Chapitre 1 :

Analyse multimédia : Normes et protocoles

Définitions :

Normalisation :

La normalisation est un processus politique, économique et technologique qui consiste à établir un ensemble de règles : Matériel (format, couleur, interface…), logiciel et Qualité. Posé par des gouvernements, industriels et universitaires, pour des besoins économique et politique.

Organisations de normalisation :

Parmi les principales organisations internationales de normalisation on trouve :

ISO : Organisation internationale de normalisation.

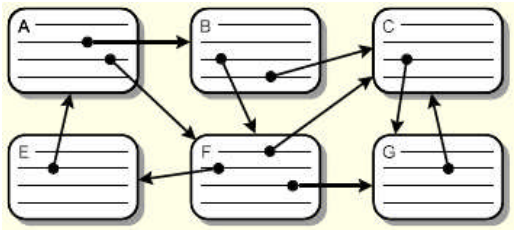
IEC : Commission électrotechnique internationale.

UIT : Union internationale des télécommunications.

Document multimédia :

Un document multimédia est un document interactif composé d'objets de natures différentes (Textes, Images, Sons, Vidéos…).

Document hypertexte : est un document structuré de manière non séquentielle c'est-à-dire une navigation dans une arborescence (liens sur un texte : cliquer sur un mot ou une phrase dans une page web vous conduisez vers une autre page web). On trouve aussi les documents hypermédia (liens sur des images). Donc, le parcours est décidé par le lecteur. Dans le cas d'un document structuré de manière séquentiel le parcours est obligatoire par exemple le diaporama.



Exemple de structure hypertexte comprenant 6 nœuds et 10 liens.

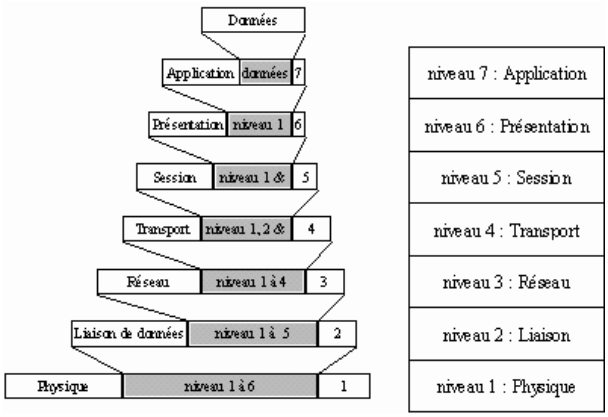
Protocole de communication :

Est un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau pour un type de communication particulier.

Rappel sur les modèles : OSI et TCP/IP

Le modèle OSI :

Le modèle OSI (Open System Interconnection) a été proposée par l'Organisation internationale de normalisation (ISO) en 1984, ce modèle gère la manière dont les transferts de données en réseau sont structurés. Ce modèle est organisé selon 7 couches :



Couche 7 application : transfert des informations entre logiciels.

Couche 6 présentation : mise en forme des données pour la lecture par le logiciel. On retrouve le cryptage, la compression - décompression de vidéo et sons, ...

Couche 5 session: gère l'établissement, la gestion et coordination des communications.

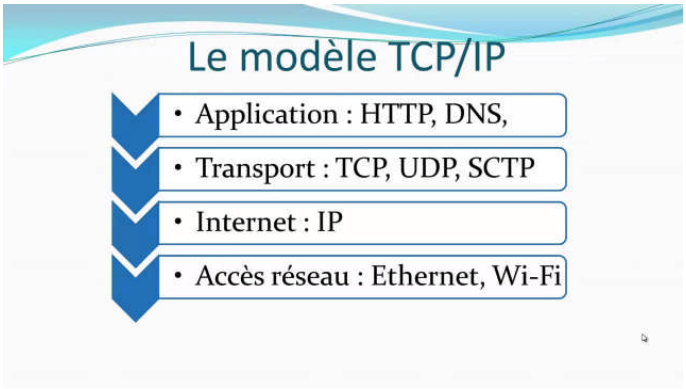
Couche 4 transport: gère les erreurs de données durant les transferts, on retrouve par exemple les protocoles UDP (User Datagram Protocol) en français protocole de datagramme utilisateur et le TCP (Transmission Control Protocol) en français protocole de contrôle de transmissions.

Couche 3 réseau: détermine les différentes routes possibles utilisées pour le transfert des données (routage). Cette couche utilise par exemple l'IP (Internet Protocol) et le FTP (File Transfer Protocol, il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur).

