

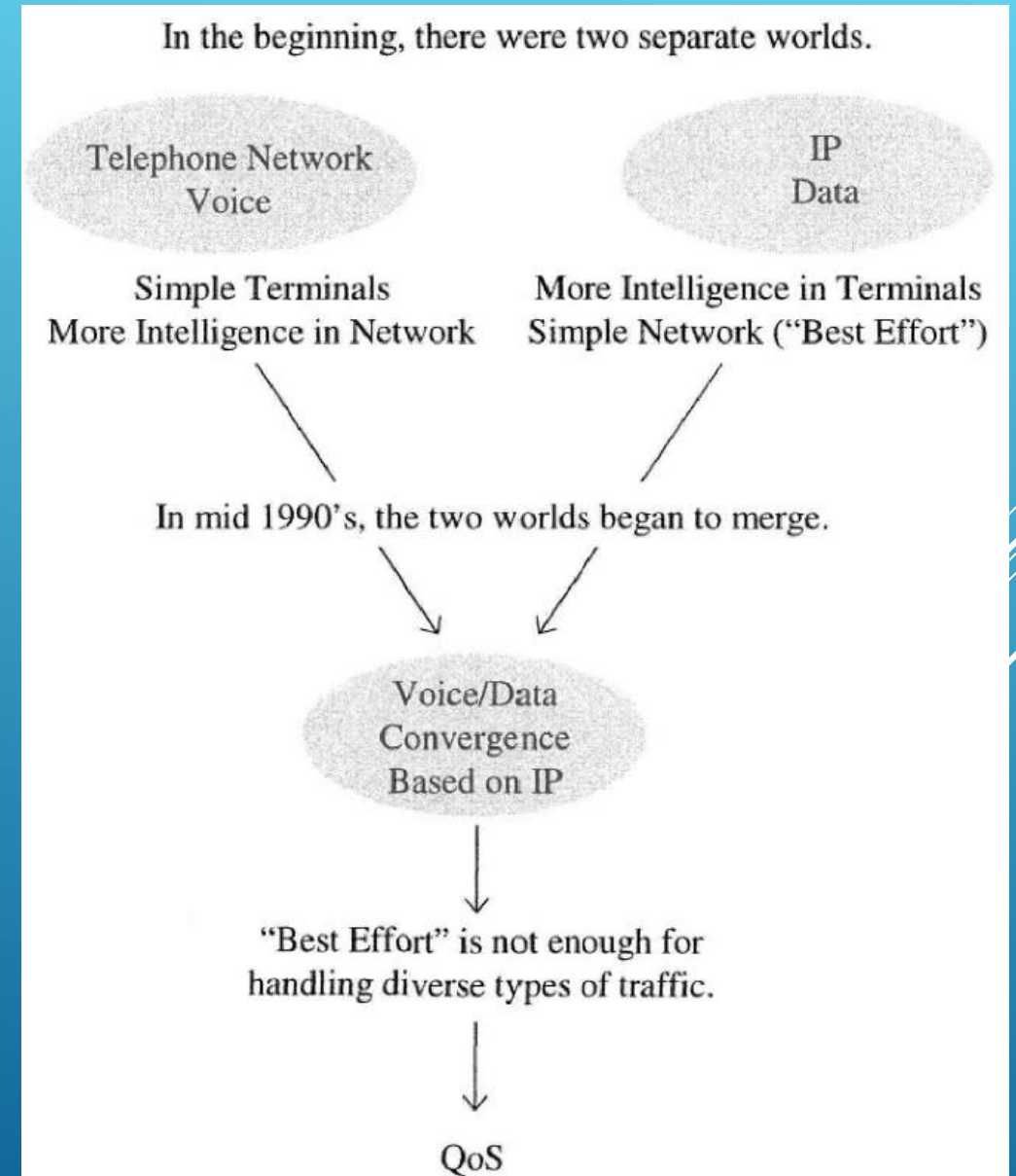


LA QUALITÉ DE SERVICE (QOS)

- ▶ Introduction/Problématique
- ▶ Mécanismes QoS
- ▶ Architectures QoS
 - ▶ DiffServ
 - ▶ IntServ
- ▶ Implémentation des Mécanismes QoS

BESOIN EN QoS

► Exemple : convergence Téléphonie/données



HISTORIQUE

1976 : recherches préliminaires sur Arpanet

- ▶ Le Department of Defense (DoD) américain décide de migrer le réseau Arpanet, ancêtre d'Internet, vers TCP/IP, et teste les premiers mécanismes de qualité de service sur le réseau.

1995 : création du protocole RSVP

- ▶ Développement et mise au point de RSVP (dont Intserv fait partie), projet conduit par Xerox PARC, le MIT ainsi que l'Information Sciences Institute et le Computer Science Department, deux entités de l'université de Californie.

1997 : Diffserv comble les lacunes de l'architecture IP

- ▶ Le groupe de travail Diffserv au sein de l'IETF revisite l'entête du paquet IPv4 et réutilise le champ dédié à la qualification des flux transportés.

1998 : MPLS rénove l'approche de la QoS

- ▶ Poussés par Cisco, les équipementiers et opérateurs se rallient au sein de l'IETF pour standardiser la procédure de routage MPLS. À ce sujet, de nombreux travaux sont encore en cours.

DÉFINITION DE LA QoS

Selon la recommandation E.800 du ITU, la qualité de service correspond à :

« l'effet général de la performance d'un service qui détermine le degré de satisfaction d'un utilisateur du service ».

Autre définition :

« la qualité de service correspond à tous les mécanismes d'un réseau qui permettent de partager équitablement et selon les besoins requis des applications, toutes les ressources offertes, de manière à offrir, autant que possible, à chaque utilisateur la qualité dont il a besoin. »

MÉTRIQUES DE PERFORMANCE

- ▶ Les métriques de performance constituent des paramètres objectifs traduisant les besoins des utilisateurs et la qualité de service demandée.
- ▶ Ces paramètres, étant mesurables, permettent d'évaluer les performance du réseau.
- ▶ Les paramètres les plus utilisées dans le cadre des réseau :
 - ▶ Débit (Throughput)
 - ▶ Latence (Latency)
 - ▶ Gigue (Jitter)
 - ▶ Taux de perte (PLR)
 - ▶ Taux d'erreurs (PER)

LATENCE (DÉLAI)

- ▶ Latence ou « délai » est la métrique de performance la plus importante pour les applications interactives. Ce délai est défini comme étant le temps écoulé entre l'envoi d'un paquet par un émetteur et sa réception par le destinataire. Il est appelé le délai de bout en bout ou délai allé simple. Le terme « délai » englobe en réalité trois aspects temporels différents :
 - ▶ le délai de propagation:
déterminé par la distance physique qui sépare la source de la destination : $t_p = D/V_p$;
(Exemple délai satellite - lien YT « ICI »)
 - ▶ le délai de transmission :
dépendant de la taille des flots. Ce paramètre est aussi étroitement lié à l'utilisation du réseau et au partage de la bande passante disponible ;
 - ▶ le délai d'attente et de traitement
des paquets à l'intérieur des dispositifs intermédiaires du réseau tels que les routeurs ou les commutateurs. Il est déterminé par la charge du réseau, ainsi que les politiques de traitement de l'information dans les routeurs pour obtenir une fluidité maximale de l'écoulement de l'information.

