

www.Mcours.com

Site N°1 des Cours et Exercices Email: contact@mcours.com

Réseaux virtuels

cours@urec.cnrs.fr



Réseaux virtuels

- 1997 : Jean-Paul Gautier
- modifications
 - 1998 : Jean-Paul Gautier

Plan

- Evolution des réseaux
- Qu'est ce qu'un réseau virtuel (VLAN)
- Les VLANs et les standards
- Règles de "design"
- Administration des VLAN's

Evolution des ressources CPU

- Evolution

– En 1980	Vax 780		1 Mips
– En 1996	IBM Power Station 590	117	
	DEC 3000 model 800		138
	SUN SS20		89
	Intel Xpress Deskside		100

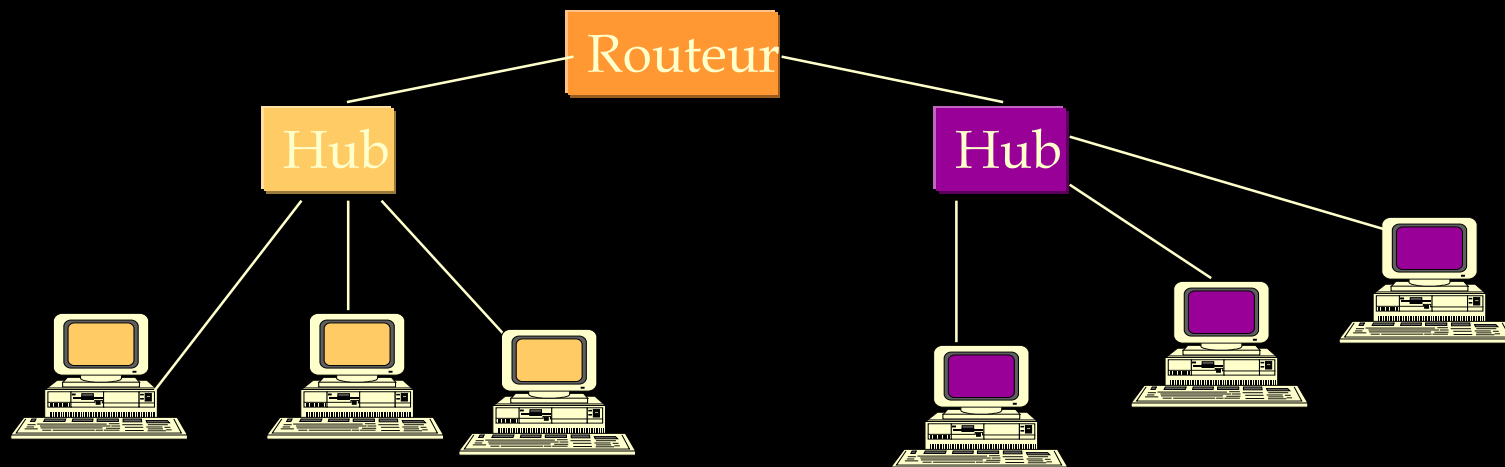
- Autorisent les applications distribuées

Evolution des applications

- Basées auparavant sur du texte, elles incluent maintenant la voix, les images, la vidéo
 - exemple : Mail avec MIME
- W W W
- De nouvelles exigences
 - Qualité de services (QoS)
 - Temps Réel ou Play-Back
 - Point à point ou Multipoint
 - Vidéoconférence, enseignement à distance, "kiosques"

