

Ministère de l'enseignement supérieur et de la recherche scientifique  
Institut Supérieur des Études Technologiques de Zaghuan  
Département Technologies de l'Informatique



Module  
**Réseaux Locaux d'Entreprises  
& Architecture TCP/IP**  
Chapitre 9  
**Les protocoles Transport**

Elaboré par  
**Rim BRAHMI**

Public cible  
**2<sup>ème</sup> année Licence Appliquée en Réseaux et Services  
Informatiques**

Année universitaire 2019-2020

**Table de matières**

|  |    |
|--|----|
| Chapitre 9 : Protocoles Transport.....                     | 3  |
| Leçon 1 : Le protocole UDP.....                            | 4  |
| Introduction .....   | 5  |
| I. Les caractéristiques UDP (User Datagram Protocol) ..... | 5  |
| II. Format de segment UDP .....                            | 5  |
| III. Protocoles applicatifs utilisant UDP.....             | 6  |
| Conclusion.....  | 7  |
| Leçon 2 : Protocole TCP .....                              | 8  |
| Introduction .....   | 9  |
| I. Fonctionnement TCP (Transmission Control Protocol)..... | 9  |
| II. Entête TCP .....                                       | 9  |
| III. Ouverture & fermeture d'une connexion.....            | 10 |
| II.1. Three Way Handshake.....                             | 10 |
| IV. Contrôle de flux.....                                  | 12 |
| V. Numéro de séquence et numéro d'acquittement.....        | 12 |
| VI. Contrôle de congestion.....                            | 13 |
| VII. TCP vs UDP .....                                      | 14 |
| VIII. Application .....                                    | 14 |
| Conclusion.....  | 15 |
| Leçon 3 : Le protocole RTP .....                           | 16 |
| Introduction .....   | 17 |
| I. Les fonctions RTP.....                                  | 17 |
| II. Format des messages RTP.....                           | 18 |
| Conclusion.....  | 19 |

## Chapitre 9 : Protocoles Transport

### Vue d'ensemble

Ce chapitre présente les protocoles de la couche transport de la pile protocolaire TCP/IP en détaillant le protocole UDP, son entête et les applications qui l'utilisent ainsi que le protocole TCP en introduisant le contrôle de flux, contrôle de congestion. Sans oublier le protocole dédié pour les applications temps réel RTP

### Objectifs

- Connaître le principe du fonctionnement du protocole TCP
- Connaître le principe du fonctionnement du protocole UDP
- Connaître le principe du fonctionnement du protocole RTP
- Comprendre le format de segment UDP
- Comprendre le format du segment TCP
- Identifier les services TCP à savoir établissement de la connexion, contrôle de flux, contrôle de congestion

### Prérequis

U.E Fondement réseaux, U.E Architecture et système I

### Durée de déroulement

- 3h de Cours
- 1 séance (1h) de TD

### Elements de contenu

- Le protocole UDP
- Le protocole TCP
- Le protocole RTP

## Leçon 1 : Le protocole UDP

|                              |  |
|------------------------------|--|
| <b>Objectif général</b>      | <ul style="list-style-type: none"><li>• Connaître le principe de fonctionnement de protocole UDP</li></ul>   |
| <b>Objectifs spécifiques</b> | <ul style="list-style-type: none"><li>• Comprendre les numéros de port et leur utilisation</li><li>• Comprendre les processus client UDP permettant d'établir la communication avec un serveur</li></ul> |
| <b>Volume horaire</b>        | <ul style="list-style-type: none"><li>• Cours : 1h</li></ul>   |
| <b>Mots clés</b>             | <ul style="list-style-type: none"><li>• la couche transport, numéro de port, UDP, sans connexion, non fiable</li></ul>   |

## Introduction

La couche transport est responsable des dialogues (sessions) entre les hôtes terminaux. Elle permet de multiplexer les communications entre les nœuds IP en offrant un support à la couche application de manière :

- Fiable et connectée avec le protocole TCP
- Non-fiable et non-connectée avec le protocole UDP

Les protocoles de la couche transport font le lien entre les hôtes (IP) et les services applicatifs (HTTP, FTP, DNS, et d'autres).