Noter qu'il y a d'autres facteurs qui peuvent influencer sur le délai (voir l'exemple du slide suivant)

EXEMPLES DE DÉLAI

Source de délai	Valeur de latence (ms)
Capture de l'échantillant par l'appareil	0.1
Délai d'encodage (algorithme+traitement)	17.5
Délai d'encapsulation/Décapsulation	20
Délai de déplacement vers la file de sortie/délai de file d'attente	0.5
Délai de transmission d'accès au Lien (montant)	10
Délai de transmission sur le réseau	variable
Délai de transmission d'accès au Lien (descendant)	10
De la file d'entré jusqu'à l'application	0.5
Gigue du Tampon	60
Délai de décodage	2
Délai de sortie de l'appareil de destination	0.5

MESURE DE LA LATENCE (DÉLAI)

- Ce délai peut être calculé par la formule:

$$\textit{Latence} = T_e + T_p + T_{tr}$$

Avec :

$$T_e (\textit{Temps d'émission ou de transmission}) = \frac{(\textit{Quantité de Données})}{\textit{Débit}}$$

$$T_p (\textit{Temps de propagation}) = \frac{\textit{Distance}}{V_{\textit{propagation}}}$$

(exemple : vitesse de l'information dans le cuivre = 273 000 km/s)

T_{tr} : *Temp de traitement* = (Variable!!)

CONSÉQUENCE DE LA LATENCE

- ▶ À cause de la latence, les temps de réponse de certaines applications se trouvent augmentés, ce qui peut s'avérer gênant pour les communications interactives (en téléphonie, on estime qu'un délai de **250 ms** est nettement perceptible et que 500 ms et plus rendent la communication très difficile)
- ▶ D'autre part, si des protocoles comme TCP s'adaptent à la latence, il en résulte cependant une limitation liée à la notion de contrôle de flux par fenêtre glissante. Par exemple, une fenêtre de 64 kOctet sur un réseau qui présente une latence de 250 ms résultera en une connexion TCP au débit maximal de **2 Mbit/s**, indépendamment de la bande passante réellement disponible qui peut être supérieure.

TAXONOMIE DES APPLICATIONS

► Applications temps réel

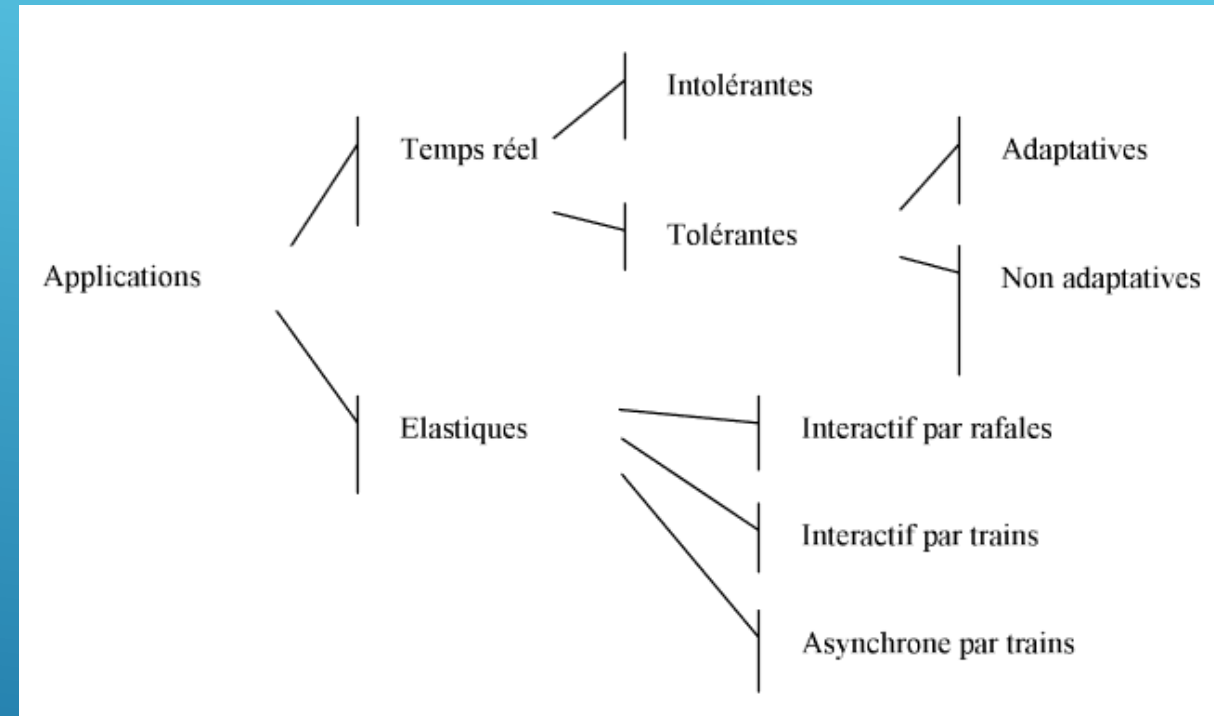
Leur caractéristique est que les données reçues après un certain délai ne sont plus utilisables par l'application réceptrice. Parmi celles-ci, on distingue :

- Applications temps réel intolérantes : pour celles-ci, lorsque des données sont perdues, le service ne peut être rendu (contrôle de procédé, ...)
- Applications temps réel tolérantes : l'application peut supporter une perte de données au prix d'une perte de qualité. Deux comportements de l'application sont distingués :
 - Applications temps réel adaptatives : l'application détecte la perte de données et s'adapte à celle-ci.
 - Applications temps réel non adaptatives : l'application ne détecte pas la perte de données.

► Applications élastiques

Elles peuvent toujours attendre des données arrivant en retard. Elles utilisent celles-ci immédiatement. On distingue trois catégories :

- Interactif par rafales, par ex. Telnet,
- Interactif par trains, par ex. FTP,
- Asynchrone par trains, par ex. mail.



EXEMPLE DE RÉFÉRENCE

- Les chiffres suivants (tirés de la recommandation UIT-T G114) sont donnés à titre indicatif pour préciser les classes de qualité et d'interactivité en fonction du délai de transmission dans une conversation téléphonique.

Classe n°	Délai par sens	Commentaires
1	0 à 150 ms	Acceptable pour la plupart des conversations.
2	150 à 300 ms	Acceptable pour des communications faiblement interactives (voir satellite 250 ms par bond)
3	300 à 700 ms	Devient pratiquement une communication half duplex
4	Au-delà de 700 ms	Inutilisable sans une bonne pratique de la conversation half duplex (militaire)

- ▶ La gigue (jitter en anglais) correspond aux variations de latence des paquets de bout en bout. Elle nous renseigne sur l'évolution du temps du délai allé simple entre deux machines (i.e. la différence entre le délai maximum et le délai minimum).

TAUX DE PERTE

- ▶ Ce paramètre représente le pourcentage des unités de données qui ne peuvent pas atteindre leur destination dans un intervalle de temps spécifique. Cette perte peut être le résultat d'un **rejet de paquets** lorsque les ressources sont saturées (mémoire saturée d'un routeur) ou d'un dépassement d'échéance sachant que pour une application temps réel un paquet arrivant au delà de son échéance ne fournira aucune information utile à l'application. Mais se traduit par une mauvaise réactualisation de l'image vidéo, des ruptures au niveau de la conversation et une hachure possible de la parole.
- ▶ Des pertes de paquets peuvent être dues à des **erreurs d'intégrité** sur les données. Cependant, dans les réseaux **filaire**s actuels où la qualité des transmissions est très bonne, cette cause est marginale. Par contre, dans le cas de liens **sans fil**, la nature du canal de communication influe fortement sur les probabilités de pertes.