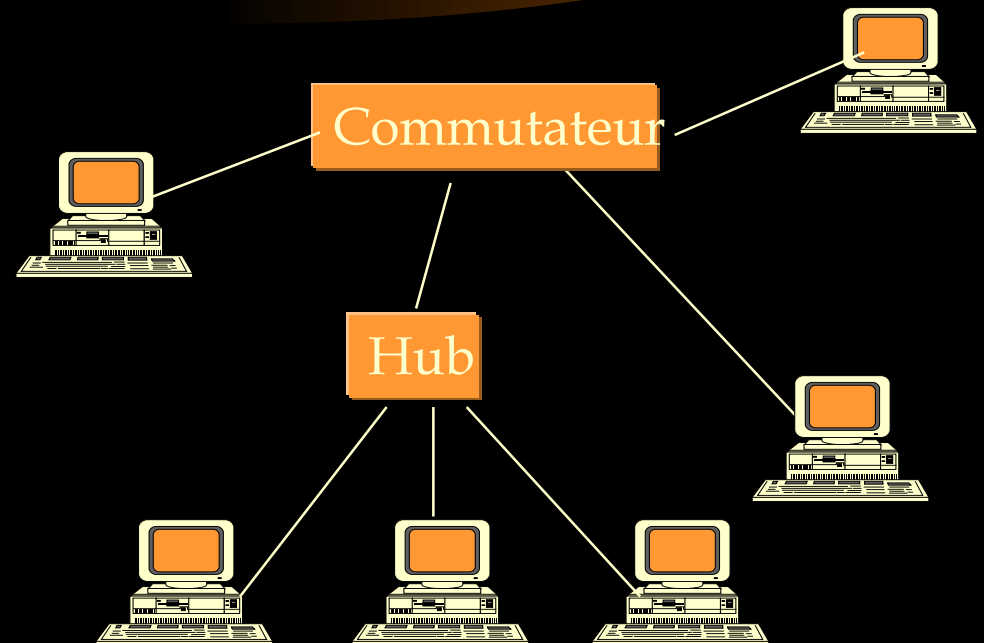
Les réseaux partagés : contraintes

- Les sous-réseaux sont liés aux hubs
- Les utilisateurs sont groupés géographiquement
- Pas de sécurité sur un segment
- Plan d'adressage difficile
- La mobilité entraîne un changement d'adresse



