



# Qualité de service dans les réseaux IP

M. Coupechoux, Ph. Martins, Ph. Godlewski

octobre 2008

ENST, Département INFRES

# Qualité de service dans les réseaux IP

---

- Introduction
- Le transport de flux temps réels : RTP/RTCP
  - Introduction
  - Présentation de RTP
  - Présentation de RTCP
- La boîte à outils de niveau Réseau
  - Gestion du trafic
  - Gestion des files d'attente
  - Ordonnancement
  - Différentiation de service
- Les mécanismes de couche 2
  - Ethernet
  - VoWLAN
- Conclusion

# Introduction

---

- L'analyse de la qualité vocale montre que les paramètres principaux de qualité de service sont :
  - La bande passante,
  - Le délai,
  - La gigue,
  - La perte des paquets (dé-séquencement, *buffer* de gigue, congestion).
- Les réseaux IP n'ont pas été initialement conçus pour transporter des flux temps réels, la voix étant transportée sur le RTC, or :
  - De nombreuses applications temps réel apparaissent aujourd'hui,
  - La voix a de plus en plus tendance à être transmise sur les réseaux IP,
  - Claire tendance vers l'intégration de services.
- Dans ce cours, on introduit les mécanismes de qualité de service dans les couches OSI suivantes :
  - Transport,
  - Réseau,
  - Liaison.

# Le transport de flux temps réel

## Introduction

---



- L'utilisation de RTP (Real Time Transport Protocol) et de RTCP (Real Time Transport Control Protocol) permet de lutter contre les problèmes liés à la qualité de service et aux réseaux IP.
- **Il faut cependant retenir que RTP et RTCP n'ont pas d'influence sur le comportement du réseau IP et qu'ils ne garantissent pas de qualité de service.**
- RTP et RTCP apportent uniquement des solutions pour transporter des flux et pour superviser la qualité de service associée au transport de ces flux.
- Charge aux participants de mettre fin à la communication si la qualité de service apportée n'est pas satisfaisante.

# Le transport de flux temps réel

## Présentation de RTP

---



- Définitions
- Une session RTP est une association entre plusieurs participants communiquant via RTP.
- Chaque participant de la session utilise au minimum deux ports UDP :
- 1 port RTP (ou plusieurs si plusieurs flux) ;
- 1 port RTCP (port de supervision) par session RTP.
- NB : UDP gère l'intégrité des données (checksum) et la notion de « port ».
- Description de RTP
- Les caractéristiques de RTP sont les suivantes :
  - RTP identifie le type de flux transporté ;
  - RTP contient des informations permettant de réordonner et de synchroniser les flux au niveau du destinataire ;
  - Il peut s'appuyer sur les services d'un réseau IP multicast ;
  - RTP transporte des étiquettes temporelles ;
  - Sécurisation possible par cryptage des données.

# Le transport de flux temps réel

## Présentation de RTP

---



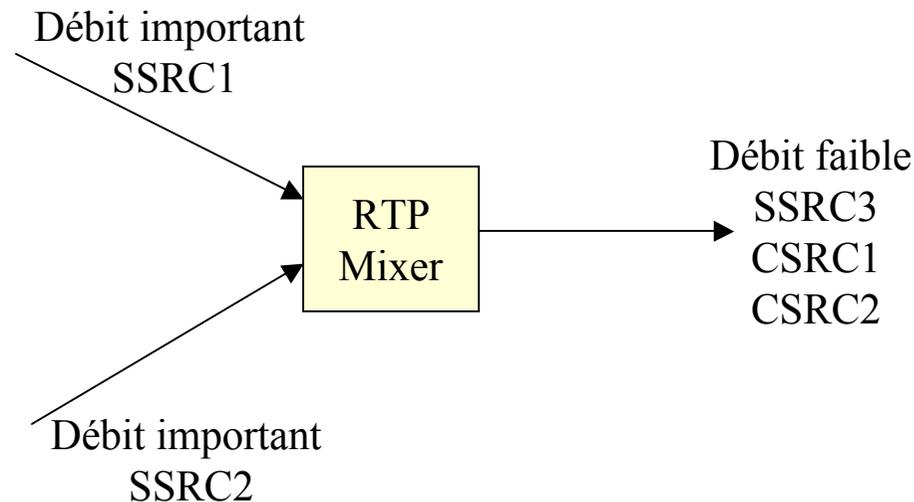
- Scénarios d'usage de RTP :
  - Unicast audio
  - Multicast audio
    - Un port RTP et un port RTCP
    - Les adresses et ports des participants sont diffusés
    - L'encryptage des données est possible
    - L'en-tête des paquets RTP contient le type d'application et l'encodage
    - Il est possible de superviser le taux de perte, les dé-senquencements et les délais
    - Les participants envoient régulièrement des rapports de réception avec leur nom et la qualité du lien
    - A la fin, les participants quittent la session en indiquant la cause du départ.

# Le transport de flux temps réel

## Présentation de RTP

- Audio et vidéo conférence
  - Il y a deux paires de ports RTP/RTCP avec le même nom global CNAME
  - Les flux et les supervisions sont indépendants
  - La synchronisation est possible grâce aux informations temporelles transportées par RTCP
  - Il n'est pas recommandé de mixer des flux RTP

- Mixers



# Le transport de flux temps réel

## Présentation de RTP

---



- Contenu du paquet RTP
- **Champ numéro de séquence** (16 bits) : incrémenté à chaque nouveau paquet RTP, le premier numéro est choisi de manière aléatoire.
- **Marqueur temporel** (32 bits) = instant d'échantillonnage du premier octet de données dans le paquet RTP en provenance de la source (numérotation différente d'un flux à l'autre). Permet la synchronisation et la mesure de la gigue.
  - Définition propre à un flux
  - Incrémenté par exemple à chaque instant d'échantillonnage
  - Pour faire le lien avec l'horloge réelle, on a besoin des informations transportées par RTCP
- **Champ type de données transportées** (7bits)
  - Audio
    - PT = 0 PCM loi  $\mu$ , PT = 8 PCM loi A
    - PT = 9 G.722, PT = 4 G.723, ...
  - Vidéo
    - PT = 34 H.263, PT = 31 H.261