Couche 2 liaison: gère la validité des données transmises (si elles sont correctes).

Couche 1 physique: la méthode physique de transmission (en gros le type du canal de transmission). Les cartes réseaux, les hubs et switchs, points d'accès sans fils, ... sont à ce niveau.

-Le modèle TCP/IP :



HTTP (HyperText Transfer Protocol) « protocole de transfert hypertexte » est un protocole de communication client-serveur développé pour le World Wide Web.

Modèle OSI

Cette couche gère les formats de données entre les logiciels.	**Application** (data)	7
Met en forme les données pour permettre aux applications de les traiter (chiffrement/déchiffrement, compression/décompression…)	**Présentation** (data)	6
Organise et synchronise les échanges et les communications	**Session** (data)	5
Responsable du bon acheminement des messages entre les machines (vérifications des erreurs) et de l'optimisation des ressources réseaux.	**Transport** (segment)	4
La couche réseau s'occupe de déterminer le mode et la méthode d'acheminement entre plusieurs machines.	**Réseau** (paquet)	3
Permet de former des paquets parmi les signaux électriques, de vérifier les erreurs et de les fournir à la couche supérieure	**Liaison de données** (trames)	2
Transmission physique des bits d'une machine à une autre (transmission électrique au travers les connecteurs et câbles)	**Physique** (bits)	1

Modèle TCP / IP

4	**Application** (data)	On trouve ici les protocoles « de haut niveau » qui sont associés à un service final comme le web (http/https), la messagerie (SMTP/POP/IMAP), le stockage de fichier (FTP/TFTP/…) ou le chiffrement (SSL) par exemple.
3	**Transport** (segment)	Responsable du bon acheminement des messages entre les machines et de l'optimisation des ressources réseaux.
2	**Réseau** (paquet)	La couche réseau s'occupe de déterminer le mode et la méthode d'acheminement entre plusieurs machines.
1	**Accès au réseau** (bits, trames)	Permet à un hôte d'envoyer des informations à un autre hôte, elle est la combinaison de la couche 1 et 2 du modèle OSI

***Le protocole UDP**

UDP=User Datagram Protocol, ce protocole est inclus sous la couche 4 du modèle OSI qui est la couche transport. Le rôle de la couche transport est de diviser les données en un ensemble de segments et elle ajoute un champ pour le protocole utilisé (UDP ou TCP).

Port Source (16 bits)	Port Destination (16 bits)
Longueur (16 bits)	Somme de contrôle (16 bits)
Données (longueur variable)	

Format du segment UDP

Il contient les quatre champs suivants :

Port Source : indique depuis quel port le paquet a été envoyé.

Port de Destination : indique à quel port le paquet doit être envoyé.

Longueur : indique la longueur totale (exprimée en octets) du segment UDP (en-tête et données). La longueur minimale est donc de 8 octets (taille de l'en-tête).

Somme de contrôle : celle-ci permet de s'assurer de l'intégrité du paquet reçu quand elle est différente de zéro. Elle est calculée sur l'ensemble de l'en-tête UDP et des données,

***Le protocole TCP**

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Port Source 2 octets																Port destination 2 octets															
Numéro de séquence																															
Numéro d'acquittement																															
Taille de l'en-tête			Réservé			ECN / NS		CWR		ECE		URG		ACK		PSH		RST		SYN		FIN		Fenêtre							
Somme de contrôle																Pointeur de données urgentes															
Options																												Remplissage			
Données																															

Format du segment TCP

Signification des champs :