### I. Les caractéristiques UDP (User Datagram Protocol)

Le protocole UDP est défini dans la norme RFC 768. Il se charge uniquement du transport des données non fiable. Il est caractérisé par :

- Mode non connecté
- Sans négociation préalable
- Sans garantie de remise
- Sans reconstitution ordonnée des données
- Sans contrôle de flux,
- Acheminement au mieux

### II. Format de segment UDP

Le datagramme qui présente le message utilisateur. L'en-tête du datagramme est simple et fixe de 8 octets. Les 8 premiers octets contiennent toutes les informations d'en-tête nécessaires et la partie restante est constituée de données.

L'en-tête est divisé en quatre champs de 16 bits.

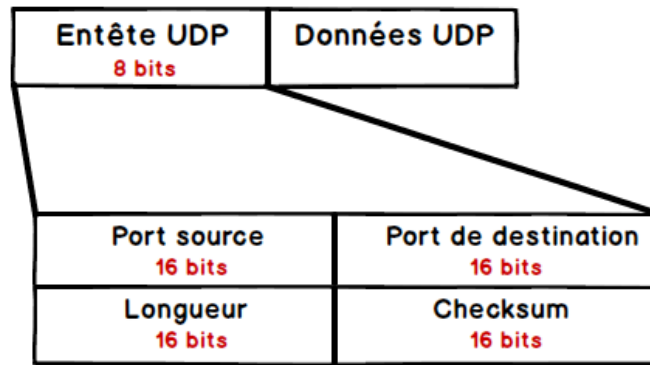


Figure 9.1. 1 : Datagramme UDP

**Port source et destination :** Les numéros de port identifient le processus émetteur et le processus de réception. La couche transport utilise le numéro de port de destination pour démultiplexer les données entrantes en provenance de la couche IP.

**Longueur :** ce champ en octets de l'en-tête UDP et les données encapsulées. La valeur minimale pour ce champ est 8 octets.

**Checksum :** Les 16 derniers bits de l'en-tête UDP sont réservés à la valeur de checksum. Ce champ est utilisé pour détecter des erreurs. Si ce champ est défini sur 0xFFFF, le checksum est désactivé. Le checksum est facultatif pour permettre aux implémentations de fonctionner rapidement.

### III. Protocoles applicatifs utilisant UDP

Le UDP est utilisé dans des communications simples, rapides, ainsi que le contrôle des flux et des erreurs sont moins préoccupant. Ce protocole convient à la multidiffusion puisque ce dernier prend en charge la commutation de paquets.

UDP est utilisé dans les mises à jour des certains protocoles de routage dynamique tels que RIP. Il est aussi conseillé pour les applications pour du trafic en temps réel à taille fixe et régulier (voix, vidéo).

Les protocoles applicatifs suivants utilisent l'UDP comme protocole de couche de transport :

- NTP (Network Time Protocol)
- DNS (Domain Name System)
- BOOTP, DHCP.

- NNP (Network News Protocol)
- Protocole TFTP, RTSP, RIP, OSPF.

UDP prend le datagramme de la couche réseau, ensuite il ajoute son en-tête et l'envoie au destinataire, il est rapide.

### **Conclusion**

Le protocole UDP fait partie de la couche transport de la pile protocolaire TCP/IP. Cette couche s'occupe essentiellement d'assurer le multiplexage, la segmentation et la reconstitution et le contrôle des erreurs. UDP sera le meilleur choix dans les applications temps réel et ne nécessitant pas le contrôle de flux.

