

Protocole UDP

Table des matières

1. Identification de la destination.....	2
2. Description de l'en-tête.....	3
3. Ports réservés/disponibles.....	5
3.1. Attribution des ports (ancienne méthode).....	6
3.2. Attribution des ports (nouvelle méthode).....	6

UDP est l'acronyme de « User Datagram Protocol », il est défini dans la RFC 768. Les données encapsulées dans un en-tête UDP sont des paquets UDP.



1. Identification de la destination

Rappel : Au niveau de la couche *Internet* les datagrammes sont routés d'une machine à une autre en fonction des bits de l'adresse IP qui identifient le numéro de réseau. Lors de cette opération aucune distinction n'est faite entre les services ou les utilisateurs qui émettent ou reçoivent des datagrammes, ie tous les datagrammes sont mélangés.

La couche UDP ajoute un mécanisme qui permet l'identification du service (niveau *Application*). En effet, il est indispensable de faire un tri entre les divers applications (services) : plusieurs programmes de plusieurs utilisateurs peuvent utiliser simultanément la même couche de transport et il ne doit pas y avoir de confusion entre eux.

Pour le système Unix les programmes sont identifiés de manière unique par un numéro de processus, mais ce numéro est éphémère, non prévisible à distance, il ne peut servir à cette fonction.

L'idée est d'associer la destination à la fonction qu'elle remplit. Cette identification se fait à l'aide d'un **entier positif** que l'on baptise **port**.

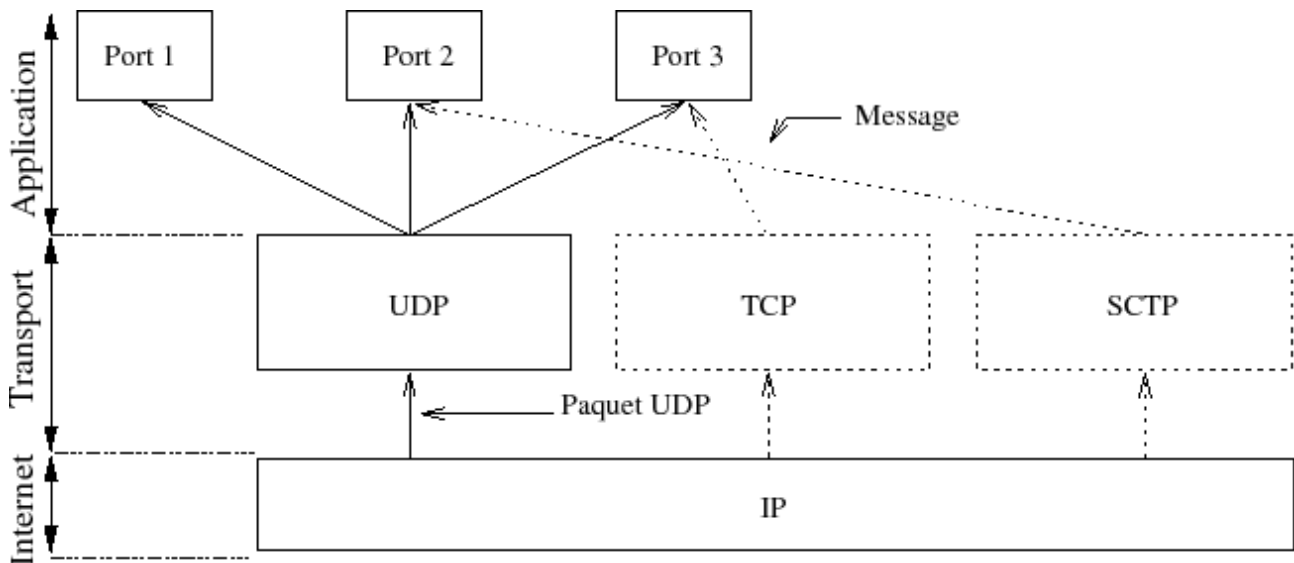
- Le système d'exploitation local a à sa charge de définir le mécanisme qui permet à un processus d'accéder à un port.
- La plupart des systèmes d'exploitation fournissent le moyen d'un accès synchrone à un port. Ce logiciel doit alors assurer la possibilité de gérer la file d'attente des paquets qui arrivent, jusqu'à ce qu'un processus (Application) les lise. A l'inverse, l'OS (Operating System), bloque un processus qui tente de lire une donnée non encore disponible.

Pour communiquer avec un service distant il faut donc avoir connaissance de son numéro de port, en plus de l'adresse IP de la machine elle-même.

On peut prévoir le numéro de port en fonction du service à atteindre.

La *figure ci-dessous* explicite la notion de port. La couche IP sépare les datagrammes SCTP, TCP et UDP grâce au champ PROTO de son en-tête, l'association du protocole de transport et du numéro de port identifie un service sans ambiguïté.