- Port source : numéro du port source
- Port destination : numéro du port destination
- Numéro de séquence : numéro de séquence du premier octet de ce segment
- Numéro d'acquittement : numéro de séquence du prochain octet attendu
- Taille de l'en-tête : longueur de l'en-tête en mots de 32 bits (les options font partie de l'en-tête)
- Indicateurs ou *Flags* :
    - Réservé : réservé pour un usage futur
    - ECN/NS : signale la présence de congestion.
    - CWR : Congestion Window Reduced : indique qu'un paquet avec ECE a été reçu et que la congestion a été traitée
    - ECE : ECN-Echo : si SYN=1 indique la capacité de gestion ECN, si SYN=0 indique une congestion signalée par IP.
    - URG : Signale la présence de données **urg**entes
    - ACK : signale que le paquet est un accusé de réception (**ack**nowledgement)
    - PSH : données à envoyer tout de suite (**p**u**sh**)
    - RST : rupture anormale de la connexion (**r**e**s**e**t**)
    - SYN : demande de **syn**chronisation ou établissement de connexion
    - FIN : demande la **fin** de la connexion
- Fenêtre : taille de fenêtre demandée, c'est-à-dire le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception.
- Somme de contrôle : somme de contrôle calculée sur l'ensemble de l'en-tête TCP et des données, mais aussi sur un pseudo en-tête (extrait de l'en-tête IP)
- Pointeur de données urgentes : position relative des dernières données urgentes
- Options : facultatives
- Remplissage : zéros ajoutés pour aligner les champs suivants du paquet sur 32 bits, si nécessaire
- Données : séquences d'octets transmis par l'application

TCP est capable :

• de faire tout ce que UDP sait faire (ports).

• de vérifier que le destinataire est prêt à recevoir les données.

• de découper les gros paquets de données en paquets plus petits pour que l'IP les accepte

• de numéroter les paquets, et à la réception de vérifier qu'ils sont tous bien arrivés, de redemander les paquets manquants et de les réassembler avant de les donnés aux logiciels. Des accusés de réception sont envoyés pour prévenir l'expéditeur que les données sont bien arrivées.

Remarque :

L'avantage de TCP sur UDP est que TCP permet des communications fiables. L'inconvénient est qu'il nécessite une négociation (par exemple les flags : syn et fin pour demander un établissement ou fin d'une connexion), ce qui prend du temps.

***Ports TCP et UDP :**

TCP, comme UDP, utilise le numéro de port pour identifier les applications. À chaque extrémité (client/serveur) de la connexion TCP est associé un numéro de port sur 16 bits (de 1 à 65535) assigné à l'application émettrice ou réceptrice. Exemples : FTP (21), HTTP (80), POP3 (110).

Les différences entre UDP et TCP :

***Le protocole IP (Internet Protocol) :**

Rappel sur l'adressage IP :

Un réseau est un ensemble de machine (hôte) reliés ensemble tout simplement (machines : PC, imprimante, automate…). Pour que ces machines se communiquent entre elles, il faut quelles possèdent des adresses, on parle ici sur les adresse IP (Internet Protocol).

Exemple :

192.168.0.1 (4 octet, le nombre maximal pour un octet est 255)

1100 0000.1010 1000.0000 0000.0000 0001

L'adresse IP sert à définir l'adresse de la machine et identifie le réseau sur lequel nous se trouve. Donc on besoin du masque sous-réseau.

192.168.0.1 (IP) (4 octets)

255.255.255.0 (masque sous-réseau) (255 par défaut) (4 octets)

Trouvez l'adresse réseau ?

D'abord on convertit l'adresse vers le binaire puis on fait un (ET logique AND) (comme un produit arithmétique).

1100 0000.1010 1000.0000 0000.0000 0001

And

1111 1111.1111 1111.1111 1111.0000 0000

= 1100 0000.1010 1**000.0000 0000.0000 0000**

(C'est la partie réseau) **(C'est la partie hôte (machine))**

192 . 168 . 0 . 0 (c'est l'adresse du réseau)

Les classes d'adresse IP :

Classe	Adresse IP	Masque
A	0.0.0.0-127.255.255.255	255.0.0.0
B	128.0.0.0-191.255.255.255	255.255.0.0
C	192.0.0.0-223.255.255.255	255.255.255.0
D	224.0.0.0-239.255.255.255	Non défini
E	240.0.0.0-255.255.255.255	Non défini

-Les adresses de classe D sont utilisées pour les communications multicast.

-Les adresses de classe E sont réservées par IANA (Internet Assigned Numbers Authority) à un usage non déterminé.

Plage adressable sur un réseau :

Combien de machine (hôte) on peut mettre sur un réseau ?

Exemple :

192.168. 0 . **0 partie hôte**

255.255.255.**0**

De 0-255 il y a 256 adresses

On a deux adresses réservées : 0 et 255

192.168.0.0 : c'est l'adresse du réseau

192.168.0.255 : c'est l'adresse de broadcast (diffusion), cette adresse sert à envoyer un message à toutes machines dans le réseau.

Donc le nombre d'adresse utilisable est 256-2=254 adresses.