## Leçon 2 : Protocole TCP

|                              |  |
|------------------------------|--|
| <b>Objectif général</b>      | <ul style="list-style-type: none"><li>• Savoir les caractéristiques du protocole TCP y compris les numéros de port et leur utilisation</li></ul>   |
| <b>Objectifs spécifiques</b> | <ul style="list-style-type: none"><li>• Comprendre les processus d'établissement et d'interruption de session TCP garantissent la fiabilité des communications</li><li>• Connaître comment les unités de données de protocole TCP sont transmises et comment leur réception est confirmée pour garantir l'acheminement des données</li></ul> |
| <b>Volume horaire</b>        | <ul style="list-style-type: none"><li>• Cours : 1h</li></ul>   |
| <b>Mots clés</b>             | <ul style="list-style-type: none"><li>• TCP, numéro de séquence, taille de fenêtre, contrôle de flux....</li></ul>   |



## Introduction

La couche transport est responsable de la gestion des exigences de fiabilité d'une conversation. Elle choisit le protocole le plus convenable pour les applications qui n'ont pas besoin du même degré de fiabilité. Dans un transfert fiable et connecté, elle utilise le protocole TCP.

### I. Fonctionnement TCP (Transmission Control Protocol)

TCP est défini dans la RFC 793. Il offre des services d'établissement et de fin des connexions ainsi que la communication en mode fiable et connecté avec :

- Orienté connexion : création d'une session entre la source et la destination : les périphériques négocient la quantité de trafic pouvant être transmise à un moment donné.
- Acheminement fiable : les données seront transmises en cas de perte.
- Accusé de réception pour garantir la transmission
- Garantie l'ordre à l'aide numéro de séquence (séquençage et ordonnancement)
- Contrôle de flux (fenêtrage) : dans le cas où TCP détermine que ces ressources sont surexploitées, il demande à l'application émettrice d'en réduire le flux
- Protocole avec état : il conserve une trace du nombre de segments qui ont été envoyés à un hôte donné à partir d'une application spécifique

### II. Entête TCP

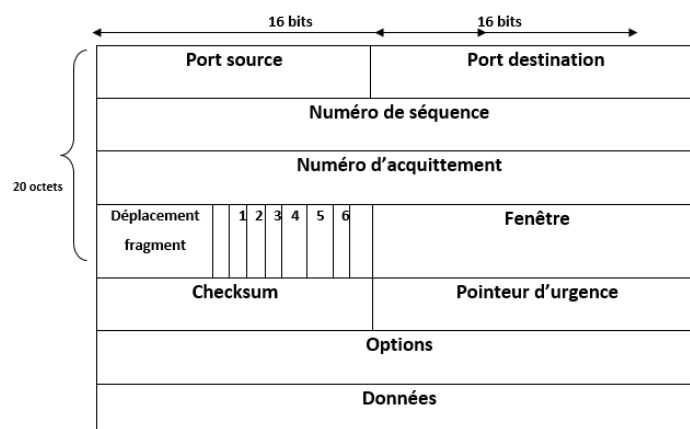


Figure 9.2. 1 : Entête TCP

- **Port source et port destination** : C'est un champ sur 16 bits qui permet d'identifier l'application. Lorsqu'une station veut ouvrir une connexion sur une machine distante en utilisant une application client, elle peut identifier l'application avec laquelle elle souhaite établir cette connexion en spécifiant le numéro de port attribué à cette application.
- Le but d'utilisation du port logique c'est le multiplexage des applications à travers le même accès internet.
  - 80 : http
  - 20,21 : FTP
  - 23 : Telnet
  - 25 : mail SMTP (Simple Mail Transfer Protocol)
- **Numéro de séquence** : Sur 32 bits, il indique le numéro du premier octet transporté par le paquet
- **Numéro d'acquittement (Ack)** : Il indique le numéro de prochain octet (SEQ) attendu.

$$N(SEQ)_{n+1} = N(SEQ)_n + (taille)_n$$

- **Fenêtre** : Contient le premier octet que le récepteur accepte de recevoir.
- **Checksum** : Permet de détecter les erreurs, il est calculé sur l'entête du paquet TCP.
- **Pointeur d'urgence** : Champs sur 16 bits contient le numéro de dernier octet d'un message urgent.
- **Options** : Les options concernent la taille de fenêtre, temporisateur, taille de fragment.