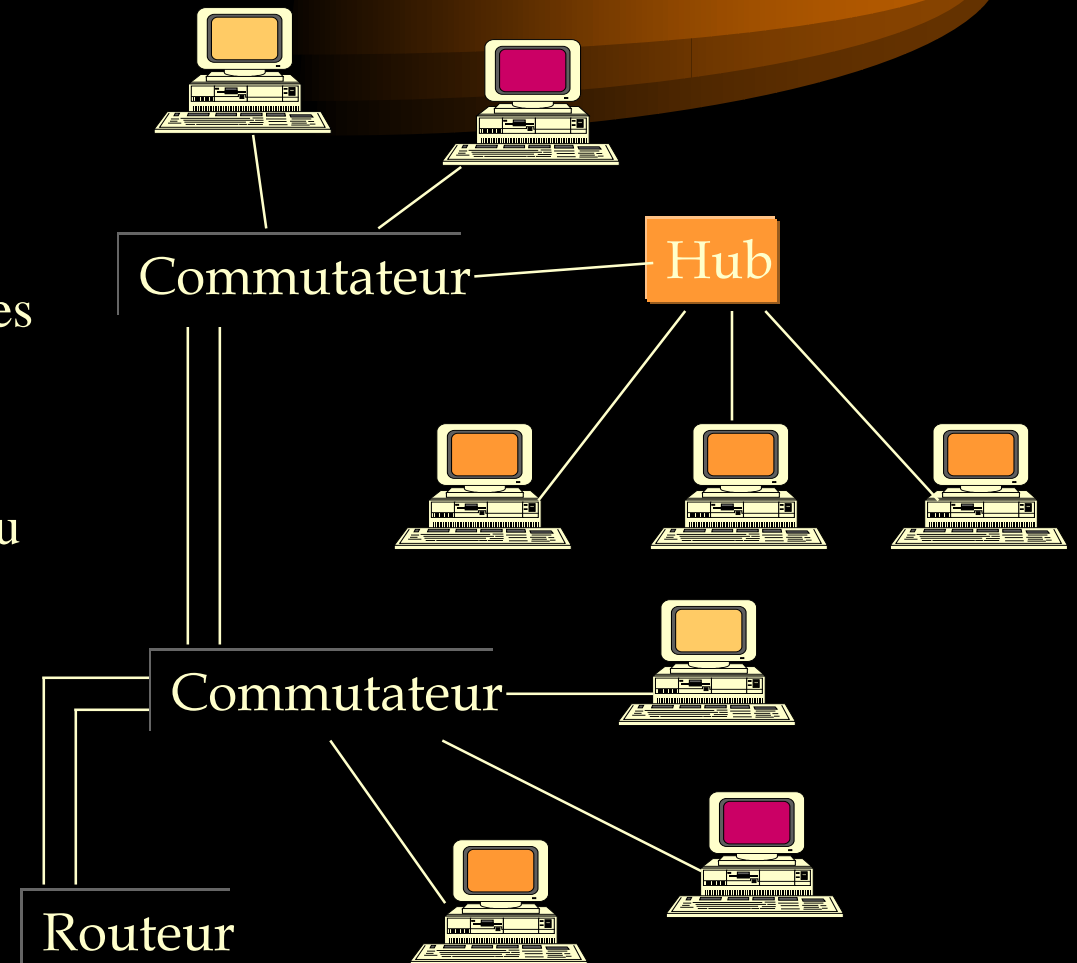
La commutation

- Meilleur accès au média
 - bande passante dédiée,
 - moins de conflits d'accès
 - collisions réduites
- Le trafic est dirigé vers la station spécifiée
- Les "broadcast" sont diffusés plus vite
- L'évolutivité reste un problème



Le réseau local commuté

- Domaines de collisions réduits
- Intelligence dans le port du commutateur
- Les frontières physiques disparaissent
- Regroupement logique des utilisateurs
- Meilleur contrôle de la bande passante et des changements dans le réseau
- Centralisation de l'administration
- Routeur pour la communication inter-réseau



Technologies commutées

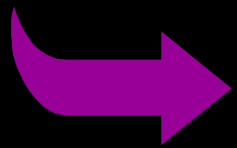
- Ethernet commuté 10/100 Mbps
- Gigabit Ethernet (IEE 802.3z)
- Token ring commuté 4/16 Mbps
- FDDI/CDDI commuté 100 Mbps

Caractéristiques communes

- Modes Half -Duplex & Full-Duplex
 - Cut-Through & Store and Forward
 - Commutateur = Pont multi-ports
-
- ATM (155 Mbps, 622 Mbps, 2.4 Gbps), circuit virtuel

Qu'est ce qu'un réseau virtuel

- Trois nécessités pour introduire le concept
 - Limiter les domaines de broadcast
 - Garantir la sécurité
 - Permettre la mobilité des utilisateurs