La plage des adresses utilisables est :

192.168.0.1-192.168.0.254

Exercice :

Soit l'adresse IP et le masque suivant :

172.128.10.5

255.255.192.0

1-déterminer l'adresse du réseau.

2-déterminer le nombre d'adresse utilisable.

3-déterminer l'adresse du broadcast du réseau.

4-donner la plage adressable du réseau.

Corrigé :

1-

1010 1100.1000 0000.0000 1010.0000 0101 and

1111 1111.1111 1111.1100 0000.0000 0000

=1010 1100.1000 0000.0000 0000.0000 0000

Donc l'adresse du réseau est : 172.128.0.0

2-

255.255.192.0

1111 1111.1111 1111.11**00 0000.0000 0000** on a 14 bits dans la parie machine donc le plus grand nombre est :

11 1111 1111=16 383+1(l'adresse du 00 0000 0000)=16384 adresses

16383-2 (adresse du réseau et l'adresse de broadcast)=16382 adresses.

Le nombre d'adresse utilisable est 16382.

3-

172.128.0.0 : l’adresse du réseau

1010 1100.1000 0000.00**00 0000.0000 0000** (14 bits pour la partie machine)

1010 1100.1000 0000.00**11 1111.1111 1111**

172.128.63.255 : l’adresse du broadcast.

4-

La plage adressable :

172.128. 0 . 1 : l’adresse du réseau+1

172.128.63.254 : l’adresse du brodcast-1

Le rôle du protocole IP :

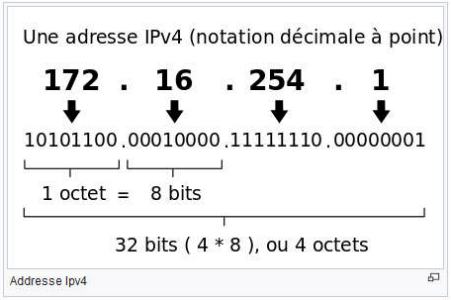
Le protocole IP est inclut sous la couche internet (2) du **modèle TCP/IP** et c’est également la couche réseau (3) du **modèle OSI**, ce protocole permet de :

-l’élaboration et le transport des paquets.

-représentation, routage et expédition des différentes informations sur le réseau.

Version du protocole IP :

IPV4 : défini par RFC 791(requests for comments) en 1981.



Une adresse IPv4 est représentée sous la forme de quatre nombres entiers séparés par des points comme 193.43.55.67. Chacun des nombres représente un octet. La plage d'attribution s'étend de 0.0.0.0 à 255.255.255.255, sachant qu'il existe des contraintes empêchant l'utilisation de certaines adresses (réservée, masque, broadcast, etc.).

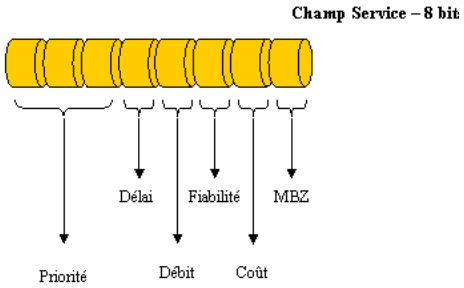
En-tête IPv4

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version d'IP				Longucur de l'en-tête				Type de service								Longueur totale															
Identification																Indicateur			Fragment offset											
Durée de vie								Protocole								Somme de contrôle de l'en-tête															
Adresse source																															
Adresse destination																															
Option(s) + remplissage																															

Version (4 bits) : Version d'IP utilisée. Ici, 4.

Longueur de l'en-tête ou IHL (pour Internet Header Length) (4 bits) : Nombre de mots de 32 bits, soit 4 octets (ou nombre de lignes du schéma). La valeur est comprise entre 5 et 15, car il y a 20 octets minimum et on ne peut dépasser 40 octets d'option (soit en tout, 60 octets).