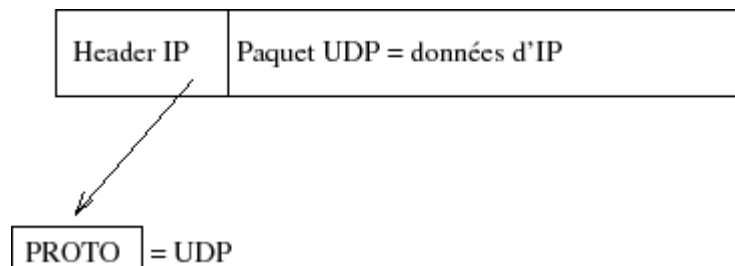
Conceptuellement on s'aperçoit alors que rien ne s'oppose à ce qu'un même service (Numéro de port) soit attribué conjointement aux trois protocoles (en pointillés sur la figure). Cette situation est d'ailleurs courante dans la réalité des serveurs.



Numéro de port comme numéro de service

2. Description de l'en-tête

Un paquet UDP est conçu pour être encapsulé dans un datagramme IP et permettre un échange de données entre deux applications, sans échange préliminaire. Ainsi, si les données à transmettre n'obligent pas IP à fragmenter, un paquet UDP génère un datagramme IP et c'est tout !



UDP encapsulé dans IP

- UDP apporte un mécanisme de gestion des ports, au dessus de la couche Internet.
- UDP est simplement une interface au dessus d'IP, ainsi l'émission des messages se fait-elle sans garantie de bon acheminement. Plus généralement, tous les défauts d'IP recensés au chapitre précédent sont applicables à UDP.

Plus particulièrement, les paquets à destination d'une application UDP sont conservés dans une pile de type FIFO¹. Si l'application destinatrice ne les consomme pas assez rapidement, les plus anciens paquets risquent d'être écrasés par les plus récents... Un risque supplémentaire (par rapport aux propriétés d'IP déjà connues) de perte de données.

¹ First In First Out

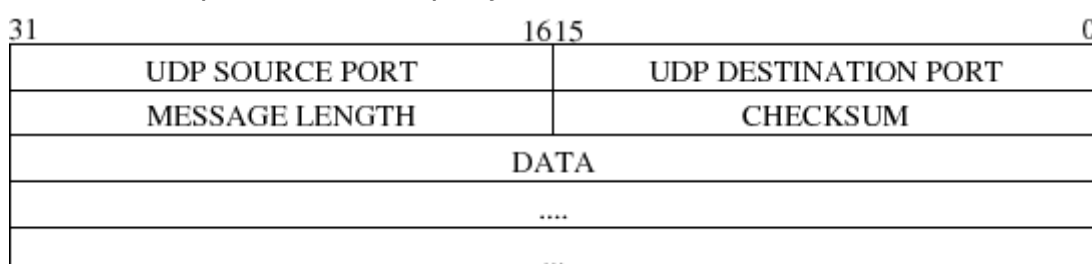
- Il n'y a aucun retour d'information au niveau du protocole pour apporter un quelconque moyen de contrôle sur le bon acheminement des données.

C'est au niveau applicatif qu'il convient de prendre en compte cette lacune.

- UDP est aussi désigné comme un mode de transport non connecté, ou encore mode datagramme, par opposition à TCP ou SCTP.

Parmi les utilisations les plus courantes d'UDP on peut signaler le serveur de noms, base de données répartie au niveau mondial, et qui s'accommode très bien de ce mode de transport.

En local d'autres applications très utiles comme tftp ou nfs sont également susceptibles d'employer UDP.



Structure de l'en-tête UDP

UDP SOURCE PORT

Le numéro de port de l'émetteur du paquet. Ce champ est optionnel, quand il est spécifié il indique le numéro de port que le destinataire doit employer pour sa réponse. La valeur zéro (0) indique qu'il est inutilisé, le port 0 n'est donc pas celui d'un service valide.

UDP DESTINATION PORT

Le numéro de port du destinataire du paquet.

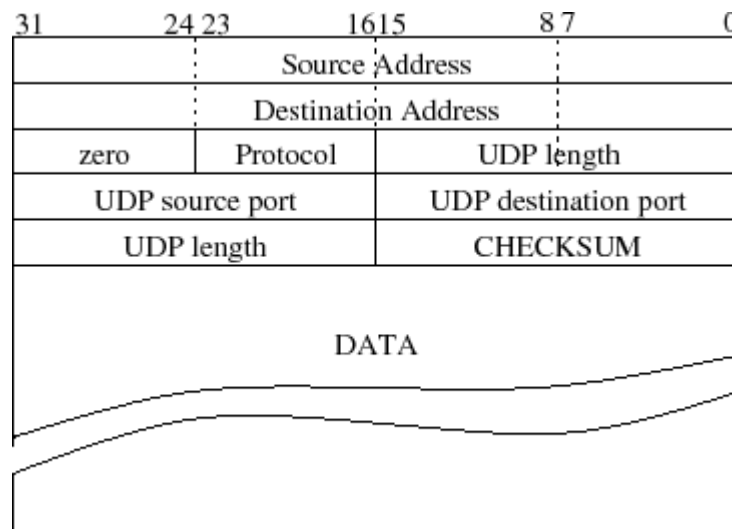
MESSAGE LENGTH

C'est la longueur du paquet, donc comprenant l'en-tête et le message.