### III. Ouverture & fermeture d'une connexion

#### II.1. Three Way Handshake

L'établissement de la connexion se fait par un **handshaking** en trois temps. Pendant la phase d'établissement de la connexion, des paramètres comme le numéro de séquence sont initialisés afin d'assurer la transmission fiable (sans perte et dans l'ordre) des données.

Le côté client de la connexion effectue une ouverture active en 3 temps :

- Le client envoie un segment SYN au serveur,

- Le serveur lui répond par un segment SYN/ACK,
- Le client confirme par un segment ACK.

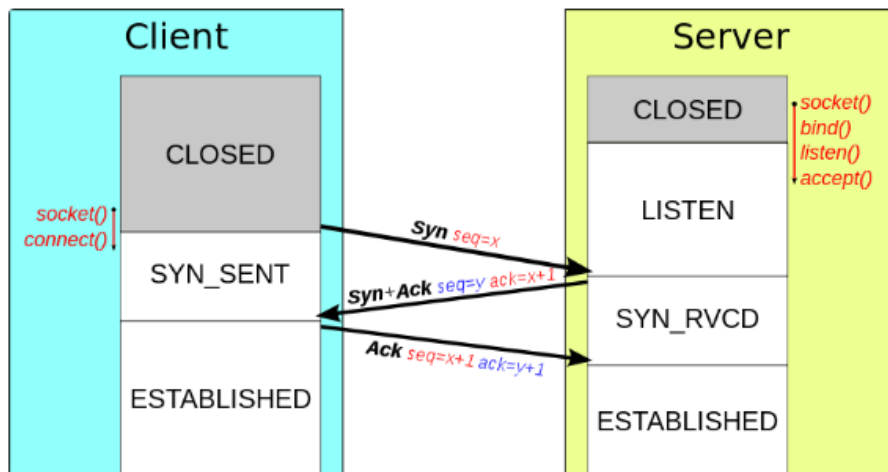


Figure 9.2. 2 : Connexion TCP (source <https://cisco.goffinet.org/>)

## II.2. Fin d'une connexion

La phase de terminaison d'une connexion utilise un **handshaking** en quatre temps. Chaque extrémité de la connexion effectue sa terminaison de manière indépendante. Ainsi, la fin d'une connexion nécessite une paire de segments FIN et ACK pour chaque extrémité.

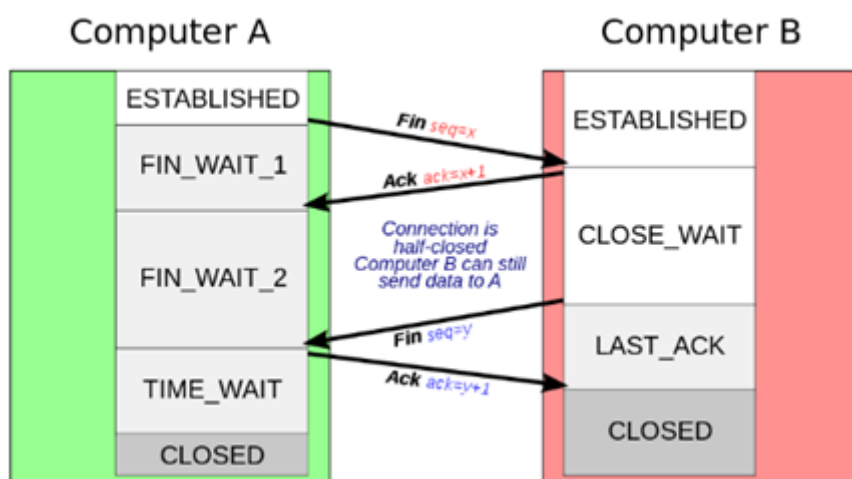


Figure 9.2. 3 : Fermeture de connexion TCP

#### IV. Contrôle de flux

Chaque extrémité dans une connexion TCP dispose d'un tampon de réception dont la taille est limitée. Afin d'éviter qu'un hôte ne surcharge l'autre, TCP prévoit plusieurs mécanismes de contrôle de flux :

- Un contrôle dans lequel le récepteur spécifie la taille de fenêtre en octet (le dernier octet admissible par le récepteur)
- Un mécanisme qui contrôle le nombre de segments qu'on peut émettre (slow start)

Chaque segment TCP contient la taille disponible dans le tampon de réception de l'hôte qui l'a envoyé. En réponse, l'hôte distant va limiter la taille de la fenêtre d'envoi afin de ne pas le surcharger.