# Le transport de flux temps réel

## Présentation de RTP

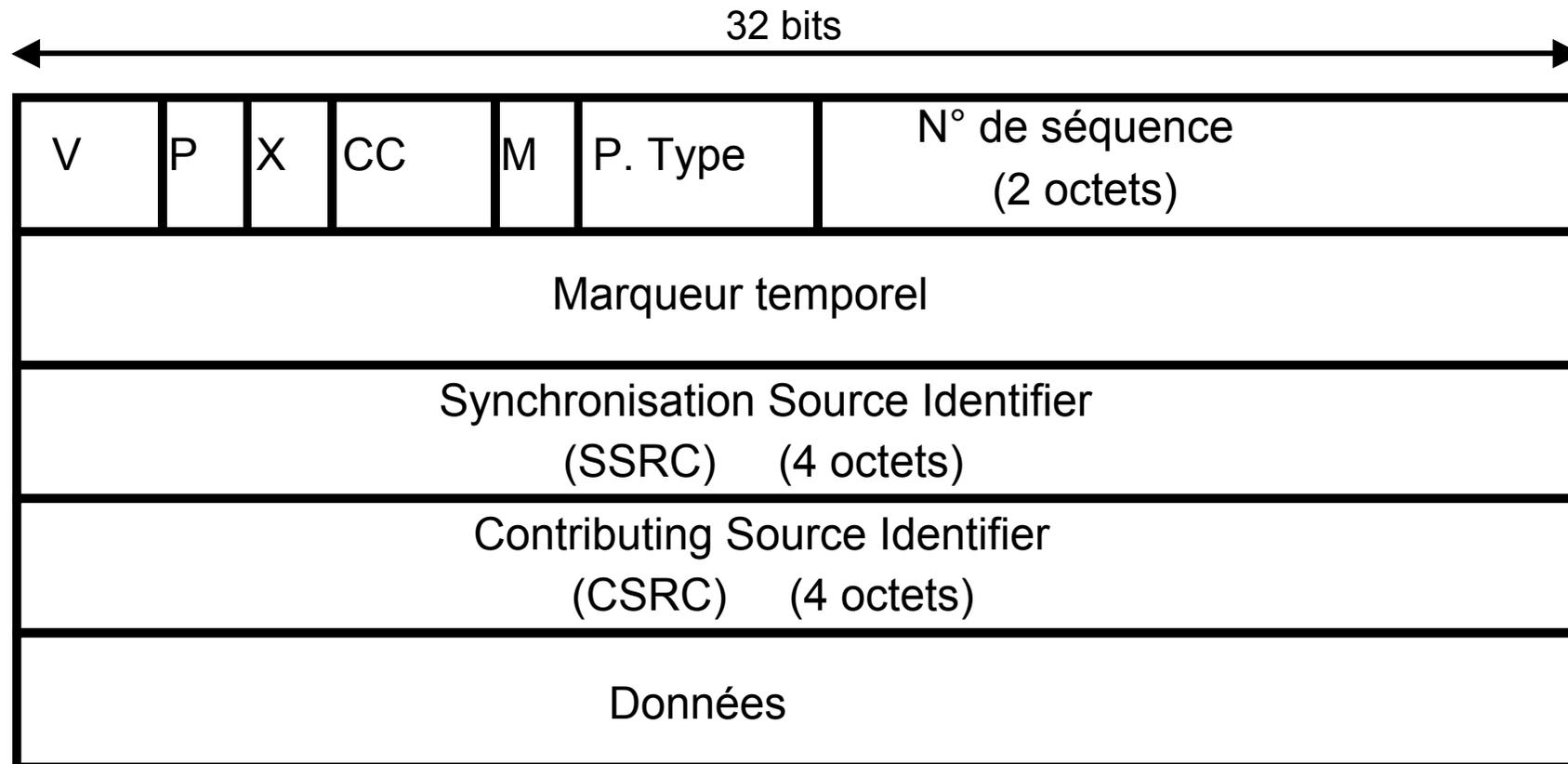
---



- **Champ SSRC** (Synchronisation Source Identifier) identifie la source du flux RTP.
  - 32 bits indépendants de l'adresse réseau
  - Exemples : micro, caméra, mixer
  - Peut-être modifié en cas de conflit ou au redémarrage de l'application
  - Choisi aléatoirement
  - Multimedia : on choisit des SSRC différents, le lien est fait par RTCP (CNAME)
- **Champ CSRC** (Contributing Source) permet de multiplexer plusieurs sources RTP en un seul flux RTP (liste de SSRC).
  - Identifiant d'une source qui a contribué à un flux mixé.
  - Fonction non utilisée par SIP et H.323.

# Le transport de flux temps réel

## Présentation de RTP



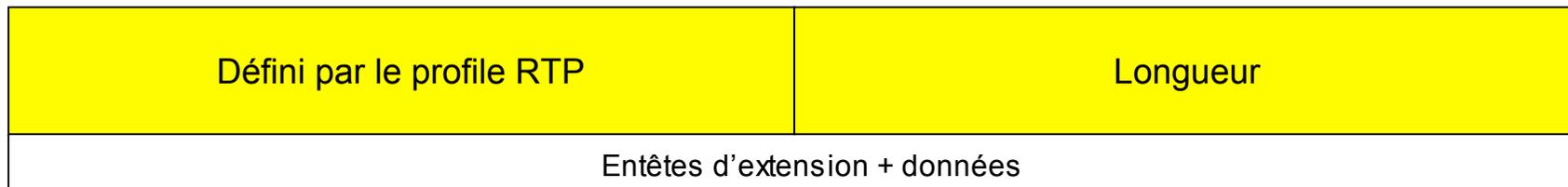
Contenu d'un paquet RTP [source IETF, RFC 1889]

# Le transport de flux temps réel

## Présentation de RTP



- P=1 → *Padding* dans le champ données (nécessaire pour certains cryptages ou pour s'adapter à certaines couche 2)
- CC (4 bits) indique le nombre de champs CSRC (nombre de flux multiplexés).
- M=1 est utilisé par l'application pour identifier des point de repères dans le flux RTP.
- X=1 bit d'extension servant à indiquer la présence d'extensions après l'entête CSRC (si présente). Permet de définir de nouveaux formats d'en-tête.



Format générales des extensions RTP [1, page 86]

- V=2 version du protocole (sur deux bits).

# Le transport de flux temps réel

## Présentation de RTCP

---



- Description générale de RTCP
- RTCP est utilisé pour transmettre aux participants d'une session RTP, des informations de supervision (environ un message toutes les 5s).
- Permet au récepteur d'un flux RTP d'envoyer des informations sur la qualité de la transmission reçue :
  - gigue observée ;
  - taux de perte des paquets ;
  - taux de dé-séquencement.
- Permet à l'émetteur de plusieurs flux d'envoyer des **informations temporelles** servant à la synchronisation de ces flux au niveau du récepteur (référence temporelle NTP + association entre les marqueurs temporels des paquets RTP issues des différents flux).
- Permet également de transporter des informations sur **l'identité des participants** (noms, adresse email, etc.), leur nombre (adaptation du débit RTCP) et de connaître les correspondances participants/flux RTP.
- Peut permettre à une tierce partie de superviser la qualité sur le réseau sans recevoir les données.

# Le transport de flux temps réel

## Présentation de RTCP

---



- Principaux types de messages RTCP
- Les messages RTCP sont des messages de supervision et d'information sur une session RTP. Ils sont « empilables ».
- Plusieurs types de messages ont été définis :
  - Rapports sur la qualité de la réception (**RR ou Receiver Reports**) : uniquement pour les terminaux qui n'envoie pas de données.
  - Envoi d'informations de synchronisation au récepteur + rapports sur la qualité de la réception (**SR Sender Reports**) – terminal faisant office d'émetteur récepteur.
  - **SDES ou Source Description** donne des informations sur les participants d'une session RTP (CNAME, NAME, EMAIL...).
  - **BYE** indique qu'une partie s'est retirée d'une session RTP.
  - APP message utilisé par l'application à des fin spécifiques.

# Le transport de flux temps réel

## Présentation de RTCP

---



- SDES
  - CNAME (Canonical Name) :
    - identifiant constant et unique du participant
    - Multimedia : les flux ont des SSRC différents mais un unique CNAME
    - Moyen de localiser la source
    - CNAME = user@host
- BYE
  - Indique la raison de la fin de session

# Le transport de flux temps réel

## Présentation de RTCP

---



- Format général des messages RTCP RR et SR
- Les messages SR ont le format décrit au transparent suivant :
  - Le champ RC indique le nombre de rapports de récepteurs RR inclus dans le message SR – champ codé sur 5 bits.
  - Le champ longueur indique la longueur du message RTCP en mots de 32 bits (en-tête non compris).
  - Le marqueur temporel correspond à l’instant d’émission du rapport SR au format NTP. Nécessaire pour le calcul des délais d’aller-retour.
  - Le marqueur temporel RTP correspond au même instant d’émission mais par rapport à l’échelle de temps du flux RTP. Permet la synchronisation des media d’un même participant.