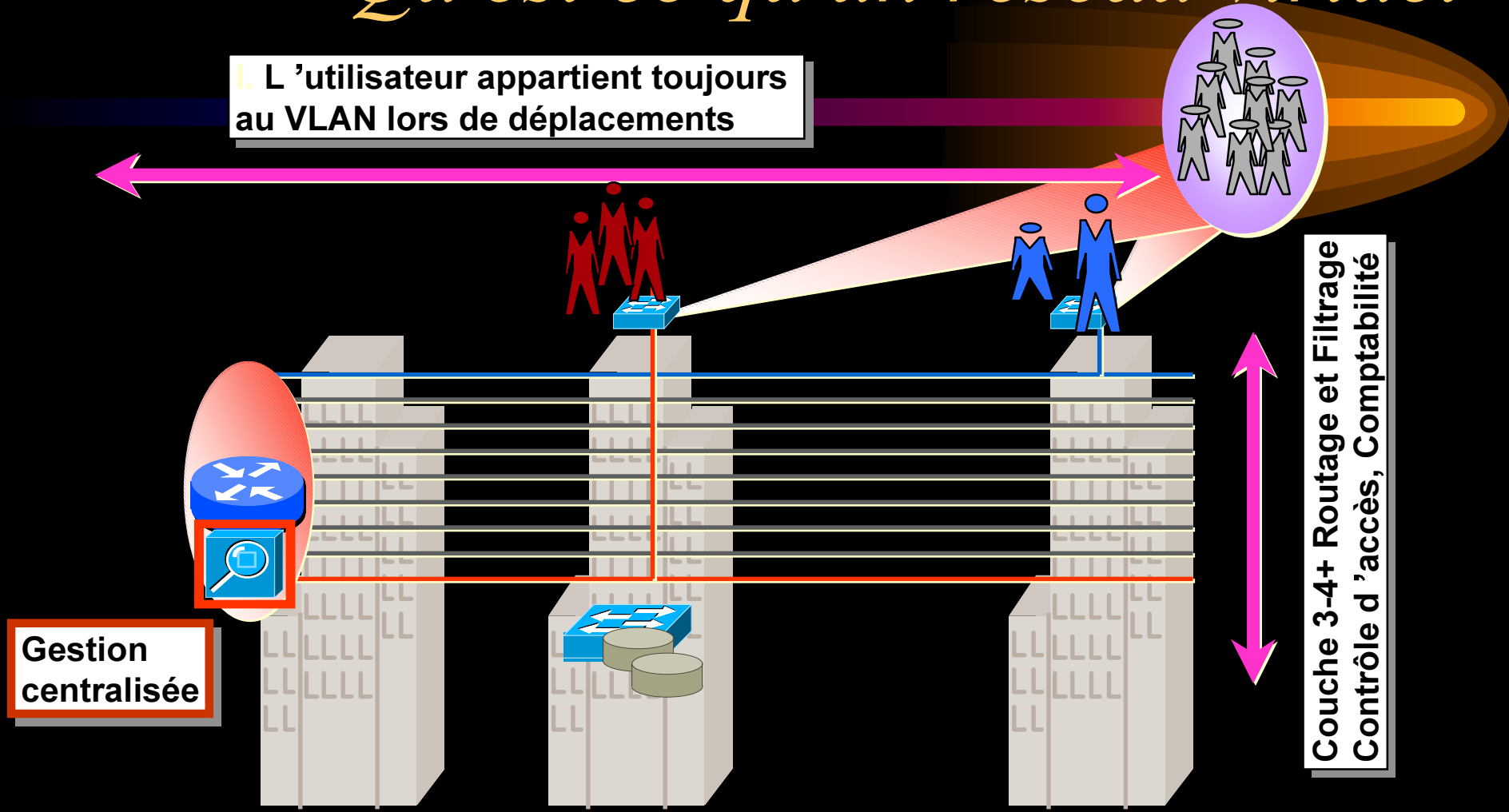


Une nouvelle manière d'exploiter la technique de la commutation pour donner plus de flexibilité aux réseaux locaux