Type de service ou ToS (pour Type of Service) (8 bits) : Ce champ permet de distinguer différentes qualités de service :



1 – Priorité

Le champ Priorité est codé sur 3 bits. Il indique la priorité que possède le paquet :

0 – 000 – Routine

1 – 001 – Prioritaire

2 – 010 – Immédiat

3 – 011 – Urgent

4 – 100 – Très urgent

5 – 101 – Critique

6 – 110 – Supervision interconnexion

7 – 111 – Supervision réseau

2 – Délai

Le champ Délai « Delay » est codé sur 1 bit. Il indique l'importance du délai d'acheminement du paquet. Voici les correspondances des différentes combinaisons :

0 – Normal

1 – Bas

3 – Débit

Le champ Débit « Throughput » est codé sur 1 bit. Il indique l'importance du débit acheminé. Voici les correspondances des différentes combinaisons :

0 – Normal

1 – Haut

4 – Fiabilité

Le champ Fiabilité « Reliability » est codé sur 1 bit. Il indique l'importance de la qualité du paquet. Voici les correspondances des différentes combinaisons :

0 – Normal

1 – Haute

5 – Coût

Le champ Coût « Cost » est codé sur 1 bit. Il indique le coût du paquet (la route minimale). Voici les correspondances des différentes combinaisons :

0 – Normal

1 – Faible

6 – MBZ

Le champ MBZ « Must Be Zero » est codé sur 1 bit. Ce dernier bit n'est pas utilisé et comme il indique nom, il doit être mis à 0.

Longueur totale en octets ou Total Length (16 bits) : Le champ Longueur totale est codé sur 16 bits et représente la longueur du paquet incluant l'entête IP et les Data associées. La longueur totale est exprimée en octets, ceci permettant de spécifier une taille maximum de 2^{16} = 65535 octets.

Identification (16 bits) : Numéro permettant d'identifier les fragments d'un même paquet. (constitue l'identification utilisée pour reconstituer les différents fragments. Chaque fragment possède le même numéro d'identification, les entêtes IP des fragments sont identiques à l'exception des champs Longueur totale, Checksum et Position fragment.

Vous trouverez tous les détails des mécanismes de fragmentation et de réassemblage dans la RFC 815)

Indicateurs ou Flags (3 bits) :

(Premier bit) actuellement inutilisé.

(Deuxième bit) DF (Don't Fragment) : lorsque ce bit est positionné à 1, il indique que le paquet ne peut pas être fragmenté.

(Troisième bit) MF (More Fragments) : quand ce bit est positionné à 1, on sait que ce paquet est un fragment de données et que d'autres doivent suivre. Quand il est à 0, soit le fragment est le dernier, soit le paquet n'a pas été fragmenté.

Fragment offset (13 bits) : Position du fragment par rapport au paquet de départ.

Durée de vie ou TTL (pour Time To Live) (8 bits) : Initialisé par l'émetteur, ce champ est décrémenté d'une unité généralement à chaque passage d'un routeur. Quand TTL = 0, le paquet est abandonné.

Protocole (8 bits) : Ce champ permet d'identifier le protocole utilisé par le niveau supérieur.

(Numéro du protocole au-dessus de la couche réseau) :

Par exemple :

01 – 00001 = ICMP

02 – 00010 = IGMP

06 – 00110 = TCP

17 – 10001 = UDP

Le protocole ICMP (Internet Control Message Protocol) : est un protocole de niveau 3 (couche de réseau) sur le modèle OSI, qui permet le contrôle des erreurs de transmission.

Le protocole IGMP (Internet Group Management Protocol) :

est un protocole qui permet à des routeurs IP de déterminer de façon dynamique les groupes multicast qui disposent de clients dans un sous-réseau.

Somme de contrôle de l'en-tête (Header Checksum) (16 bits) : Si la somme de contrôle est invalide, le paquet est abandonné sans message d'erreur.

Adresse source (32 bits) : Adresse IP de l'émetteur sur 32 bits.

Adresse destination (32 bits) : Adresse IP du récepteur 32 bits.

Options: Facultatif.

Remplissage (Padding) : Champ de taille variable comprise entre 0 et 7 bits. Il permet de combler le champ option afin d'obtenir un en-tête IP multiple de 32 bits. La valeur des bits de bourrage est 0.