# Le transport de flux temps réel

## Présentation de RTCP

V	P	RC (5bits)	PT=200 (SR) ( 7 bits)	Longueur (16 bits)
SSRC de l'émetteur				
Marqueur temporel (8 octets)				
Marqueur temporel RTP				
Nombre de paquets envoyés				
Nombre d'octets envoyés				
SSRC 1 (SSRC de la première source)				
Bloc de réception RR				
SSRC n (SSRC de la source n)				
Bloc de réception RR				

format d'un rapport SR (source [1])

# Le transport de flux temps réel

## Présentation de RTCP

- Les messages RR ont le format suivant :

SSRC de la source	
Taux de perte (8 bits)	Nombre cumulé de paquets perdus
Plus grand numéro de séquence reçu	
Valeur de la gigue	
Dernier marqueur temporel reçu (LSR)	
Délai depuis l'arrivée du dernier marqueur temporel reçu (DLSR)	

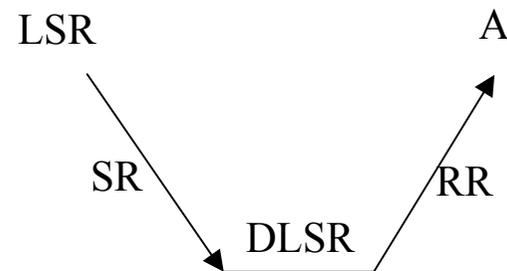
format d'un rapport RR (source [1])

# Le transport de flux temps réel

## Présentation de RTCP

---

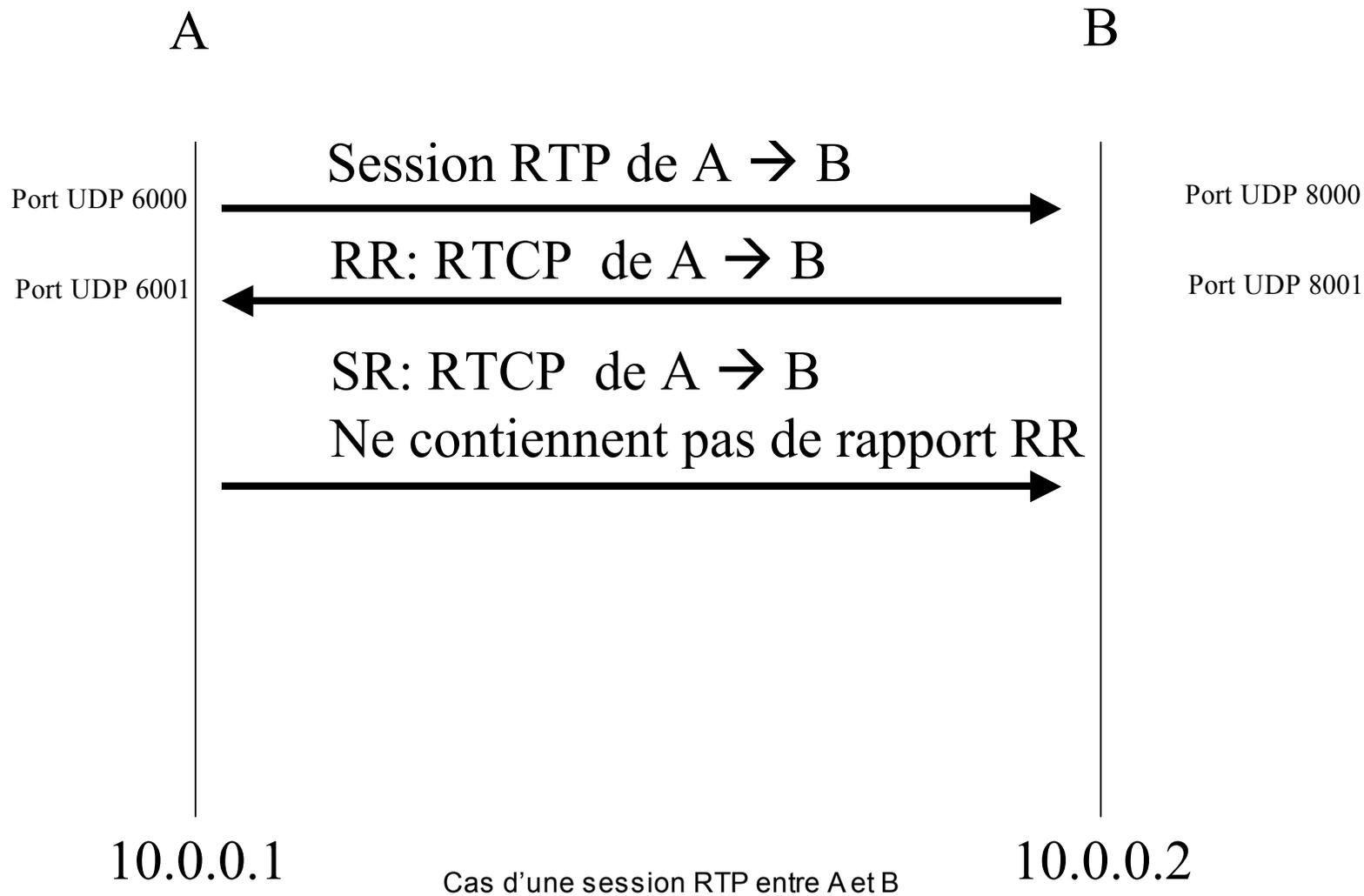
- Analyse des rapports :
  - Emetteur : modifier la transmission, adapter le débit/l'encodage à la bande passante disponible,
  - Récepteur : déterminer si les problèmes sont locaux ou globaux,
  - Tierce partie (administrateur réseau) : estimer les débits de la source, contrôler la qualité de service sur le réseau sans avoir à recevoir les flux de données.
  
- Exemple de calcul du temps d'aller-retour :



$$\text{Round Trip Delay} = A - \text{LSR} - \text{DLSR}$$

# Le transport de flux temps réel

## Synthèse





# La boîte à outils de niveau Réseau

## Introduction

---



- Les réseaux actuels doivent servir des applications ayant des exigences de **qualité de service** diverses.
- Exemples : Voix, vidéo-conférence, imagerie médicale, transferts de fichiers, télévision, navigation Internet, etc.
- Les réseaux IP ont été conçus essentiellement pour transporter des services « au mieux » (*best effort*).
- La nécessité existe donc de développer des algorithmes capables de garantir des qualités de services variées.
- On peut distinguer :
  - La gestion du trafic : comment mettre en forme le trafic pour respecter un contrat de qualité de service ?
  - La gestion des files d'attente : quels paquets éliminer/marquer en cas de congestion ?
  - L'ordonnancement : quel flux servir à chaque instant ?
  - La différenciation de service : comment traiter des flux ayant des exigences de qualité de service différentes ?