c'est un réseau logique

Qu'est ce qu'un réseau virtuel

L'utilisateur appartient toujours au VLAN lors de déplacements

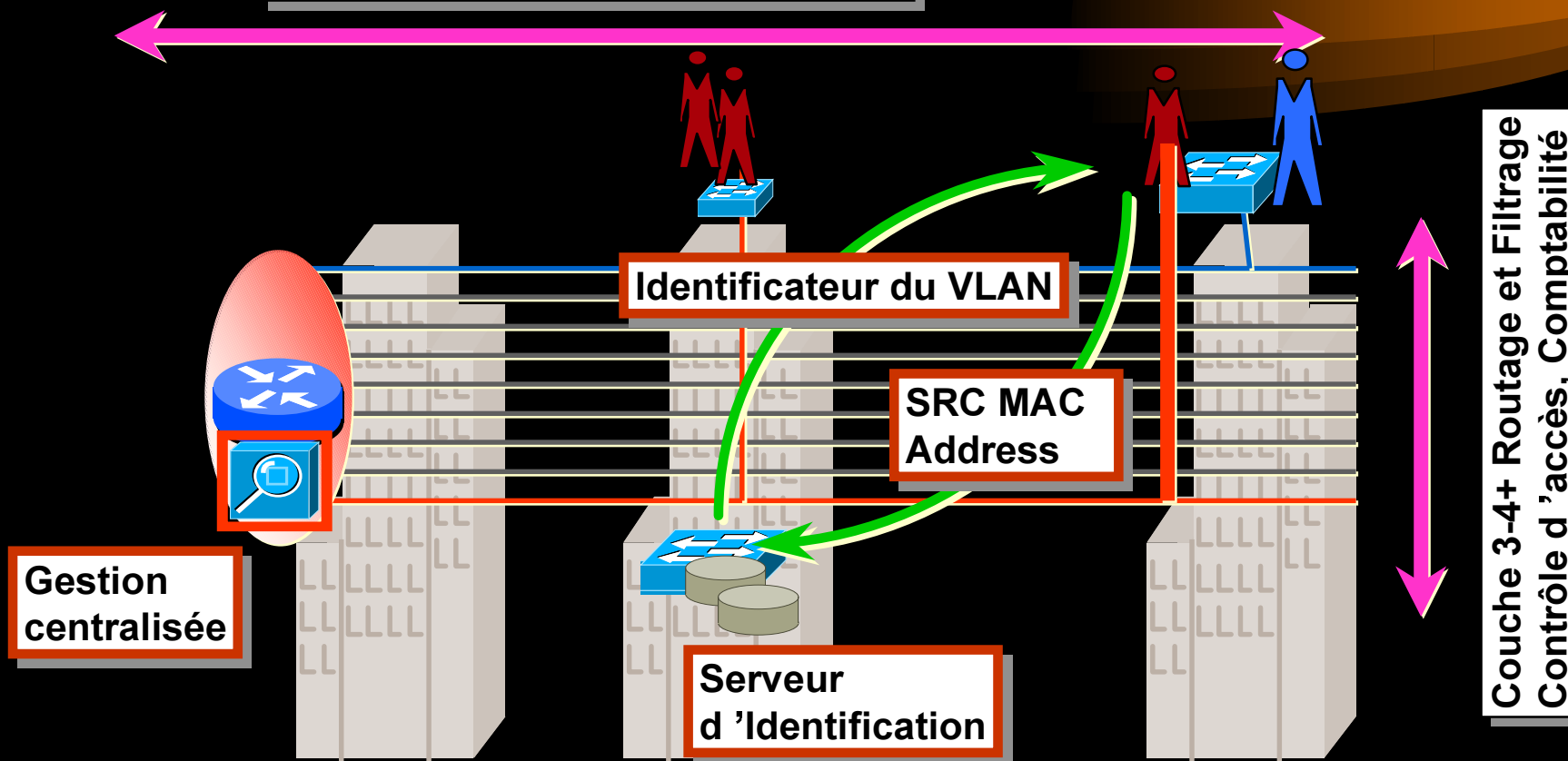


Gestion centralisée

Couche 3-4+ Routage et Filtrage
Contrôle d'accès, Comptabilité

Qu'est ce qu'un réseau virtuel

L'utilisateur appartient toujours au VLAN lors de déplacements



Le réseau virtuel (VLAN)

- Permet la gestion dynamique de la mobilité
- Permet a des utilisateurs géographiquement dispersés de partager des données
- Maintient la sécurité
- Conserve les domaines de broacast traditionnels des LANs
- Requiert une couche 3 pour la communication entre VLANs