#### V. Numéro de séquence et numéro d'acquittement

Les numéros d'ordre sont utilisés pour remettre les segments dans l'ordre d'origine. Lors de la configuration de la session, un numéro d'ordre initial nommé ISN est défini. Le premier segment a un numéro d'ordre ISN+1. Le numéro d'ordre est incrémenté du nombre d'octets ayant été transmis.

L'hôte récepteur place les données d'un segment dans une mémoire tampon. Les segments sont remis dans l'ordre correct et sont transmis à la couche application une fois qu'ils ont été réassemblés. Le numéro d'ordre et celui de l'accusé de réception sont utilisés ensemble pour confirmer la réception.

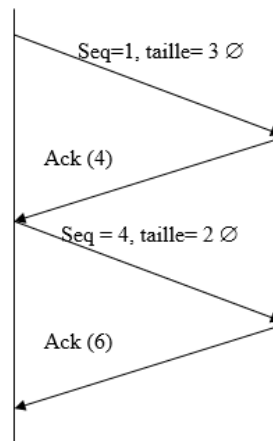
**Exemple :**

Figure 9.2. 4 : Exemple communication

**VI. Contrôle de congestion**

La congestion intervient lorsque trop de sources tentent d'envoyer trop de données trop vite pour que le réseau soit capable de les transmettre. Ceci entraîne la perte de nombreux paquets et de longs délais. En général, l'absence d'acquittements d'un paquet est la seule information sur l'état du réseau, mais la variation du **RTT** (Round trip time, Le délai aller-retour) ou l'**ECN** (Explicit Congestion Notification) est parfois utilisé aussi, l'ECN est négociée pour chaque connexion : elle n'est utilisée que lorsque les deux hôtes échangeant des données signalent leur intention de l'utiliser. À l'aide de temporisations, les émetteurs et destinataires TCP peuvent modifier le comportement du flux de données. C'est ce que nous nommons généralement le contrôle de congestion.

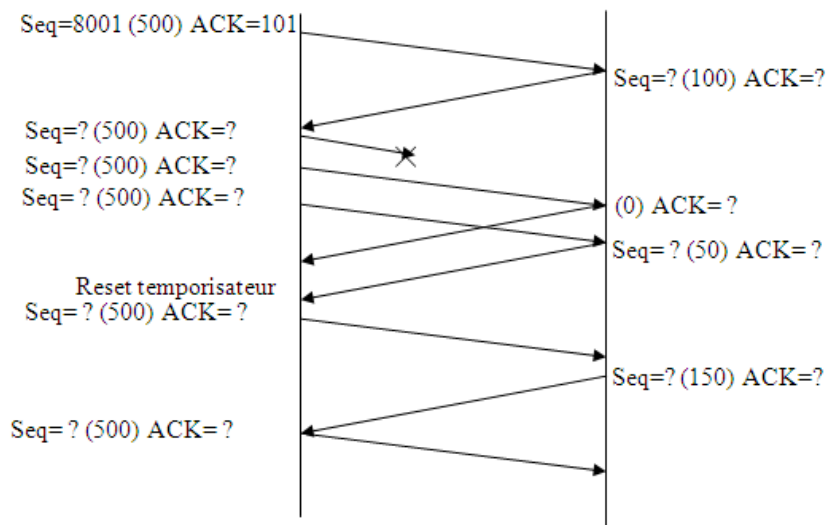
**VII. TCP vs UDP**

|                               | <b>Protocole TCP</b>   | <b>Protocole UDP</b>        |
|-------------------------------|--|-----------------------------|
| <b>Mode de fonctionnement</b> | Avec connexion.  | Sans connexion.             |
| <b>Taille de l'entête</b>     | 20 octets + taille de l'option   | 8 octets.                   |
| <b>Contrôle d'erreur</b>      | Assuré par le checksum.  | Le checksum est facultatif. |
| <b>Contrôle de flux</b>       | Mécanisme de fenêtre coulissante.  | Pas de contrôle de flux.    |
| Phase de transfert            | <ul style="list-style-type: none"> <li>○ Ouverture de connexion</li> <li>○ Transfert de données</li> <li>○ Fermeture de connexion</li> </ul> |                             |