- La définition d'un contrat avec QoS nécessite la définition de :
  - Service Level Agreement (SLA) : définit les cibles en termes de QoS pour les types de trafic concernés,
  - Traffic Conditioning Agreement (TCA) : ce sont les conditions d'applications du SLA (les clauses du contrat). Il peut s'agir typiquement de contraintes sur le volume de trafic.
- Le contrat de trafic (SLA+TCA) peut être implémenté en utilisant :
  - Un contrôle d'admission fondé sur le TCA,
  - Une réservation des ressources fondée sur le SLA.

# La boîte à outils de niveau Réseau

## Introduction



- Extrait de SLA :

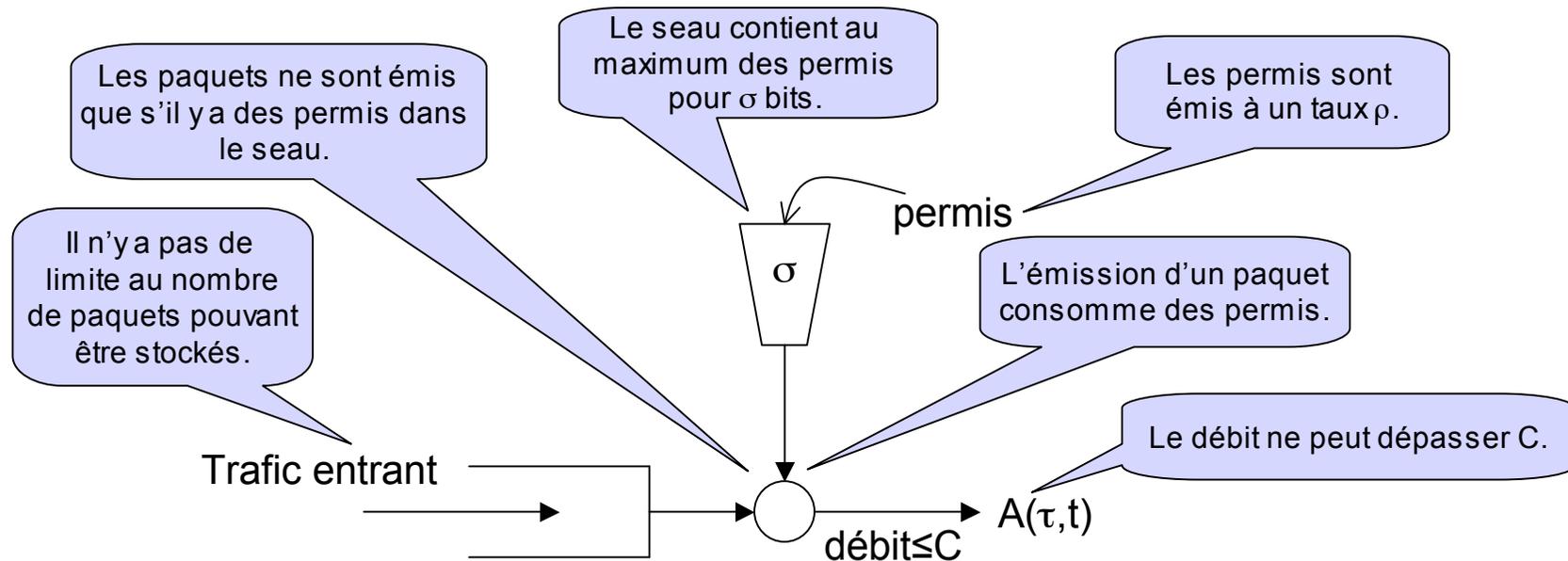
### LATENCY

The average network delay ("Latency") will be measured via roundtrip pings on an ongoing basis every five (5) minutes to adequately determine a consistent average monthly performance level for Latency at the relevant POPs. Latency is calculated as follows:

$$\frac{\Sigma (\text{Roundtrip Delay for relevant POP-POP trunks})}{\text{Total Number of relevant POP-POP trunks}} = \text{Latency}$$

Region	Goal	Actual Latency = Remedy		
<b>North America</b>				
Intra U.S.	50 ms	51 – 60 ms = 10% of MRC	61 – 80 ms = 25% of MRC	Greater than 80 ms = 50% of MRC
Intra U.S.- Off Net	95 ms	96 – 105 ms = 10 % of MRC	106 – 115 ms = 25% of MRC	Greater than 115 ms = 50% of MRC
Intra Canada	65 ms		Greater than 65 ms = 10% of MRC	
Canada to U.S.	90 ms		Greater than 90 ms = 10% of MRC	
Intra Mexico	90 ms		Greater than 90 ms = 10% of MRC	
Mexico to U.S	90 ms		Greater than 90 ms = 10% of MRC	
Puerto Rico to U.S.	135 ms		Greater than 135 ms = 10% of MRC	

- Exemple de mise en forme/conditionnement du trafic : « le seau percé » (*leaky bucket*)



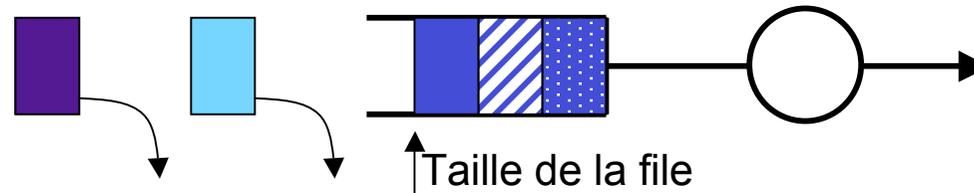
- Le débit moyen est contrôlé avec  $\rho$ , le débit pic avec  $C$ , la sporadicité avec  $\sigma$  et  $C$ . Le paramètre  $\sigma$  est la taille maximale d'une salve (*burst*).
- On dit que le trafic est contraint par un mécanisme de « *leaky bucket* ».

$$A(t_1, t_2) \leq \min \left\{ (t_2 - t_1)C, \sigma + \rho(t_2 - t_1) \right\}$$

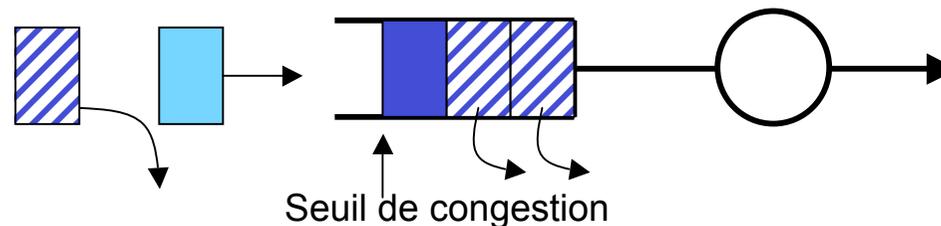
# La boîte à outils de niveau Réseau

## Gestion des files d'attente

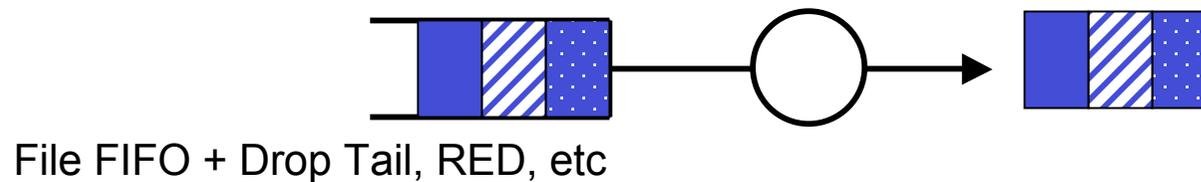
- **But** de la gestion des files (*buffer management*) : sélectionner les paquets à supprimer en cas de congestion (la mémoire est pleine).
- **Drop Tail** : supprime les derniers paquets arrivés.
  - Implémentation très simple.
  - Problème : plusieurs flux TCP peuvent être impactés et vont réduire leur fenêtre d'émission (*slow start*) → oscillations possibles des débits.