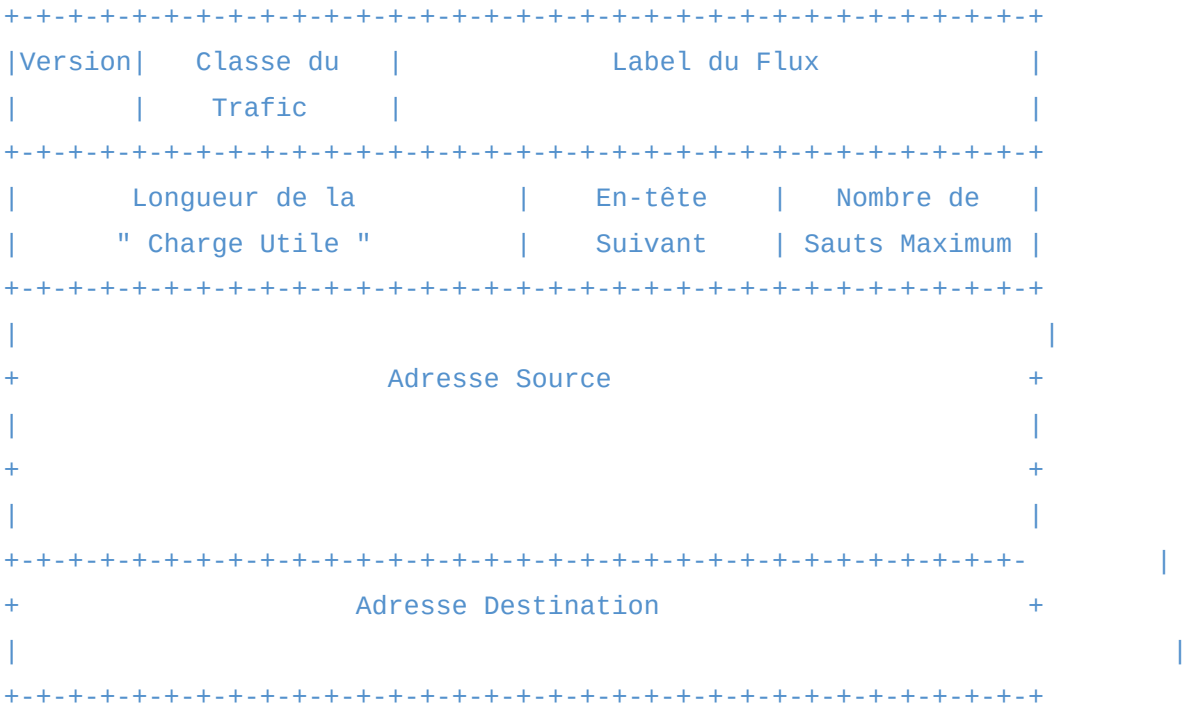
***Remarque :**

Le problème de cette version c'est qu'elle est limitée dans le nombre d'adresse qu'elle peut fournir, c'est une adresse codée sur 32 bits donc 2^{32} (4 294 967 296) adresses en théorie (pratiquement il y a des adresses non utilisables). A cause de l'unicité des adresses IP cette limite est en train d'être attente.

IPV6 : défini par RFC 2460 en 1998.

C'est une adresse codée sur 128 bits donc 2^{128} ($3.4*10^{38}$) adresses possibles. La notation décimale pointée employée pour les adresses IPv4 (par exemple 172.31.128.1) est abandonnée au profit d'une écriture hexadécimale, où les 8 groupes de 2 octets (16 bits par groupe) sont séparés par un signe deux-points :

2001:0db8:0000:85a3:0000:0000:ac1f:8001



Version (Version)

Numéro de version du Protocole Internet (= 6) sur 4 bits

Classe du Trafic (Traffic Class)
Le champ Classe du Trafic est sur 8 bits. Ce champ est utilisé par les routeurs pour identifier les différentes priorités ou type de service de paquets.

Label du Flux (Flow Label)
Le champ Label du Flux est sur 20 bits. Ce champ est utilisé par une source pour indiquer qu'une séquence de paquets nécessite un traitement spécial par les routeurs. Ce traitement spécial peut être une qualité de service différente du service par défaut ou un service " temps réel ".

Longueur de la "Charge Utile" (Payload Length)
sur 16 bits. Les en-têtes d'extension présents sont aussi considérés.

En-tête Suivant (Next Header)
sur 8 bits. Identifie le type de l'en-tête suivant. Utilise les mêmes valeurs que le champ " protocole ".

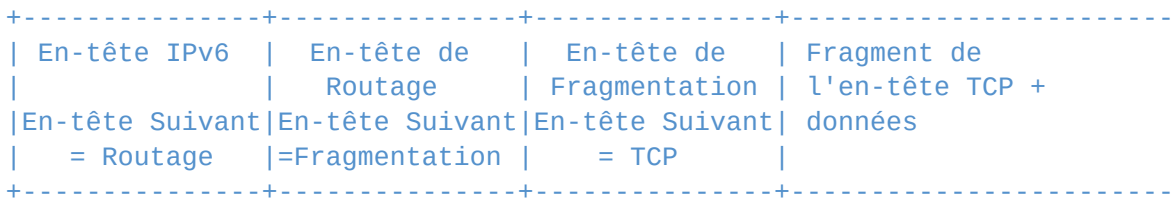
Nombre de Sauts Maximum (Hop Limit)
sur 8 bits.le meme pricipe que TTL de IPv4.