**VIII. Application**

Soit le diagramme temporel suivant donnant l'échange de segments TCP entre un émetteur et un récepteur. Nous donnons pour chaque segment émis le numéro de séquence en émission Seq, la taille du segment (entre parenthèses) et le numéro de séquence en réception ACK.

1. Qu'est-ce que le numéro de séquence ?
2. Que représente l'acquittement ?
3. Compléter les numéros SEQ et ACK manquants (indiqués par des points d'interrogation) ?



## Conclusion

Les protocoles ARP et RARP diffèrent des autres protocoles TCP/IP car ils ne sont pas transmis dans les datagrammes IP. Ils se situent au niveau de la couche Internet et relient IP et Ethernet.

## Leçon 3 : Le protocole RTP

|                              |  |
|------------------------------|--|
| <b>Objectif général</b>      | <ul style="list-style-type: none"><li>• Comprendre le fonctionnement de protocole RTP</li></ul>  |
| <b>Objectifs spécifiques</b> | <ul style="list-style-type: none"><li>• Connaitre les fonctions de RTP</li><li>• Identifier les différents champs du message RTP</li></ul> |
| <b>Volume horaire</b>        | <ul style="list-style-type: none"><li>• Cours : 30mn</li></ul>   |
| <b>Mots clés</b>             | <ul style="list-style-type: none"><li>• RTP, RTCP, qualité de service, gigue...</li></ul>  |



## Introduction

L'existence d'applications temps réel, comme la parole numérique ou la visioconférence, est un problème pour Internet. Ces applications demandent une qualité de service (QoS) que les protocoles classiques d'Internet ne peuvent offrir. RTP (Real-time Transport Protocol) a été conçu pour résoudre ce problème, qui plus est directement dans un environnement multipoint. RTP a à sa charge aussi bien la gestion du temps réel que l'administration de la session multipoint

### I. Les fonctions RTP

Les fonctions de RTP sont les suivantes :

- Le séquençement des paquets par une numérotation. Cette numérotation permet de détecter les paquets perdus, ce qui est important pour la recomposition de la parole. La perte d'un paquet n'est pas un problème en soi, à condition qu'il n'y ait pas trop de paquets perdus. En revanche, il est impératif de repérer qu'un paquet a été perdu de façon à en tenir compte et à le remplacer éventuellement par une synthèse déterminée en fonction des paquets précédant et suivant.
- L'identification de ce qui est transporté dans le message pour permettre, par exemple, une compensation en cas de perte. La synchronisation entre médias, grâce à des estampilles.
- L'indication de tramage : les applications audio et vidéo sont transportées dans des trames (frames), dont la dimension dépend des codecs effectuant la numérisation. Ces trames sont incluses dans les paquets afin d'être transportées. Elles doivent être récupérées facilement au moment de la dépaquetisation pour que l'application soit décodée simplement.
- L'identification de la source. Dans les applications en multicast, l'identité de la source doit être déterminée.

RTP utilise le protocole RTCP (Real-time Transport Control Protocol), qui transporte les informations supplémentaires suivantes pour la gestion de la session :

- Indiquant la variance d'une distribution. La gigue d'un réseau, ou plutôt du temps de réponse d'un réseau, permet de savoir si les paquets arrivent à peu près régulièrement ou au contraire très irrégulièrement.

- Retour de la qualité de service lors de la demande de session. Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS. les applications multimédias sont souvent transportées par des flots distincts. Par exemple, la voix et l'image, ou même une application numérisée sur plusieurs niveaux hiérarchiques, peuvent voir les flots générés suivre des chemins distincts.
- Identification. Les paquets RTCP contiennent des informations d'adresse, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.
- Contrôle de la session. RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement une indication de leur comportement.