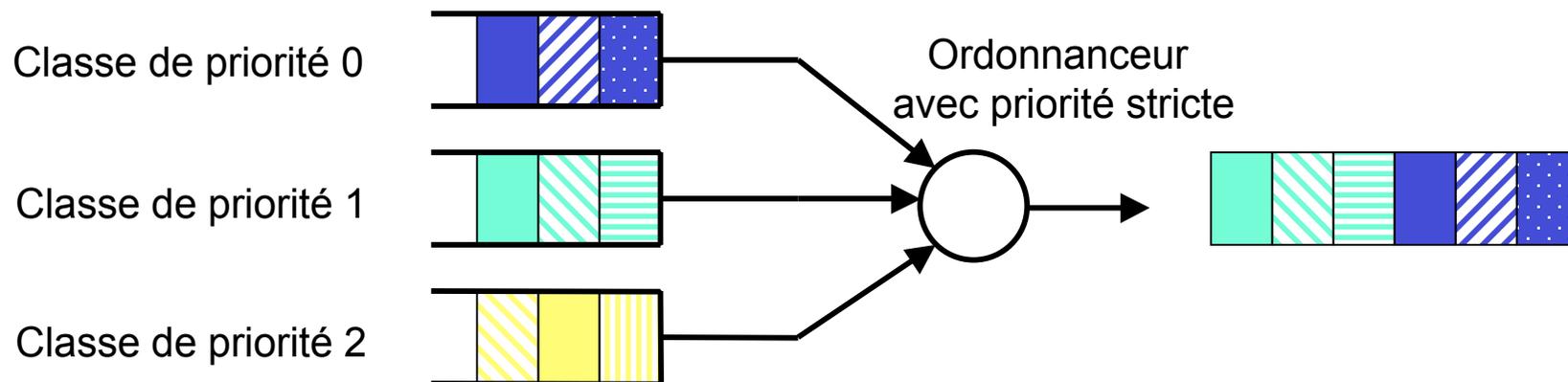
- **Selective Discard** : seuls certains paquets (éligibles) sont supprimés.
- **RED** (Random Early Detection) : entre le seuil de congestion et la limite de la file, les paquets sont supprimés avec une probabilité croissante.



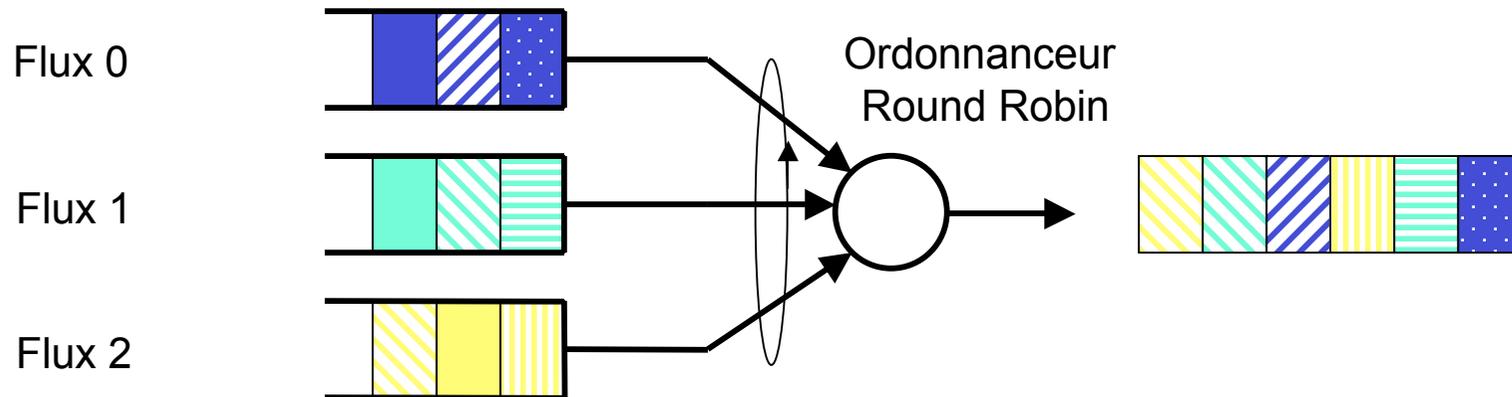
- **FIFO (*First In First Out*)** est l'ordonnanceur le plus simple : les paquets sont servis dans l'ordre de leur arrivée. FIFO peut être associé à différents algorithmes de gestion des files d'attente, par exemple RED.



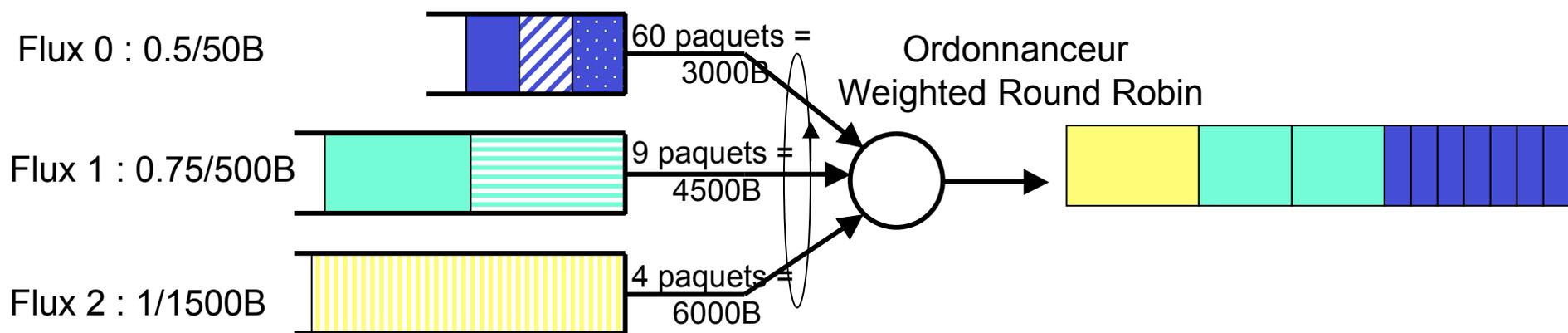
- **Priorité stricte** : on associe une file à chaque classe et on sert les classes de plus grande priorité en premier.