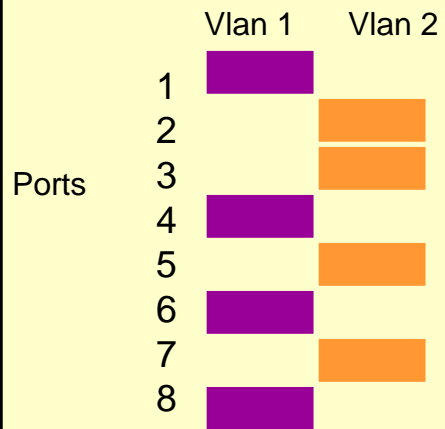
Réseaux virtuels : Plusieurs types

1ère Génération de la technologie VLAN

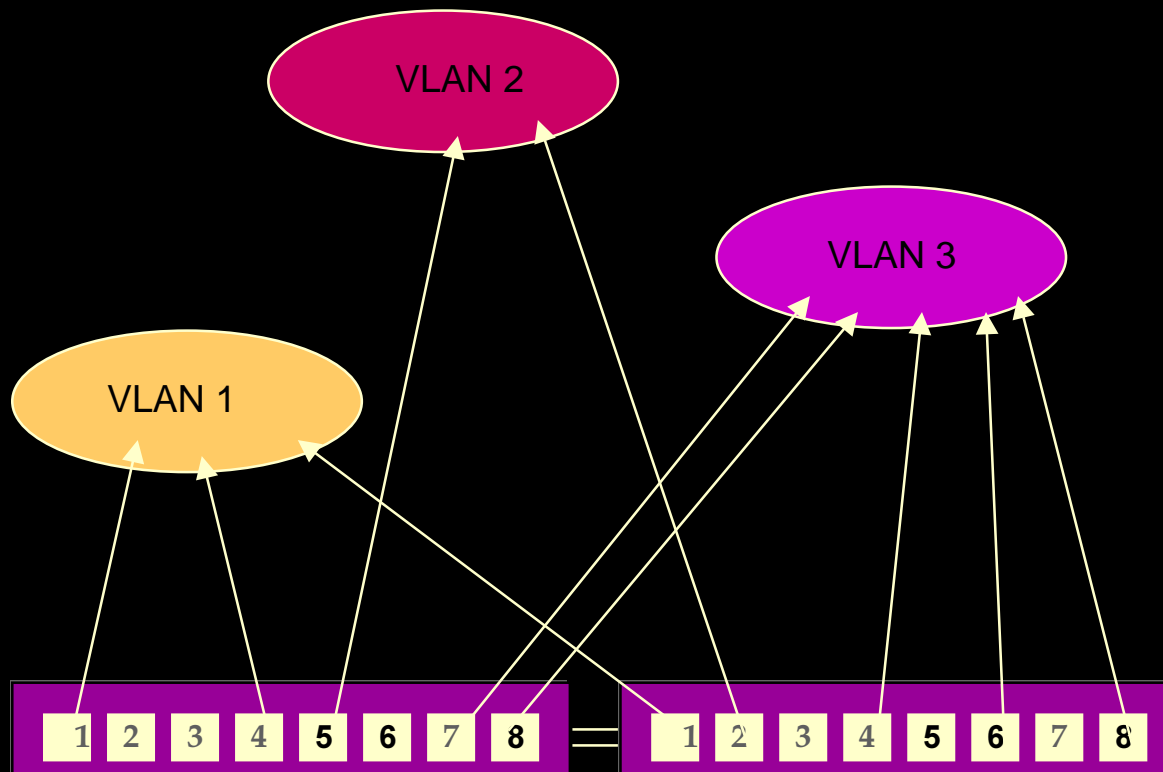
2ère Génération de la technologie VLAN

VLANs de niveau 1

Groupe de segments



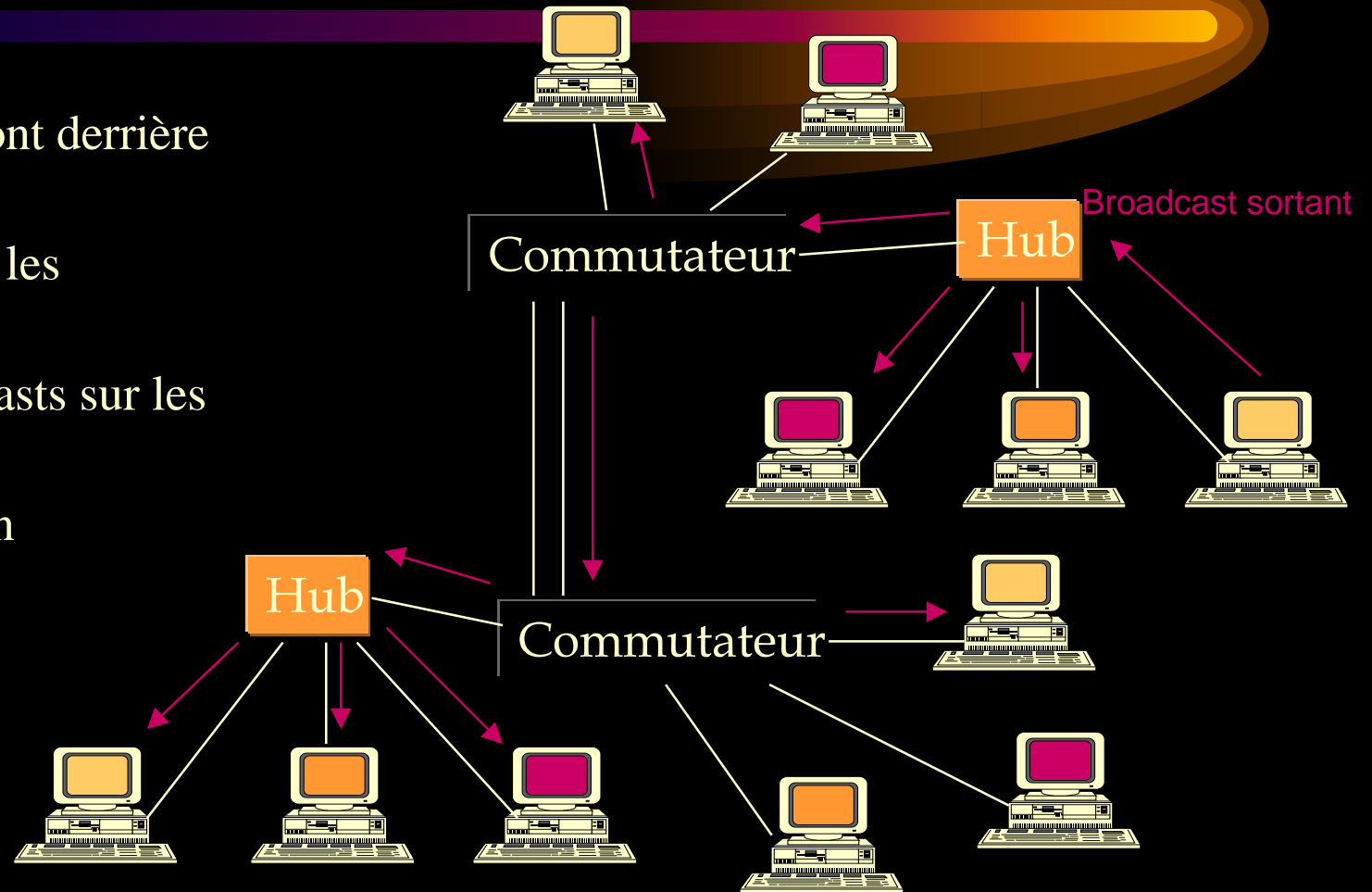
Appartenance par port



- Association port-utilisateur
Association port-segment
- Ne nécessite pas de recherche si fait par des ASICs
- Aucun paquet ne quitte son domaine
- Sécurité maximale entre VLANs
- Facilement contrôlable dans le réseau

Plusieurs VLANs par port ?

- Quand plusieurs clients sont derrière le même port
- Nécessitent de rechercher les adresses
- Pas de filtrage des broadcasts sur les segments partagés
