils indiquer ?