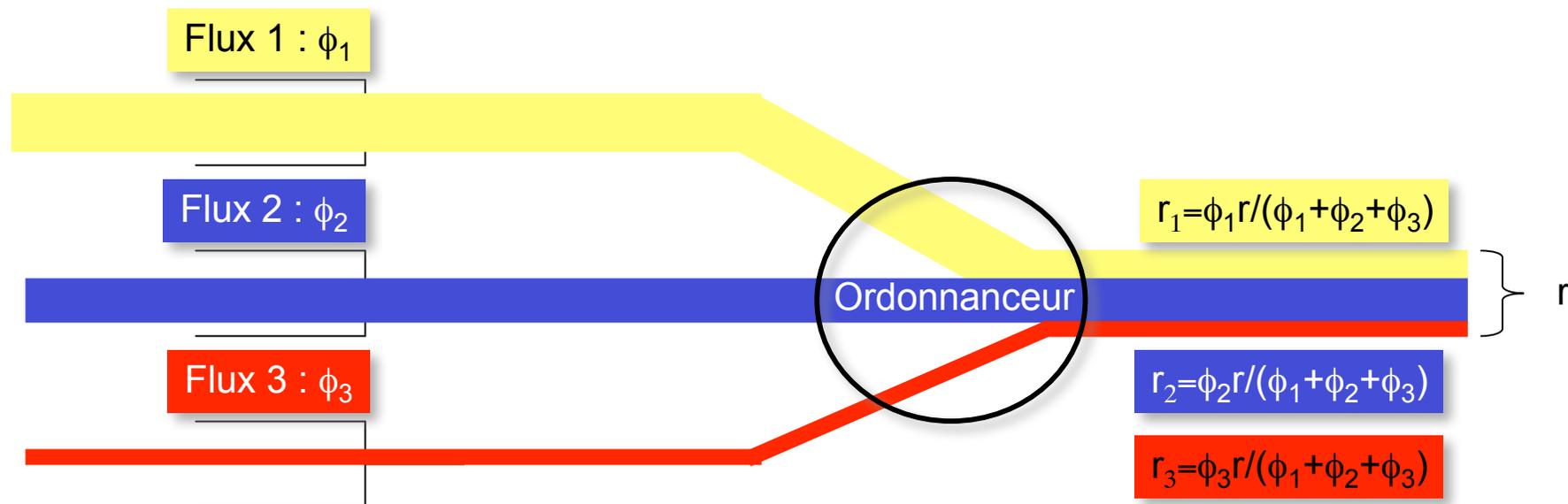
- **Round Robin (RR)** : les flux sont servis tour à tour.



- **Weighted Round Robin (WRR)** : l'ordonnanceur sert un nombre de paquet proportionnel au poids de chaque flux et prend en compte la taille des paquets.



- **GPS (Generalized Processor Sharing)** : l'ordonnanceur équitable.
- **Intuitivement**, un ordonnanceur est équitable s'il alloue la ressource disponible de manière proportionnelle au poids de chaque flux.
- Principe du GPS illustré : le modèle fluide.



# La boîte à outils de niveau Réseau

## Ordonnancement

---

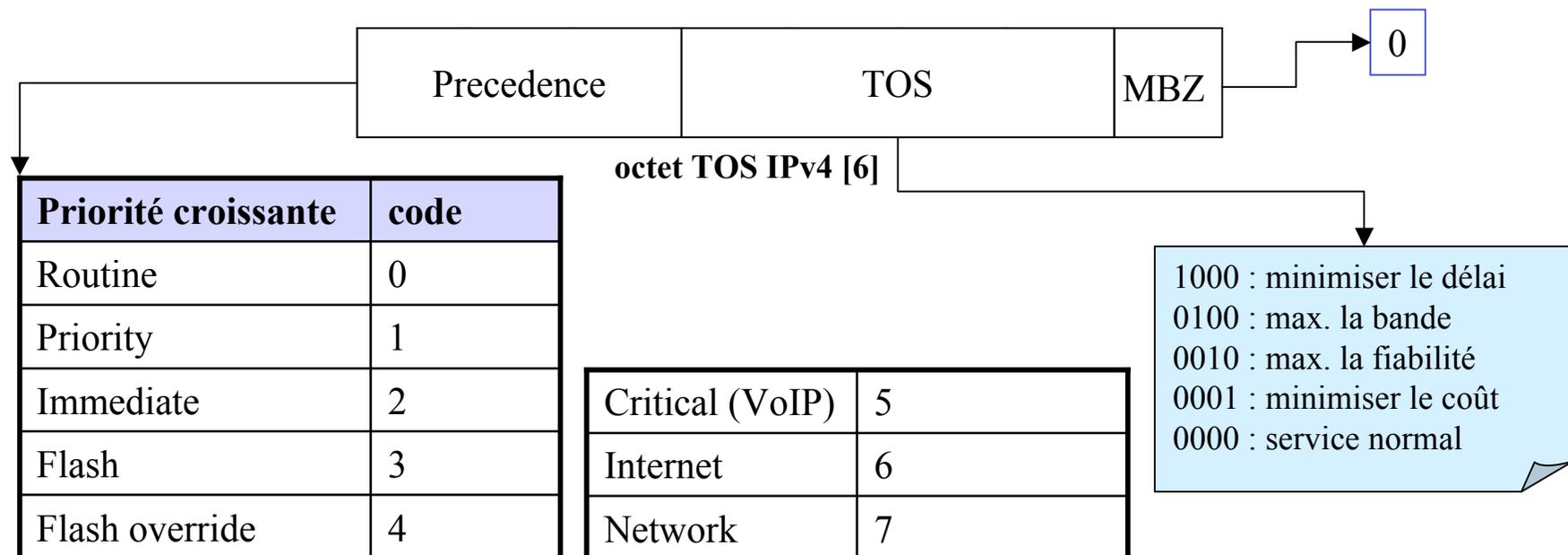


- Intérêts de GPS :
  - ordonnanceur parfaitement équitable (référence) ;
  - pour une source contrôlée par un sceau percé, on peut borner le délai dans le routeur, et, par extension, de bout en bout.
- Inconvénient de GPS :
  - le modèle fluide n'est pas réaliste : dans un réseau de **paquets**, une seule connexion peut être servie à la fois et un paquet doit être transmis entièrement avant qu'un autre puisse l'être.
- **WFQ** (Weighted Fair Queueing ou PGPS pour Packet-by-packet GPS) est une approximation de GPS pour les réseaux de paquets.
  - les paquets sont servis par ordre croissant de date de départ sous GPS.