EXEMPLE DE SITE POUR LE TESTE DES PARAMÈTRES QOS

- ▶ <https://fr.packetlosstest.com>

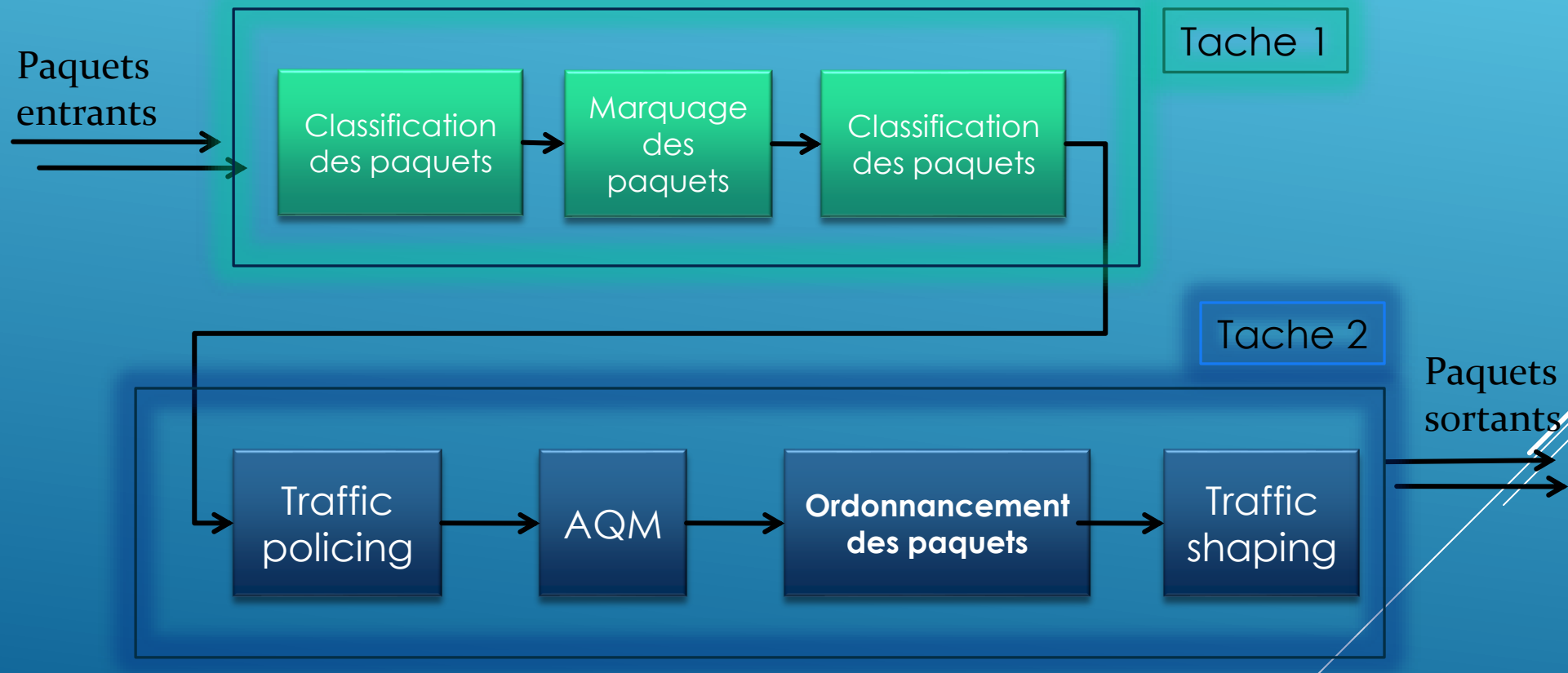
- Le tableau suivant donne le niveau d'exigence de quelques applications :

Application	Taux erreurs	Délai	Gigue	débit
Messagerie électronique	élevée	faible	faible	faible
Transfert de fichiers	élevée	faible	faible	moyenne
Accès Web	élevée	moyenne	faible	moyenne
Accès distant	élevée	moyenne	moyenne	faible
Audio sur demande	faible	faible	élevée	moyenne
Vidéo sur demande	faible	faible	élevée	élevée
Téléphonie	faible	élevée	élevée	faible
Vidéoconférence	faible	élevée	élevée	élevée

GESTION DE LA QoS

- ▶ **Mécanismes de QoS Internes aux équipements**
- ▶ **Modèles et protocoles de QoS**

CHAINE DE TRAITEMENT



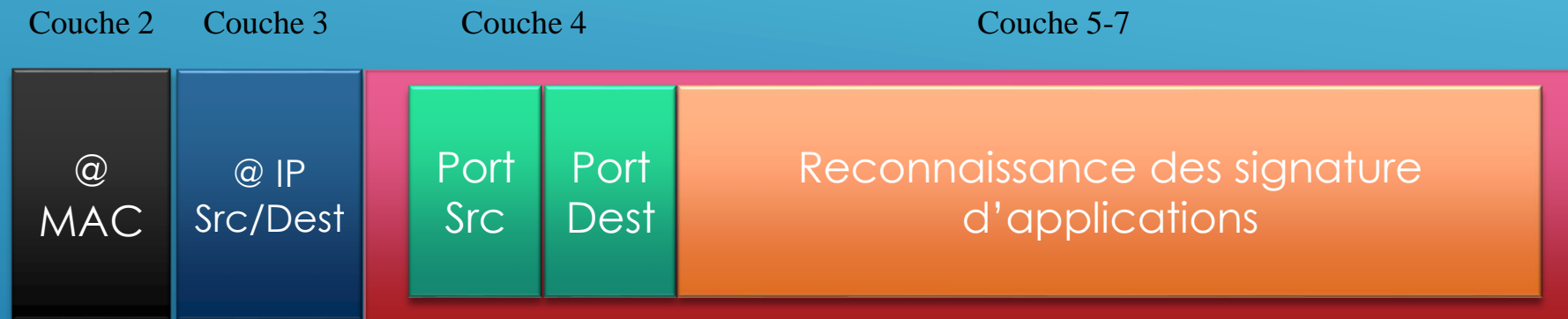
CLASSIFICATION & MARQUAGE



CLASSIFICATION

- ▶ **Examiner un ou plusieurs aspects du paquet afin de savoir ce qu'il portent !!**
- **Pourquoi?**
 - **Pour le bien traiter en fonction des besoin.**
- **Comment traiter?**
 - **Regrouper les paquets dans des groupes spécifiques afin de les traiter différemment!!**

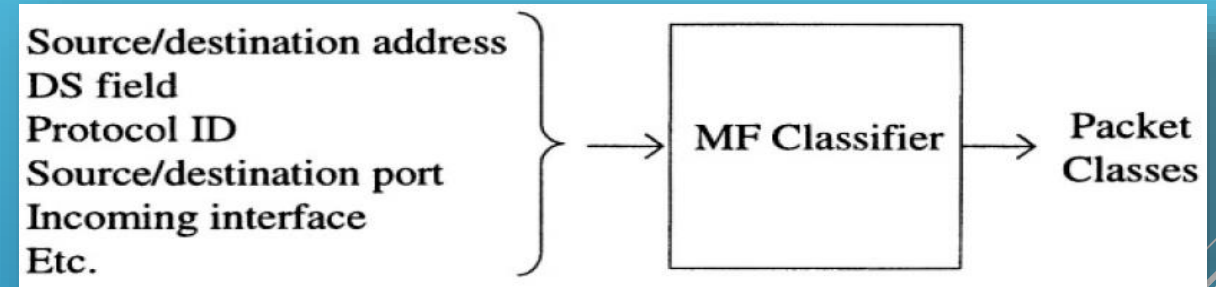
CLASSIFICATION



MÉTHODES DE CLASSIFICATION DES PAQUETS

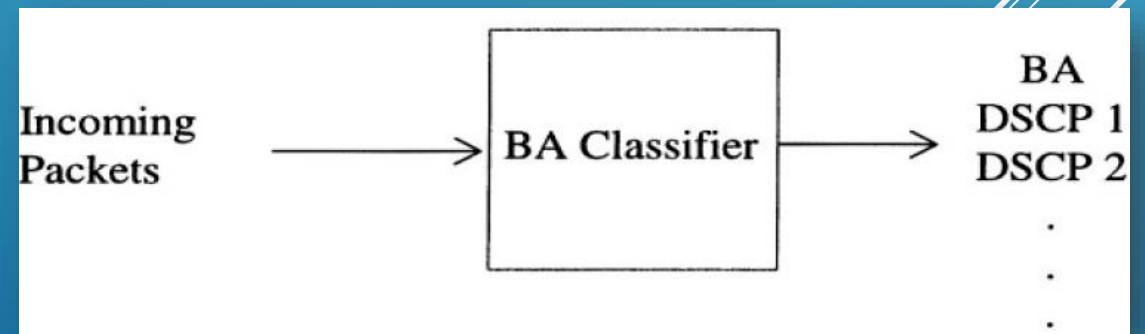
► Multi-Field (MF) classification :

Dans cette méthode, les paquets sont classifiés en se basant sur une combinaison de valeurs d'un ou plusieurs champs des entêtes ou autres paramètres, p.ex., interface d'entrée.