- Beaucoup d'administration



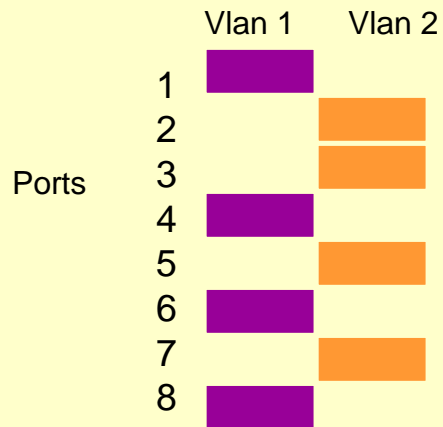
Réseaux virtuels : Plusieurs types

1ère Génération de la technologie VLAN

2ème Génération de la technologie VLAN

VLANs de niveau 1

Groupe de segments



VLANs de niveau 2

Groupe d'adresses Mac

Vlan 1	Vlan 2
0525de78ad2c	205678ae10a6
0a20487541ed	7247ef1dc52a
0b4cf246371d	02602909a214
12df467852ce	2084dcb1a705

Chaque adresse Mac appartient à un seul VLAN,
Plusieurs VLAN par port autorisés

Appartenance par adresse MAC

- Filtrage requis
 - *impact sur les performances*
- Echange des tables d'adresses des VLANs entre les commutateurs
 - overhead dû à l'administration