# La boîte à outils de niveau Réseau

## Différentiation de service

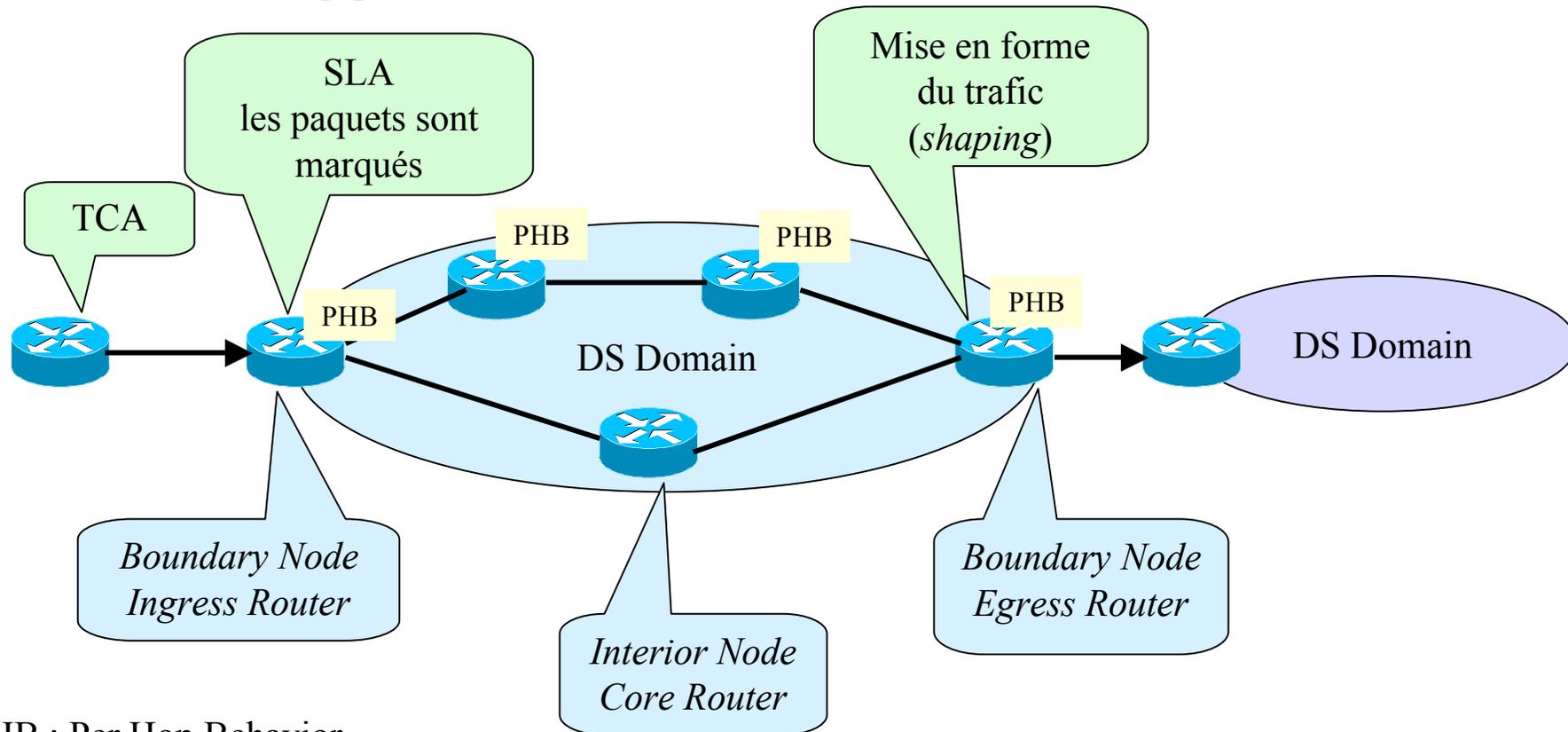
- **Octet TOS d'IPv4** : il contient des indications sur la manière dont doit être traité le paquet IP du point de vue de la qualité de service.
- Il contient les champs suivants [1][5][6] :
  - « Precedence » (3 bits) : priorité donné au paquet ;
  - « Champs TOS » (4 bits) : permet, à l'intérieur d'une priorité, d'arbitrer entre délai, débit, fiabilité et coût ;
  - « Must Be Zero » : 1 bit réservé.



# La boîte à outils de niveau Réseau

## Différentiation de service

- **Differentiated Services (DiffServ)** : c'est une architecture de qualité de service pour réseau IP, i.e., un cadre général pour l'implémentation de mécanismes de QoS.
- **Architecture [7]** :



PHB : Per Hop Behavior

- **Marquage :**
  - L'octet TOS d'IPv4 (resp. Traffic Class d'IPv6) est réutilisé pour le champ DS (*DSCoDePoint*) sur 6 bits ; 2 bits sont réservés. 64 niveaux de priorité.
  - DiffServ traite (et marque) des agrégats de flux et non des micro-flux.
  - A un champ DS est associé un PHB (association valable par domaine).
- **Per Hop Behavior :** comportement d'un nœud vis-à-vis des paquets marqués avec une même valeur du champ DS. On distingue 3 groupes :
  - *Default PHB (DE)* : service « au mieux » (*best effort*), la transmission est fondée sur les ressources disponibles.
  - *Assured Forwarding (AF)* : définition de 4 classes, chacune ayant 3 sous-classes avec différentes priorités d'élimination des paquets (*drop precedence*).
  - *Expedited Forwarding (EF)* : classe « premium », faible délai, faible gigue, bande passante assurée (VoIP). « Ligne louée virtuelle ».
  - La RFC ne précise pas comment il faut implémenter les PHB, cela dépend du vendeur d'équipements et des configurations de l'opérateur.

# La boîte à outils de niveau Réseau

## Différentiation de service

---

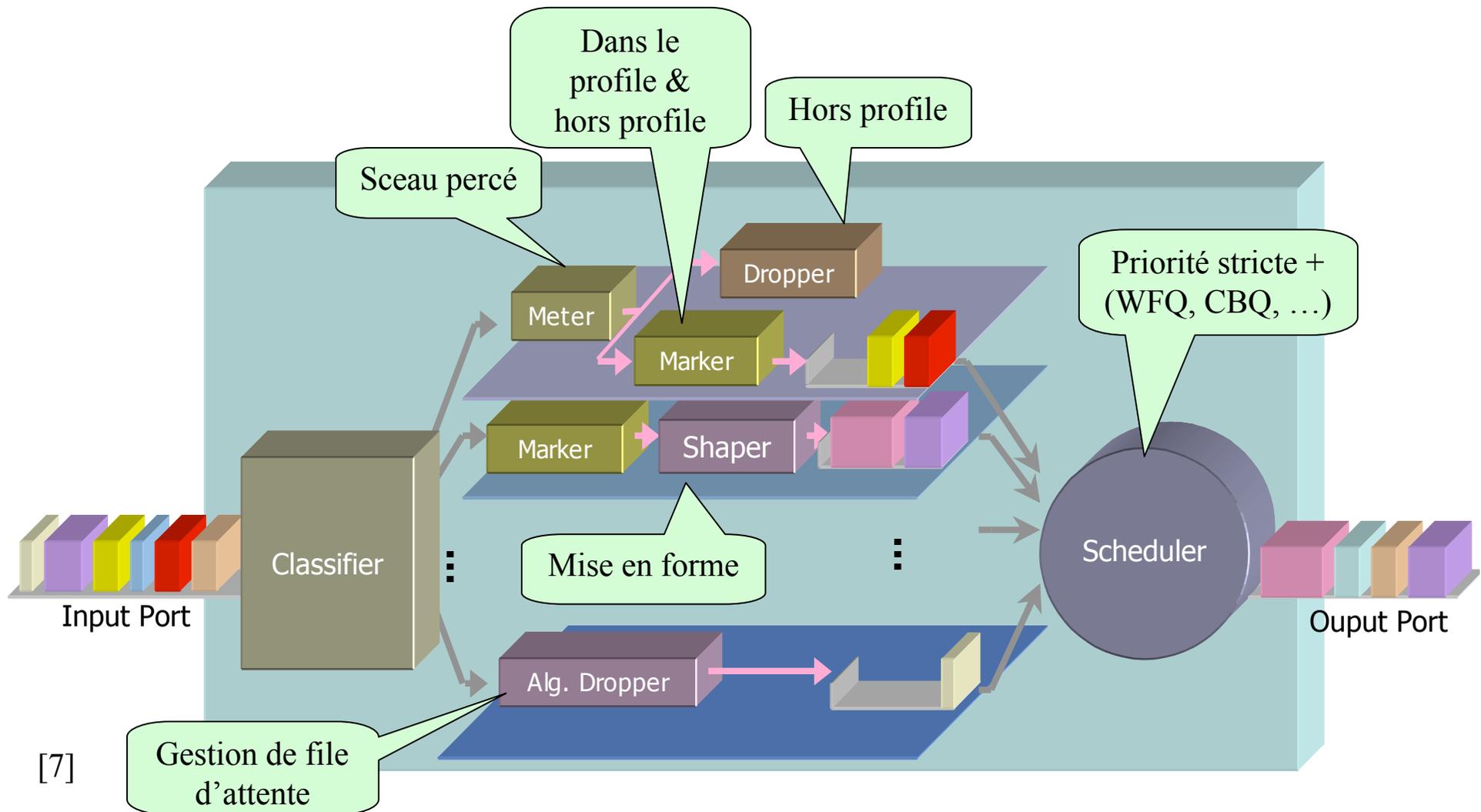


- Exemples de marquage :
  - VoIP contrôle : TOS=3, DSCP=AF3 drop low
  - VoIP données : TOS=5, DSCP=EF
  - Vidéo contrôle : TOS=3, DSCP=AF3 drop low
  - Vidéo données : TOS=4, DSCP=AF4 drop low
  - Data : TOS=0-2, DSCP=DE

# La boîte à outils de niveau Réseau

## Différentiation de service

- Architecture d'un nœud :



# Les mécanismes de couche 2

## Ethernet

---



- Principales normes :
  - IEEE 802.1p : priorités au niveau 2 définies sur 3 bits ;
  - IEEE 802.1Q : les *Virtual Local Area Networks* (VLAN) ;
  - IEEE 802.1D : les ponts Ethernet.
  