- La longueur minimal est 8
- La longueur maximale est $65\ 535 - H(IP)$. Dans le cas courant (IP sans option) cette taille maximale est donc de 65 515.

CHECKSUM

Le checksum est optionnel et toutes les implémentations ne l'utilisent pas. S'il est employé, il porte sur un pseudo en-tête constitué de la manière suivante :



Cas du checksum non nul

Ce pseudo en-tête est prévu initialement pour apporter une protection en cas de datagrammes mal routés !

3. Ports réservés/disponibles

Le numéro de port est un entier 16 bits non signé, les bornes sont donc $[0, 65535]$, par construction. Nous avons vu précédemment que le port 0 n'est pas exploitable en tant que désignation de service valide, donc le segment réellement exploitable est $[1, 65535]$.

Toute machine qui utilise la pile TCP/IP se doit de connaître un certain nombre de services bien connus, repérés par une série de ports bien connus (well known port numbers), pour pouvoir dialoguer avec les autres machines de l'Internet (vs Intranet). Sur une machine Unix, cette liste de services est placée dans le fichier `/etc/services` et lisible par tous les utilisateurs et toutes les applications.

En effet, un service (comprendre un programme au niveau applicatif) qui démarre son activité réseau (et qui donc est considéré comme ayant un rôle de serveur) s'attribue le (les) numéro(s) de port qui lui revient (reviennent) conformément à cette table.

Nom	Port	Proto	Commentaire
echo	7	tcp	
echo	7	udp	
ftp-data	20	tcp	#File Transfer [Default Data]
ftp-data	20	udp	#File Transfer [Default Data]
ftp	21	tcp	#File Transfer [Control]
ftp	21	udp	#File Transfer [Control]

ssh	22	tcp	#Secure Shell Login
ssh	22	udp	#Secure Shell Login
smtp	25	tcp	mail #Simple Mail Transfer
smtp	25	udp	mail #Simple Mail Transfer
domain	53	tcp	#Domain Name Server
domain	53	udp	#Domain Name Server
http	80	tcp	www www-http #World Wide Web HTTP
http	80	udp	www www-http #World Wide Web HTTP
pop3	110	tcp	#Post Office Protocol - Version 3
pop3	110	udp	#Post Office Protocol - Version 3
imap	143	tcp	#Interim Mail Access Protocol
imap	143	udp	#Interim Mail Access Protocol
https	443	tcp	#Secure World Wide Web HTTP
https	443	udp	#Secure World Wide Web HTTP

Ce tableau présente quelques uns des ports bien connus plus connus les plus utilisés, il y en a quantité d'autres...

L'IANA, centralise et diffuse l'information relative à tous les nombres utilisés sur l'Internet via une RFC. La dernière en date est la RFC 1700, elle fait plus de 200 pages !

Par voie de conséquence cette RFC concerne aussi les numéros de ports.

3.1. Attribution des ports (ancienne méthode)

Historiquement les ports de 1 à 255 sont réservés aux services bien connus, plus récemment, ce segment à été élargi à [1,1023]. Aucune application ne peut s'attribuer durablement et au niveau de l'Internet un numéro de port dans ce segment, sans en référer à l'IANA, qui en contrôle l'usage.

À partir de 1024 et jusqu'à 65535, l'IANA se contente d'enregistrer les demandes d'usage et signale les éventuels conflits.

3.2. Attribution des ports (nouvelle méthode)

Devant l'explosion du nombre des services enregistrés l'IANA a modifié la segmentation qui précède. Désormais les numéros de ports sont classés selon les trois catégories suivantes :

1. **Le segment [1,1023]** est toujours réservés aux services bien connus.

Les services bien connus sont désignés par l'IANA et sont mis

en œuvre par des applications qui s'exécutent avec des droits privilégiés (**root** sur une machine Unix)

2. **Le segment [1024,49151]** est celui des services enregistrés.

Ils sont énumérés par l'IANA et peuvent être employés par des processus ayant des droits ordinaires.

Par exemple :

Nom	Port	Proto	Commentaire
bpcd	13782	tcp	VERITAS NetBackup
bpcd	13782	udp	VERITAS NetBackup

3. **Le segment [49152, 65535]** est celui des attributions dynamiques et des services privés.