## II. Format des messages RTP

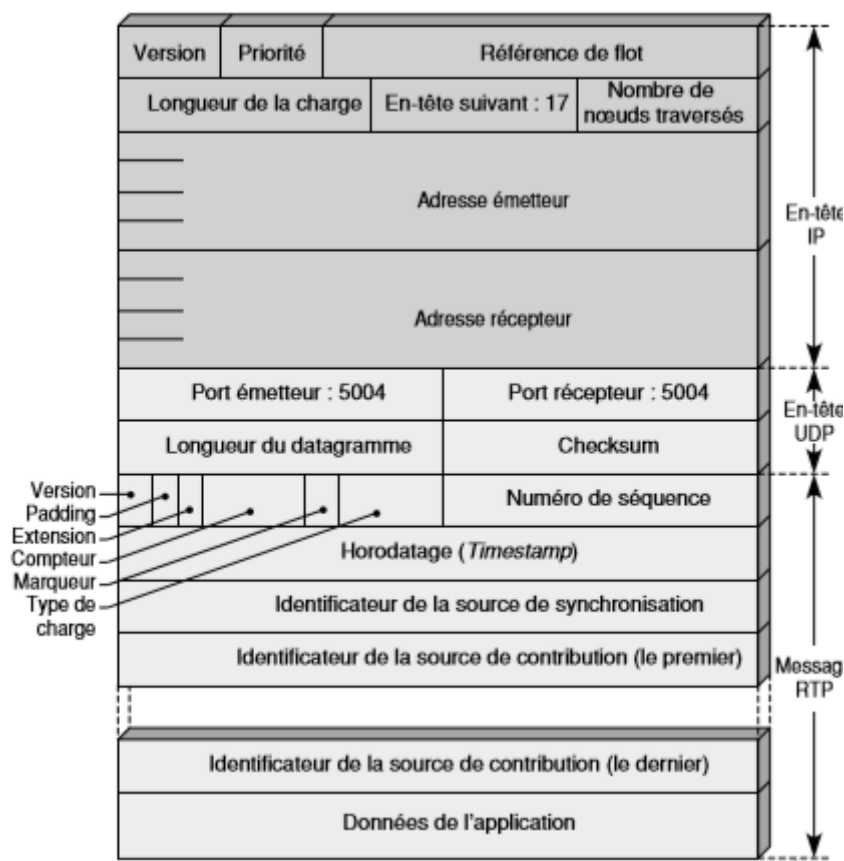


Figure 9.3. 1 : message RTP

Le format des messages RTP est illustré à la figure ci-dessus.

Les deux premiers octets contiennent six champs distincts. Les deux premiers bits indiquent le numéro de version (2 dans la version actuelle).

Le troisième bit indique si des informations de bourrage (padding) ont été ajoutées. Si la valeur de ce bit est égale à 1, le dernier octet du paquet indique le nombre d'octets de bourrage. Le bit suivant précise s'il existe une extension au champ d'en-tête de RTP, mais, en pratique, aucune extension n'a été définie jusqu'à présent par l'IETF. Le champ suivant, Contributor Count, indique le nombre d'identificateurs de contributeurs à la session RTP qui doivent être spécifiés dans la suite du message (jusqu'à 15 contributeurs peuvent être recensés). Le bit Marker met à la disposition de l'utilisateur une marque indiquant la fin d'un ensemble de données. Les sept éléments binaires suivants complètent les deux premiers octets et indiquent ce qui est transporté dans le paquet RTP.

### **Conclusion**

La RFC 1889 spécifie un protocole de transport de bout en bout pour des informations possédant des contraintes de temps réel telles que les données audios et vidéo interactives. Elle définit RTP (Real time Transport Protocol) et son compagnon RTCP (Real time Transport Control Protocol). Ils permettent respectivement de transporter et de contrôler des flots de données qui ont des propriétés temps réel.