► Behavior Aggregate (BA) classification

Dans ce type de classification, l'équipement de traitement se base uniquement sur le champ DSCP (DiffServ Code Point).



MARQUAGE DES PAQUETS

- Dans le sens général des mots, le marquage des paquets revient en principe à modifier le champ binaire approprié dans l'entête IP/MAC. L'objectif est de spécifier des valeurs pour une éventuelle différenciation d'un type de paquets IP par rapport à un autre. En fait les critères de distinction des paquets peuvent être l'adresse source, l'adresse destination, la combinaison des deux ou d'autres paramètres.

MARQUAGE, EST-IL NÉCESSAIRE ?

... Non !!

SITUATIONS DE MARQUAGE

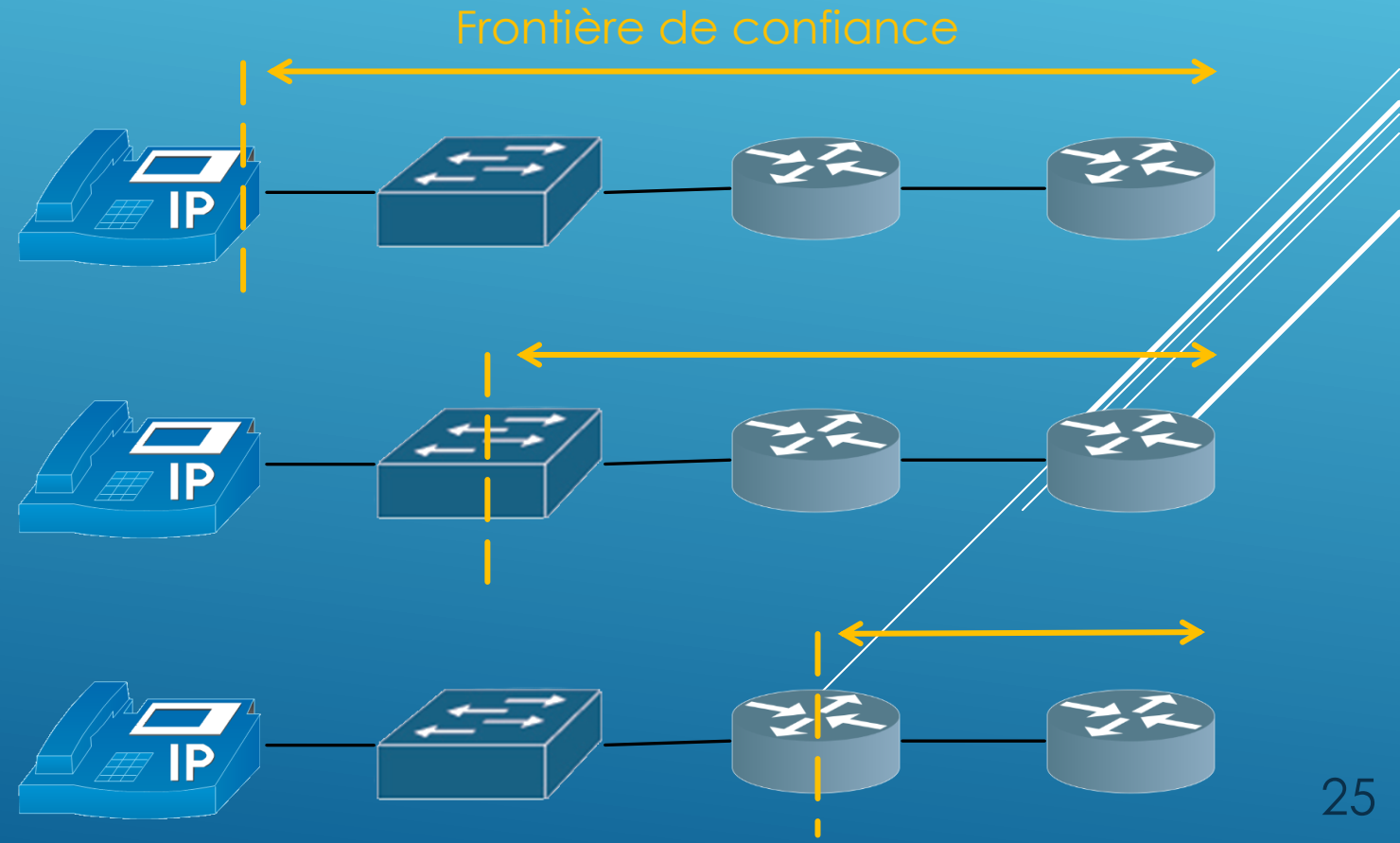
- ▶ Lorsque des paquets entre dans un équipement réseau, trois possibilités de marquage se présente :
 - ▶ Les paquets **ne sont pas marqués**.
 - ▶ Les paquets sont **marqués**, mais ce marquage **n'est pas approuvé**.
 - ▶ Les paquets sont **marqués** et ce marquage est **approuvé**.

FRONTIÈRE DE CONFIANCE

- ▶ Si, par contre, le paquet arrive sans marque, il doit être marqué, si bien sûr le routeur se trouve au bon endroit de marquage imposé par la politique de gestion du réseau. Cet endroit s'appelle «Frontière de confiance » (trust boundary) qui doit être choisi avec soin car tout le reste de la classification peut se baser sur le résultat de ce marquage.

- ▶ Il existe deux propositions :

1. Effectuer le marquage le plus proche possible de la source.
2. Effectuer le marquage près des équipements de transit d'un réseau haut débit (p.ex. FastEthernet) à une liaison faible débit (Liaison série).



RE-MARQUAGE DES PAQUETS

- ▶ Si, par contre, le paquet était déjà marqué, il pourra être re-marqué, par exemple :
 - ▶ Si le paquet est sujet au trafic policing et le résultat de la réglementation montre une **violation des règles** imposées par la politique adoptée.
 - ▶ Autre cause de re-marquage du paquet réside dans la **SLA** (Service Level Agreement) cette notion sera traitée dans une autre section de ce cours) du fait que lorsque le paquet passe d'un domaine DS à un autre il pourra avoir besoin d'être re-marqué afin de satisfaire au contrat de niveau de service « SLA » signée entre les deux domaines.

TYPES DE MARQUAGE

- ▶ **Niveau 2 (OSI) :**
 - ▶ Ethernet (CoS)
 - ▶ Frame relay (DE bit)
 - ▶ ATM (CLP bit)
 - ▶ MPLS (Exp bits)
- ▶ **Niveau 3 (OSI) :**
 - ▶ IP precesence
 - ▶ DSCP

COMPARAISON DES MARQUEURS

Marqueur	Portée	Plage de valeurs
IP precedence	Travers tout le réseau	8 valeurs, 2 réservées (0 à 7)
DSCP	Travers tout le réseau	64 valeurs, 32 sont standard (0 à 63)
QoS group	Locale au routeur	100 valeurs (0 à 99)
MPLS experimental bits	À travers un réseau MPLS	8 valeurs
Frame Relay DE bit	À travers un réseau Frame Relay	2 valeurs (0 ou 1)
ATM CLP bit	À travers un réseau ATM	2 valeurs (0 ou 1)
CoS (IEEE 802,1Q ou ISL)	À travers un réseau LAN	8 valeurs

IP PRECEDENCE (ANCIEN)