- VLAN permettent :
  - de créer des domaines de diffusion séparés,
  - de sécuriser les flux entre VLANs,
  - de créer des groupes de travail indépendants de l'infrastructure physique.  
Exemple : 1 VLAN/VoIP, 1 VLAN/Données, 1 VLAN/Administration.
  
- **802.1Q** insère dans l'en-tête MAC un champ de 4 octets :
  - Identification du protocole : 2 octets (8100),
  - *User Priority* (UP) : 3 bits, la voix peut être associé à la classe 5 (*delay critical*),
  - Canonical Format Identifier (CFI) : 1 bit (interconnexion avec Token Ring),
  - VLAN Id : 12 bits, identifiant du VLAN.

- **Les problématiques** liées à VoWLAN :
  - **La qualité du lien radio** : mieux vaut dimensionner le réseau VoWLAN de manière à avoir partout un très bon niveau de signal (SNR > 25 dB),
  - **Les interférences** : imprédictible a priori car la bande 2.4 GHz est sans licence,
  - **Délais importants** dus au CSMA/CA : problème pour l'instant incontournable,
  - **Partage du canal** : séparer la voix et les données ou utiliser 802.11e,
  - **Sécurité** : crypter les données (WPA, 11i, VPN), authentifier, etc,
  - **Mobilité** : le hand over est quasiment impossible,
  - **Economie d'énergie** : mettre en place les mécanismes d'économie d'énergie prévus par la norme.

## Les mécanismes de couche 2

### VoWLAN

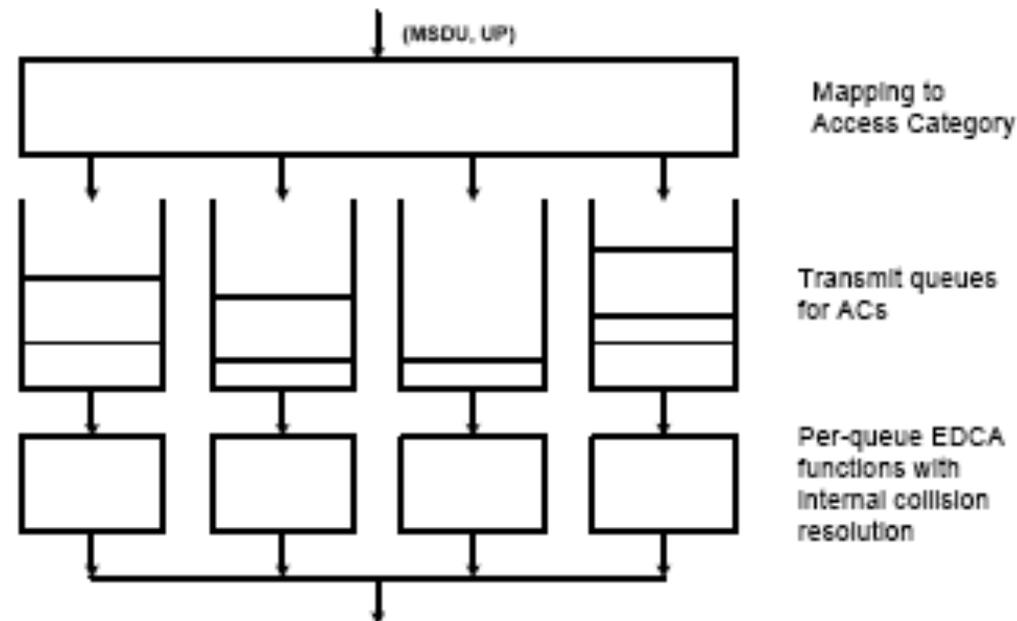
---



- Exemples de capacités en IEEE 802.11b (11 Mbps) [9] :
  - G711 (10 ms) : 5 appels simultanés,
  - GSM EFR (20 ms) : 12 appels,
  - G723 (30 ms) : 18 appels.
  
- Exemples de capacités en IEEE 802.11a/g (54 Mbps) [10] :
  - G711 (20 ms) : 47 appels,
  - G729 (20 ms) : 53 appels,
  - G723 (30 ms) : 80 appels,
  - iLBC (30 ms) : 78 appels.
  
- Mais : ces valeurs décroissent avec la distance au point d'accès.

- **Principes de IEEE 802.11e :**

- 4 classes de services sont disponibles,
- Chaque file d'attente se comporte comme une station WLAN à l'intérieur d'une station 802.11e,
- Les classes de priorité élevée ont accès privilégié au canal via un choix de paramètres CSMA/CA associé.



# Conclusion

---

- Dans ce cours, on a vu :
  - Au niveau transport, RTP/RTCP permettent de transporter des flux temps réel de bout en bout mais ne fournissent pas de mécanismes de QoS.
  - Au niveau réseau, on dispose de nombreux mécanismes qui sont mis en œuvre dans l'architecture DiffServ.
  - Au niveau liaison, on effectue de la différenciation de service assez simple via 802.1p/802.1Q sur Ethernet ou IEEE 802.11e sur WLAN.
- Ces points n'ont pas été abordés :
  - IntServ/RSVP : peu utilisé car cette architecture passe difficilement à l'échelle,
  - MPLS : utilisé dans le cœur des réseaux.

# Références

---

- [1] La voix sur IP, Oliver Hersent, David Gurle, Jean Pierre Petit, éditions DUNOD.
- [2] IETF RFC 1889, Description du protocole RTP/RTCP.
- [3] Ph. Martins, Transport de flux temps réel sur réseaux IP : RTP/RTCP, cours ENST.
- [4] R. Casellas, G. Hébuterne, D. Kofman, M. Marot, J.L. Rougier, « Scheduling and Switching Architecture », ENST, rapport interne, 2004.
- [5] D. D. Chowdhury, « Unified IP Internet-working », Springer, 2001.
- [6] IETF RFC 1349, Type of Service Byte.
- [7] S. Beker, D. Kofman, G. Le Grand, J. L. Rougier, Quality of Service in IP Networks, cours ENST.
- [8] T. Wallingford, Switching to VoIP, O'Reilly, 2005.
- [9] M. Coupechoux, L. Brignol et V. Kumar, « Voice over IEEE 802.11b Capacity », ITCSS Conference, 2004.
- [10] L. X. Cai et al., « Voice Capacity Analysis of WLAN with Unbalanced Traffic », IEEE Trans. On Vehicular Technology, Mai 2006.