Adresse Source (Source Address)
Adresse sur 128 bits de l'expéditeur initial du paquet.

Adresse Destination (Destination Address)
adresse sur 128 bits du destinataire projeté du paquet (qui peut ne pas être le destinataire ultime, si un en-tête de routage est présent).

En-têtes IPv6 d'extension

Avec IPv6, les informations optionnelles sont encodées dans des en-têtes séparés qui peuvent être placés entre l'en-tête IPv6 et l'en-tête de la couche supérieure d'un paquet.



Remarque : Les deux versions sont incompatibles, par exemple un hôte dispose qu'une adresse IPV4 ne peut communiquer avec un autre hôte que dispose qu'une adresse IPV6. Donc la transition est toujours en cour de réalisation.

***Transmission en temps réel (streaming)**

streaming = technique de transfert de données sous forme d'un flux régulier et continu permet de diffuser et de visualiser des contenus multimédia en temps réel, par exemple : formation à distance, Web TV et radios Web.

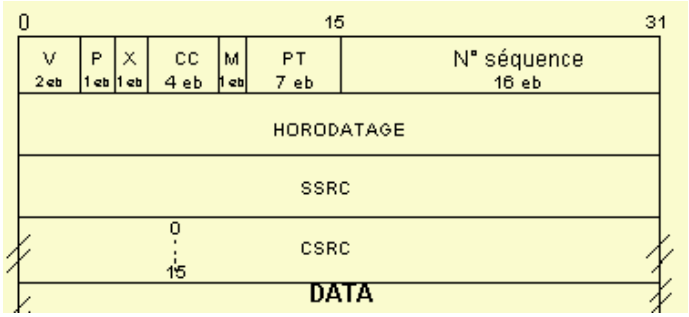
***Le protocole RTP (Real-time Transport Protocol)**

Le RTP a été standardisé en novembre 1995, est un protocole de la couche transport pour la transmission en temps réel, c'est-à-dire le streaming.

Le protocole RTP est basé sur UDP où le paquet RTP est caché dans un paquet UDP, le RTP est utilisé sur le protocole UDP plutôt que le TCP parce que le TCP garantis la fiabilité et perde la rapidité.

RTP est assez insensible pour la perte de paquets, donc cela ne nécessite pas la fiabilité de du TCP. De plus l'UDP possède un en-tête plus petit par rapport le TCP, donc un paquet peut transporter plus de données.

L'en-tête RTP



V (version)= indiquent le numéro de version (2 dans la version actuelle).

P (Padding)= indique si des informations de bourrage (padding) ont été ajoutées.

X (extension)= précise s'il existe une extension au champ d'en-tête de RTP.

CC (Contributor Count) : indique le nombre d'identificateurs de sources contributrices (CSRC) à la session RTP.

M (Marqueur) : indique la fin d'un ensemble de données.

PT (payload type) : indique la nature des données multimédia transportées dans le paquet RTP par exemple : (audio, video,…).

Numéro de séquence : permet de déterminer si un paquet est perdu.

Horodatage (timestamp): Indicatif sur l'instant de lecture du paquet RTP.

SSRC : Identificateur de la source de synchronisation (la source considérée comme un repaire).

CSRC : Identificateurs des sources contributrices.

RTP ne fourni pas des mécanismes de contrôle de flux, donc la qualité de service n'est pas garanti.

Pour contrôler le flux, le protocole RTP travail avec le protocole RTCP (Real-Time Control Protocol) pour obtenir des feed-back (retour d'information) concernant la qualité de la transmission tel que le nombre d'octet et de paquets transmis, le nombre de paquets perdus, la gigue.

La gigue (jitter): C'est le délai entre la transmission de deux paquets de donnés. L'effet de la gigue peut être supprimé en plaçant une mémoire tampon du côté du récepteur. Ce tampon de gigue provoque un délai au début du flux.