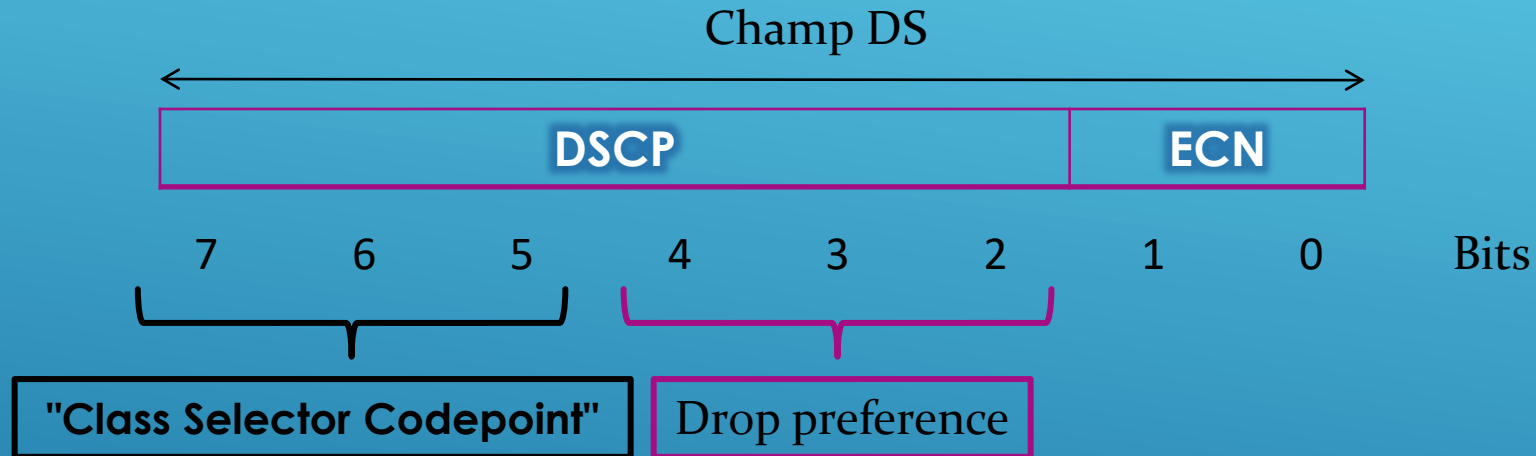
L1	L2	ToS	IP source	IP destination
----	----	-----	-----------	----------------	------

B7 b6 b5 b4 b3 b2 b1 b0



7 - Réserve
6 - Réserve
5 - Voix
4 - Vidéo
3 - signalisation des appels
2 - Données de haute priorité
1 - Données de moyenne priorité
0 - Best Effort

DSCP (DIFFSERV CODEPOINT) (NOUVEAU) - RFC 2474



TRANSMISSION EXPÉDIÉE : EF

- ▶ RFC 3246 définit le PHB de transmission expédié (EF) : « Le PHB EF peut être utilisé pour établir une **basse perte**, une **faible latence**, une **gigue faible**, une **bande passante assurée**, un service de bout en bout par des domaines DS (Diffserv). Un tel service apparaît aux points finaux comme une connexion point par point ou « une ligne louée virtuel ». Ce service a été également décrit comme « service de première classe ». Le point de code **101110** est recommandé pour le PHB EF qui correspond à une valeur DSCP de **46**.
- ▶ Remarque : RFC 3246 remplace le RFC 2598

- ▶ **Performances :**
 - ▶ **Faible perte de paquet**
 - ▶ **Faible latence**
 - ▶ **Faible gigue**
 - ▶ **Bande Passante Assuré**
- ▶ **Niveau de Service : Premium**
- ▶ **Ressemble à une liaison virtuelle louée**
- ▶ **Valeur du « Code Point » : 101110 (DSCP)**

TRANSMISSION ASSURÉE : AF

- ▶ RFC 2597 définit la transmission assurée (AF) PHB et la décrit comme moyen pour un domaine DS fournisseur d'offrir **différents niveaux** de garantie de transmission pour des paquets IP reçus d'un **domaine DS client**. Le PHB de transmission assurée garantit une **certaine partie de la bande passante à une classe AF** et permet l'accès à la bande passante supplémentaire si disponible.
- ▶ Remarque : RFC 2597 à été mise à jours par la RFC 3260

- ▶ Il y a quatre classes AF, de AF1x à AF4x.
- ▶ Dans chaque classe, il y a trois probabilités de perte.
- ▶ Niveau de Service : En total, nous avons 12 niveaux de services possibles
- ▶ Selon la stratégie donnée d'un réseau, des paquets peuvent être sélectionnés pour un PHB selon le débit, le retard, la gigue, la perte requis ou selon la priorité de l'accès aux services réseau.
- ▶ Valeur du « Code Point » : xxxxx0 (DSCP)

DSCP

6. IANA Considerations

The DSCP field within the DS field is capable of conveying 64 distinct codepoints. The codepoint space is divided into three pools for the purpose of codepoint assignment and management: a pool of 32 RECOMMENDED codepoints (Pool 1) to be assigned by Standards Action as defined in [CONS], a pool of 16 codepoints (Pool 2) to be reserved for experimental or Local Use (EXP/LU) as defined in [CONS], and a pool of 16 codepoints (Pool 3) which are initially available for experimental or local use, but which should be preferentially

Nichols, et. al.

Standards Track

[Page 14]



RFC 2474

Differentiated Services Field

December 1998

utilized for standardized assignments if Pool 1 is ever exhausted. The pools are defined in the following table (where 'x' refers to either '0' or '1'):

Pool	Codepoint space	Assignment Policy
----	-----	-----
1	xxxxx0	Standards Action
2	xxxx11	EXP/LU
3	xxxx01	EXP/LU (*)

(*) may be utilized for future Standards Action allocations as necessary

This document assigns eight RECOMMENDED codepoints ('xxx000') which are drawn from Pool 1 above. These codepoints MUST be mapped, not to specific PHBs, but to PHBs that meet "at least" the requirements set forth in Sec. 4.2.2.2 to provide a minimal level of backwards compatibility with IP Precedence as defined in [RFC791] and as deployed in some current equipment.

<0-63>	Differentiated services	codepoint value
af11	Match packets with AF11 dscp	(001010)
af12	Match packets with AF12 dscp	(001100)
af13	Match packets with AF13 dscp	(001110)
af21	Match packets with AF21 dscp	(010010)
af22	Match packets with AF22 dscp	(010100)
af23	Match packets with AF23 dscp	(010110)
af31	Match packets with AF31 dscp	(011010)
af32	Match packets with AF32 dscp	(011100)
af33	Match packets with AF33 dscp	(011110)
af41	Match packets with AF41 dscp	(100010)
af42	Match packets with AF42 dscp	(100100)
af43	Match packets with AF43 dscp	(100110)
cs1	Match packets with CS1 (precedence 1) dscp	(001000)
cs2	Match packets with CS2 (precedence 2) dscp	(010000)
cs3	Match packets with CS3 (precedence 3) dscp	(011000)
cs4	Match packets with CS4 (precedence 4) dscp	(100000)
cs5	Match packets with CS5 (precedence 5) dscp	(101000)
cs6	Match packets with CS6 (precedence 6) dscp	(110000)
cs7	Match packets with CS7 (precedence 7) dscp	(111000)
default	Match packets with default dscp	(000000)
ef	Match packets with EF dscp	(101110)

EXEMPLE

					b7	b6	b5	b4	b3	b2	b1	b0				
					Type Of Service											
					DSCP										DSCP	
Notation décimale	Précédence IP												NOM	Notation décimale		
	NOM															
7	Network	1	1	1	0	0	0	x	x	CS7	56					
6	Internet	1	1	0	0	0	0	x	x	CS6	48					
5	Critical	1	0	1	1	1	0	x	x	EF	46					
4	Flash-override	1	0	0	0	0	0	x	x	CS4	32					
					0	1	0	x	x	AF41	34					
					1	0	0	x	x	AF42	36					
					1	1	0	x	x	AF43	38					
3	Flash	0	1	1	0	0	0	x	x	CS3	24					
					0	1	0	x	x	AF31	26					
					1	0	0	x	x	AF32	28					
					1	1	0	x	x	AF33	30					
2	Immediate	0	1	0	0	0	0	x	x	CS2	16					
					0	1	0	x	x	AF21	18					
					1	0	0	x	x	AF22	20					
					1	1	0	x	x	AF23	22					
1	Priority	0	0	1	0	0	0	x	x	CS1	8					
					0	1	0	x	x	AF11	10					
					1	0	0	x	x	AF12	12					
					1	1	0	x	x	AF13	14					
0	Routine	0	0	0	0	0	0	x	x	BE	0					

Les Class Selector représentent des **catégories**.