***Le protocole RTSP (Real Time Streaming Protocol)**

RTSP a été standardisé en 1998, on utilise le RTSP au-dessus de RTP dans la couche application, ce protocole ne s'occupe pas du transport de données. Il fonctionne comme « télécommande » du réseau pour régler l'émission. RTSP fourni des messages pour établir une connexion temps réel, pour lancer, pauser et arrêter la reproduction du film et pour avancer ou rembobiner le film.

***Protocole de réservation de ressource (RSVP : Resource Reservation Protocol)**

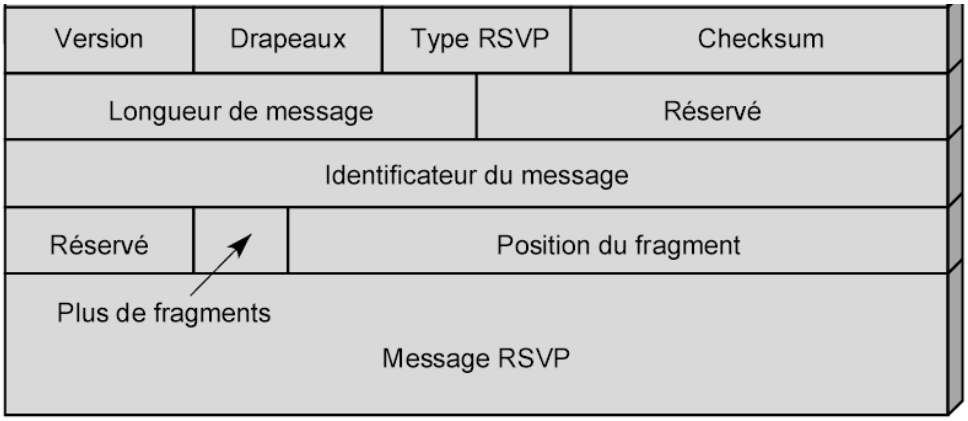
RSVP est un protocole de signalisation, qui a pour but d'avertir les nœuds intermédiaires de l'arrivée d'un flot correspondant à des qualités de service déterminées.

Ce protocole garantit les taches suivantes ;

-Utilisé par les applications temps réel pour réserver les ressources nécessaires au niveau des routeurs situés le long du chemin de transmission.

-Une règle de Contrôle (Policy Control) détermine si l'utilisateur à la permission administrative de faire de la réservation.

-Le contrôle d'admission (Admission Control) détermine si le nœud à suffisamment de ressource pour fournir la QoS demandée.



Le format du RSVP

Les champs du protocole RSVP

Outre deux champs réservés, le paquet RSVP contient les huit champs suivants :

• Le premier champ indique le numéro de la version en cours de RSVP.

• Les quatre bits Flags (Drapeaux) sont réservés pour une utilisation ultérieure.

• Le type caractérise le message RSVP. Actuellement, deux types sont les plus utilisés :

Le message de chemin et le message de réservation.

Les valeurs qui ont été retenues pour ce champ sont les suivantes :

Path: envoyé par la source pour indiquer la liste des routeurs du chemin suivi par les données;

Resv: demande de réservation;

PathErr: message d'erreur concernant le chemin;

ResvErr: message d'erreur de demande de réservation;

PathTear: indique aux routeurs d'annuler les états concernant la route;

ResvTear: indique aux routeurs d'annuler les états de réservation (fin de session);

ResvConf (optionnel): message de confirmation envoyé par le routeur au demandeur de la réservation;

• Le champ Cheksum permet de détecter des erreurs sur le paquet RSVP.

• La longueur du message est ensuite indiquée sur 2 octets.

• Un premier champ est réservé aux extensions ultérieures.

• La zone Identificateur du message contient une valeur commune à l'ensemble des fragments d'un même message.

• Un champ est réservé pour des extensions ultérieures.

• Le bit Plus du fragment indique que le fragment n'est pas le dernier. Un zéro est mis dans ce champ pour le dernier fragment.

• Le champ Position du fragment indique l'emplacement du fragment dans le message.

La partie Message RSVP. regroupe une série d'objets. Chaque objet se présente de la même façon, avec un champ Longueur de l'objet, sur 2 octets, puis le numéro de l'objet, sur 1 octet, qui détermine l'objet, et enfin 1 octet pour indiquer le type de l'objet.

***Session multimédia « temps réel »**

1-réservation de ressources pour l'établissement de la session (RsvP).

2-transmission des données dans des paquets (RTP).

3-contrôle de la qualité de la session (débit, gigue, perte) par des paquets (RTCP).