L'équipement lie l'**importance** de la transmission du paquet à la valeur de la précedence IP.

Les Assured Forwarding représentent des **sous catégories**.

Les bits b4 et b3 indiquent une priorité de poubellisation (DROP).

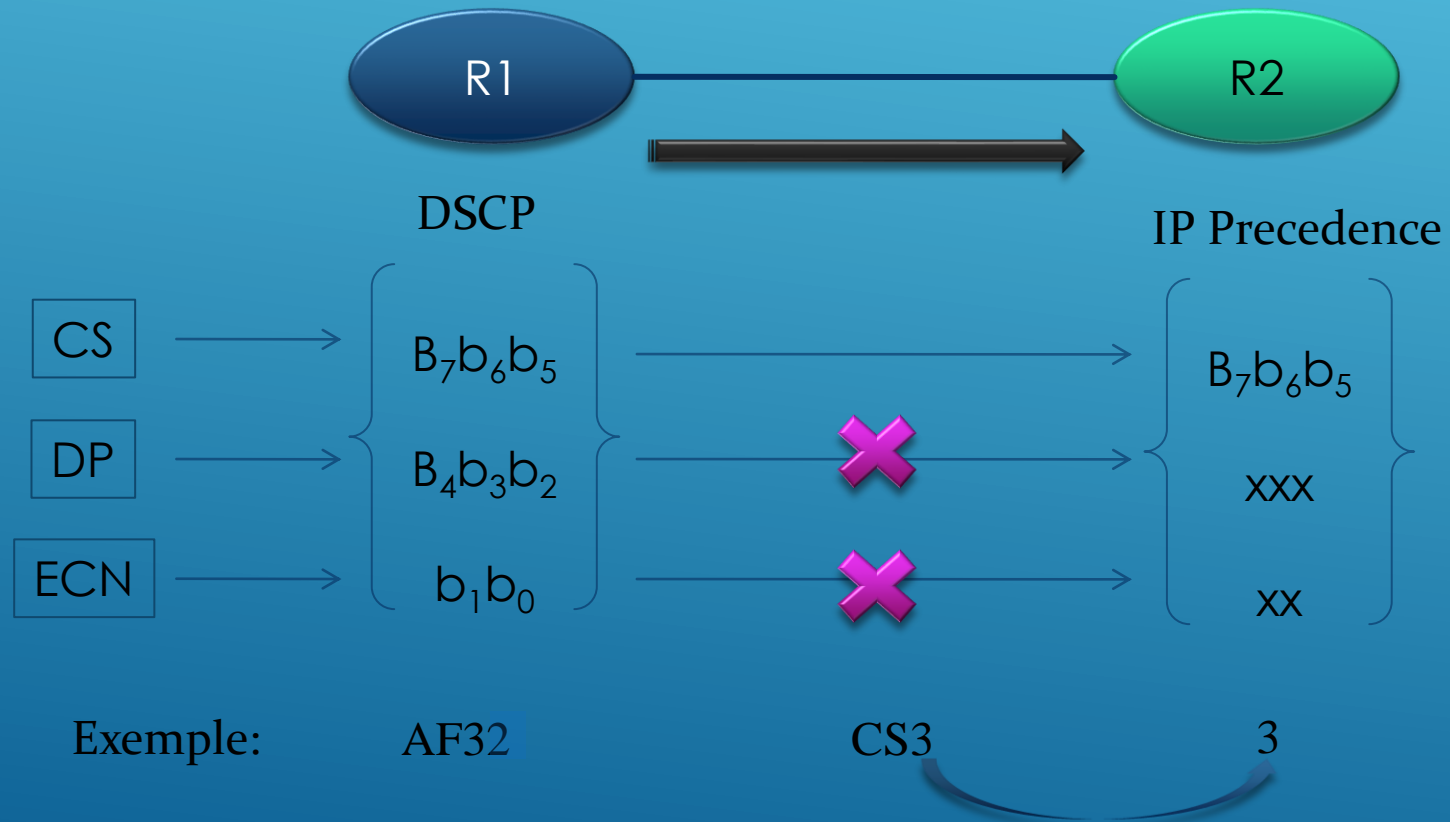
A l'inverse des CS, l'équipement lie la poubellisation (DROP) à la valeur des bits b4 et b3.

Exemple:

AF41 > AF43 > AF21

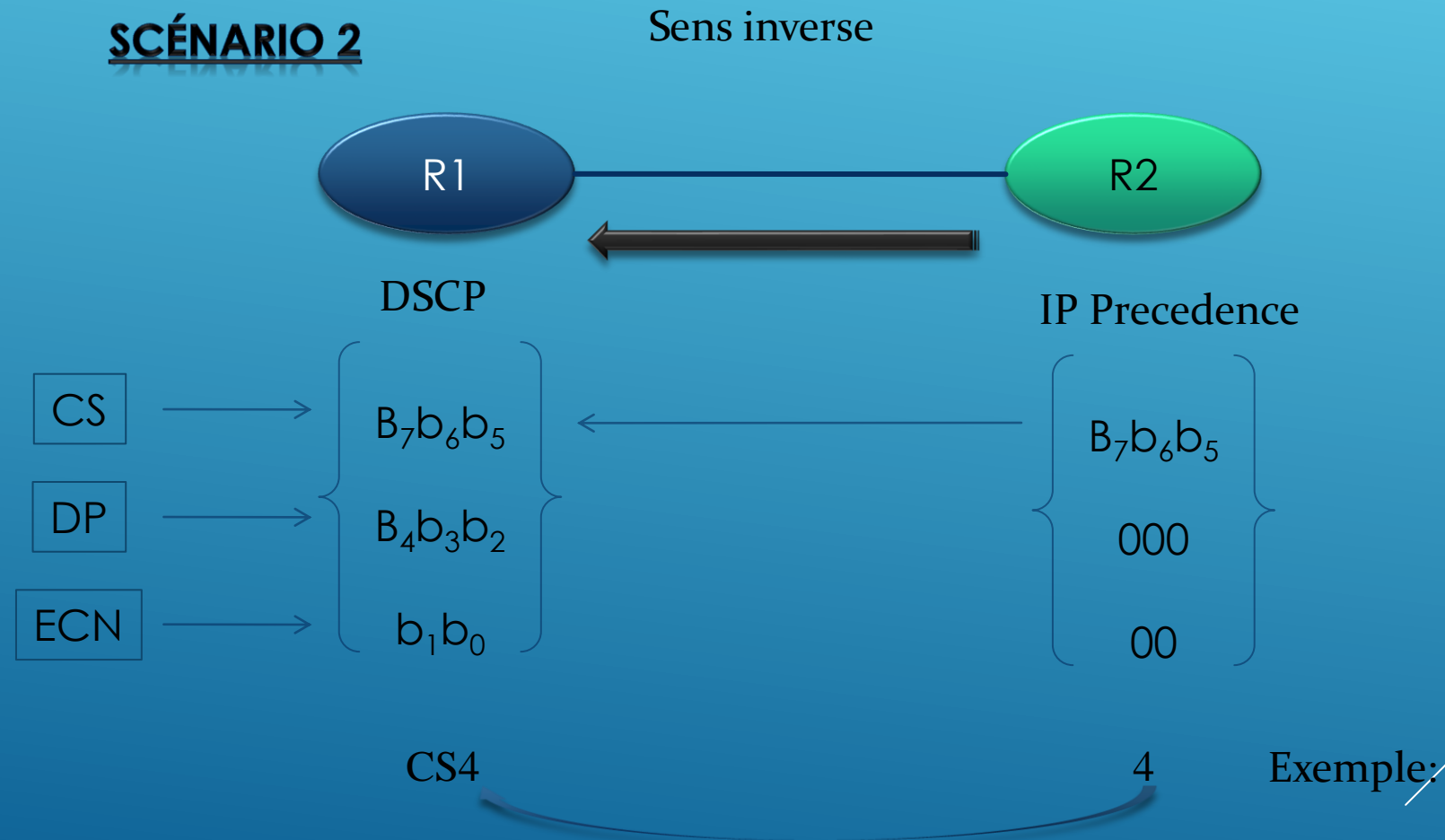
INTEROPÉRABILITÉ IPP & DSCP

SCÉNARIO 1



INTEROPÉRABILITÉ IPP & DSCP

SCÉNARIO 2

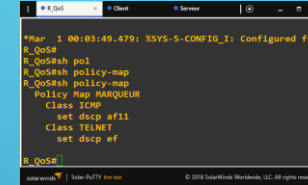


IMPLÉMENTATION : MODÈLE MQC

Exemple pour la classification & le Marquage

MODES DE CONFIG CISCO

- ▶ CLI
- ▶ Modular QoS CLI (MQC)
- ▶ AutoQoS
- ▶ QoS Policy Manager (QPM)



```
Router 1 00:03:49:479: XSYS-5-CONFIG_1: Configured for
R_QoS#
R_QoS# pol
R_QoS# policy-map
R_QoS# policy-map
  Policy Map MARQUEUR
    Class ICMP
      set dscp ef11
    Class TELNET
      set dscp ef
R_QoS#
```



COMPARAISON

	CLI	MQC	AutoQoS VoIP	AutoQoS Enterprise
Ease of Use	Poor	Easier	Simple	Simple
Ability to Fine-Tune	OK	Very Good	Very Good	Very Good
Time to Deploy	Longest	Average	Shortest	Shortest
Modularity	Poor	Excellent	Excellent	Excellent

MODULAR QOS CLI (MQC)



Définit les classes de trafic.

“A quel trafic on doit faire attention?”

Chaque classe de trafic: *class map*.

Définir les *Policy* de QoS pour les classes

“Qu’est-ce qu’on doit faire à ce trafic?”

Définit une *policy map*, qui configure les mécanismes de la QoS associé aux classes de trafic identifiées en utilisant la *class map*

Appliquer la *Service Policy*

“ou va-t-il être implémentée?”

Attacher une *service Policy* Configurée par la *policy map* sur une Interface.

CLASSIFICATION

router(config) #

SYNTAX

class-map [match-any | match-all] class-map-name

OU

ET

Nom de la class-map (40 car
alphanumériques maximum)

Accès au mode class-map

router(config-cmap) #

SYNTAX

match condition

Critère de classification
(voir slid suivant)

router(config-cmap) #

SYNTAX

match class-map class-map

Classification à partir
d'un autre class-map

router(config-cmap) #

SYNTAX

match not match-criteria

router(config-cmap) #

SYNTAX

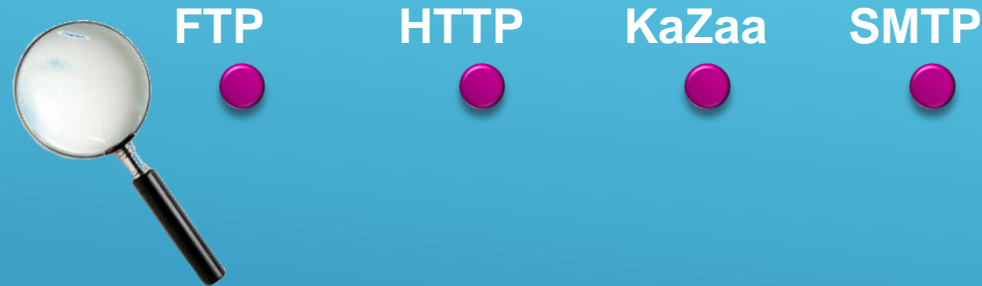
match any

CLASSIFICATION MF

- ▶ Les options de classification sont configurées dans une « class-map »
- ▶ Nécessite une « policy-map » pour fonctionner
- ▶ Les options de classification MQC peuvent inclure:

- Access list
- IP precedence value
- IP DSCP value
- QoS group number
- MPLS experimental bits
- Protocol (NBAR)
- Using another class map
- Frame Relay DE bit
- IEEE 802.1Q/ISL CoS/Priority values
- Input interface
- Source MAC address
- Destination MAC address
- RTP (UDP) port range
- Any packet

CLASSIFICATION MF | NBAR



- ▶ **Inspection profonde des paquets (Niveau 4 – 7)**
 - ▶ HTTP (URL, MIME, Nom d'hôte...)
 - ▶ Nom des applications (KaZaa, Napster, citrix, Exchange)
 - ▶ ...
- ▶ **Pré-requis : CEF doit être activé**
- ▶ **Mise à jour à l'aide des PDL.**
- ▶ **Autre utilité : supervision.**

TCP and UDP Static Port Protocols				
BGP	IMAP	NNTP	RSVP	SNMP
BOOTP	IRC	Notes	SFTP	SOCKS
CU-SeeMe	Kerberos	Novadigm	SHTTP	SQLServer
DHCP/DNS	L2TP	NTP	SIMAP	SSH
Finger	LDAP	PCAnywhere	SIRC	STELNET
Gopher	MS-PPTP	POP3	SLDAP	Syslog
HTTP	NetBIOS	Printer	SMTP	Telnet
HTTPS	NFS	RIP	SNMP	X Windows

TCP and UDP Stateful Protocols			
Citrix ICA	Gnutella	r-commands	StreamWorks
Exchange	HTTP	RealAudio	SunRPC
FastTrack	Napster	RTP	TFTP
FTP	Netshow	SQL*NET	VDOLive

Non-UDP and Non-TCP Protocols	
EGP	ICMP
EIGRP	IPINIP
GRE	IPSec

CLASSIFICATION BA

IP Precedence

IP Precedence Value	IP Precedence Name
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

DSCP

DSCP Value	DSCP Class Name
0 (000000)	default
1 (001000)	cs1
2 (010000)	cs2
3 (011000)	cs3
4 (100000)	cs4
5 (101000)	cs5
6 (110000)	cs6
7 (111000)	cs7
46 (101110)	ef

DSCP Value	DSCP Class Name
10 (001010)	af11
12 (001100)	af12
14 (001110)	af13
18 (010010)	af21
20 (010100)	af22
22 (010110)	af23
26 (011010)	af31
28 (011100)	af32
30 (011110)	af33
34 (100010)	af41
36 (100100)	af42
38 (100110)	af43

EXEMPLES DE CONFIG

CLASS-MAP /GOLD

router1(config)#class-map Or

router1(config-cmap)#match access-group name Gold

router1(config)#ip access-list extended Gold

**router1(config-ext-nacl)#permit ip any any precedence
flash-override**

TRAITEMENT « POLICY-MAP »

- ▶ **Marquage**
- ▶ **Gestion de congestion**
- ▶ **Ordonnancement**
- ▶ **Réglementation**
- ▶ **Lissage**
- ▶ ...

POLICY-MAP

Nom de la class-map (40 car
alphanumériques maximum)

```
router(config) #
```

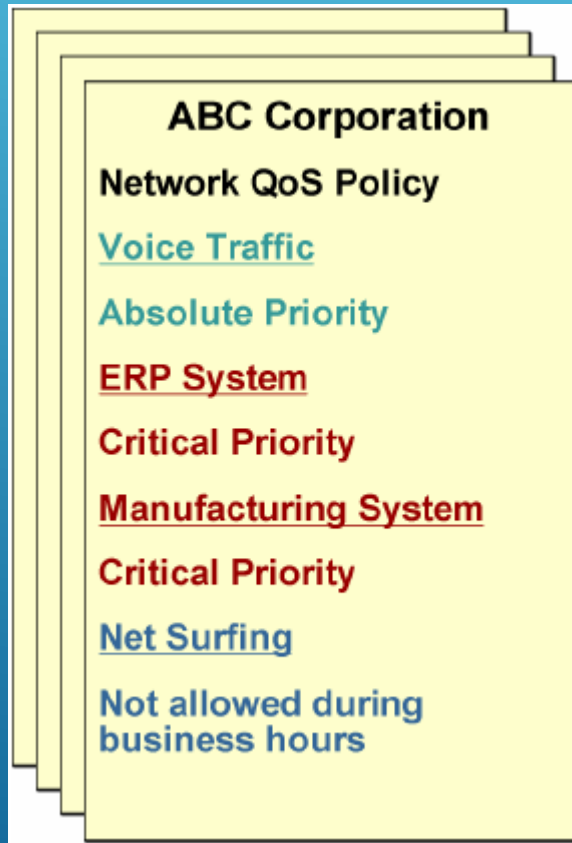
SYNTAX

```
policy-map policy-map-name
```

Accès au mode class-map

POLICY-MAP

Cahier de charge



```
policy-map TEST
  class Gold
    bandwidth 216
  class Silver
    bandwidth 169
  class Bronze
    bandwidth 108
  class class-
  default
    bandwidth 31
  class Platinum
    priority 384
```

SERVICE-POLICY

```
router(config-if) #
```

```
SYNTAX
```

```
service-policy {input | output} policy-map-name
```

Nom de la class-map (40 car
alphanumériques maximum)

Accès au mode class-map

L e sens du trafique

SERVICE-POLICY

- ▶ **router1(config)#interface serial 0/0**
- ▶ **router1(config-if)#service-policy output TEST**

MARQUAGE

- IP precedence
- IP DSCP
- QoS group
- MPLS experimental bits
- IEEE 802.1Q or ISL CoS/priority bits
- Frame Relay DE bit
- ATM CLP bit

MARQUAGE

Niveau 2 :

```
router(config-pmap-c) #
```

SYNTAX

```
set cos cos-value
```

Niveau 3 :

```
router(config-pmap-c) #
```

SYNTAX

```
set ip precedence ip-precedence-value
```

```
router(config-pmap-c) #
```

SYNTAX

```
set ip dscp ip-dscp-value
```


EXEMPLE DE CONFIGURATION

```
El-jadida(config)#class-map FTP
El-jadida(config-cmap)#match protocol ftp
El-jadida(config-cmap)#exit
```

```
El-jadida(config)#class-map URL
El-jadida(config-cmap)#match protocol http url "*.flv*"
El-jadida(config-cmap)#exit
```

```
El-jadida(config)#class-map HTTP
El-jadida(config-cmap)#match protocol http
El-jadida(config-cmap)#end
```

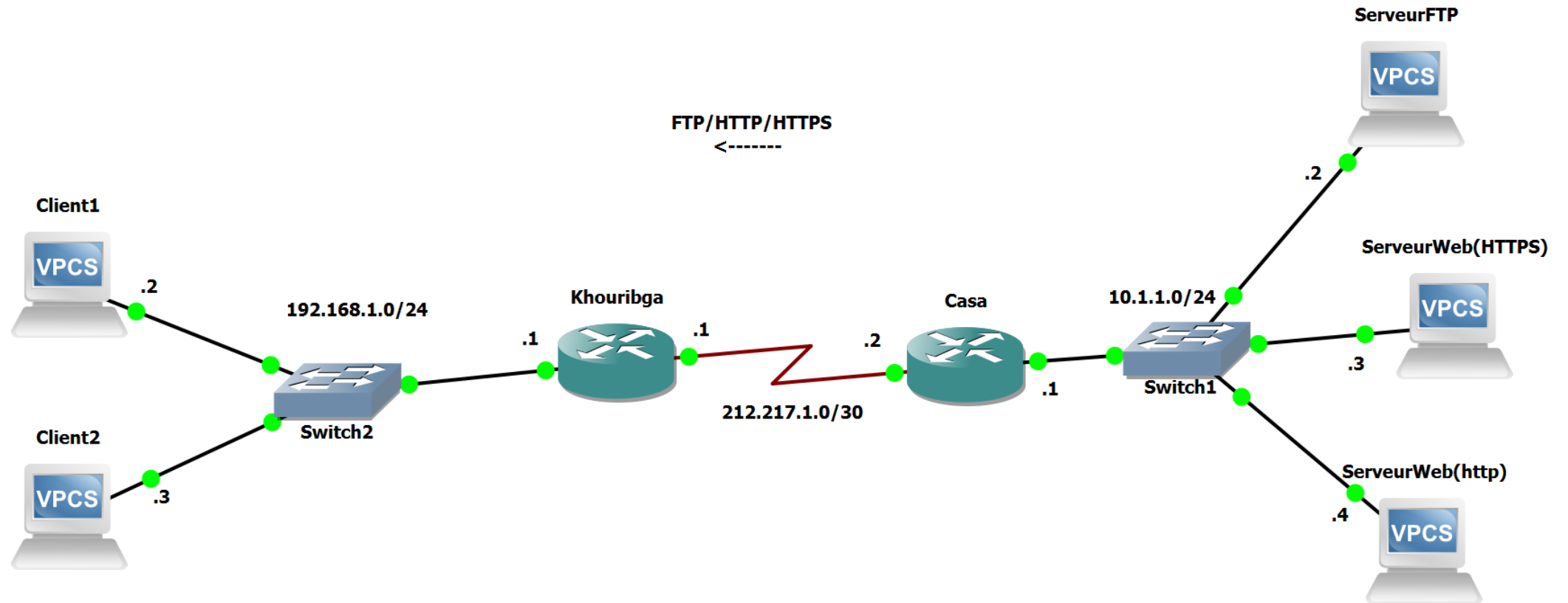
```
El-jadida(config)#policy-map MARQUER
El-jadida(config-pmap)#class FTP
El-jadida(config-pmap-c)#set ip dscp af33
El-jadida(config-pmap-c)#exit
```

```
El-jadida(config-pmap)#class URL
El-jadida(config-pmap-c)#set ip dscp af22
El-jadida(config-pmap-c)#exit
```

```
El-jadida(config-pmap)#class HTTP
El-jadida(config-pmap-c)#set ip dscp af11
```

```
El-jadida(config)#interface FastEthernet 1/0
El-jadida(config-if)#service-policy input MARQUER
```

SCHÉMA CLASSIFICATION & MARQUAGE



Cahier des charges :

- Classification MF sur le routeur « Casa »
 - Classe 1 : Trafic **FTP**
 - Classe 2 : Trafic **HTTP** du « Serveur Web » HTTP vers le Client 2
 - Classe 3 : Trafic **HTTPS**
 - Classe 4 : Par **défaut**
- Marquage sur le routeur « Casa » :
 - Classe1 → **EF**
 - Classe2 → **AF31**
 - Classe3 → **AF22**
 - Classe 4 → **Default (00)**

- Classification BA sur le routeur « Khouribga » :

- Classe Or (**EF**)
- Classe Argent (**AF31**)
- Classe Bronze (**AF22**)
- Classe Routine (Default (**00**))

- Re-Marquage sur le routeur « Khga » :

- Classe Or (Classe1) → **AF32**
- Classe Argent (Classe2) → **AF21**
- Classe Bronze (Classe3) → **Default**
- Classe Routine (Classe 4) → **AF33**

Testes :

- utiliser Wireshark et le ping modifié.

COMMANDES

- ▶ **Classification MF (Routeur de Casa)**
- ▶ **class-map match-all HTTP**
 - match protocol http
 - match access-group name HTTP
- ▶ **class-map match-all FTP**
 - match protocol ftp
- ▶ **class-map match-all HTTPS**
 - match protocol secure-http
- ▶ **ip access-list extended HTTP**
 - permit ip host 10.1.1.4 host 192.168.1.3
 - deny ip any any