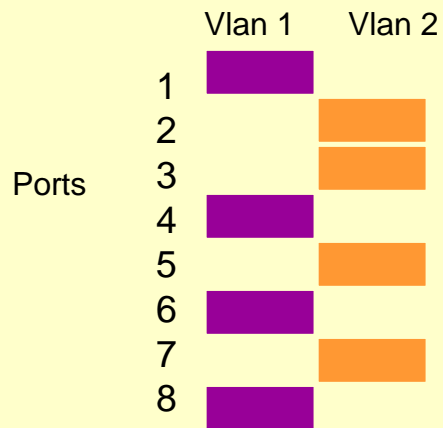
Réseaux virtuels : Plusieurs types

1ère Génération de la technologie VLAN

2ère Génération de la technologie VLAN

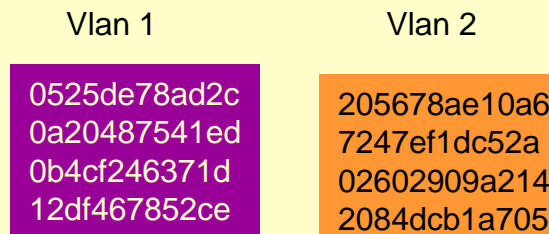
VLANs de niveau 1

Groupe de segments



VLANs de niveau 2

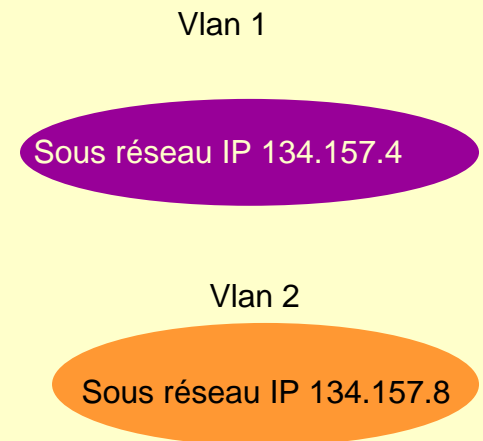
Groupe d'adresses Mac



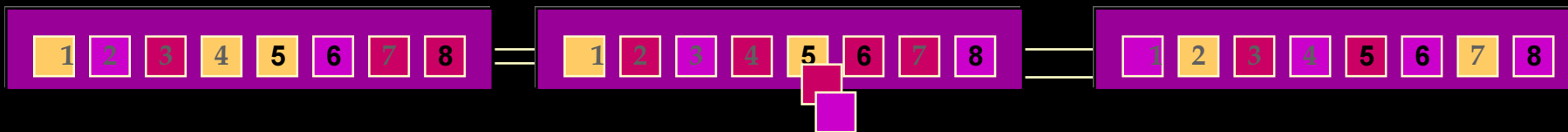
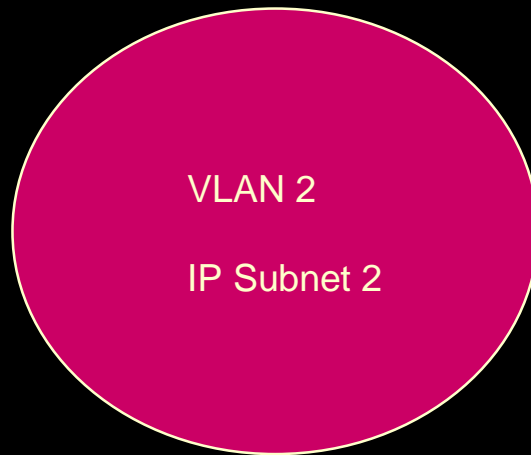
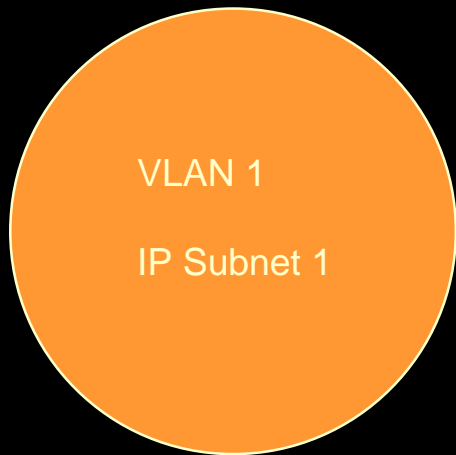
Chaque adresse Mac appartient à un seul VLAN,
Plusieurs VLAN par port autorisé

VLANs de niveau 3

Sous-réseau protocolaire (ex IP)



Appartenance par sous-réseau



Appartenance par sous-réseau

- Domaine de broadcast de niveau 2 automatiquement construit sur l'adresse de niveau 3.
- Pas d'administration manuelle des VLANs
- Uniquement avec les protocoles routables

- Simplicité des VLANs par port (statique)
- Facilité d'administration des VLANs par port (dynamique)
- Intérêt des VLANs par sous-réseau pour les protocoles routables et des VLANs par adresse MAC pour les protocoles non routables
- Administration centralisée

Utilisation des VLANs aujourd'hui

- Gestion du trafic broadcast et multicast
- Centralisation des serveurs
 - administration, sécurité
- Isolement de certaines applications
 - protection du "backbone"
- Administration centralisée
 - groupes logiques d'utilisateurs
 - contrôle de chaque utilisateur, chaque port, chaque commutateur

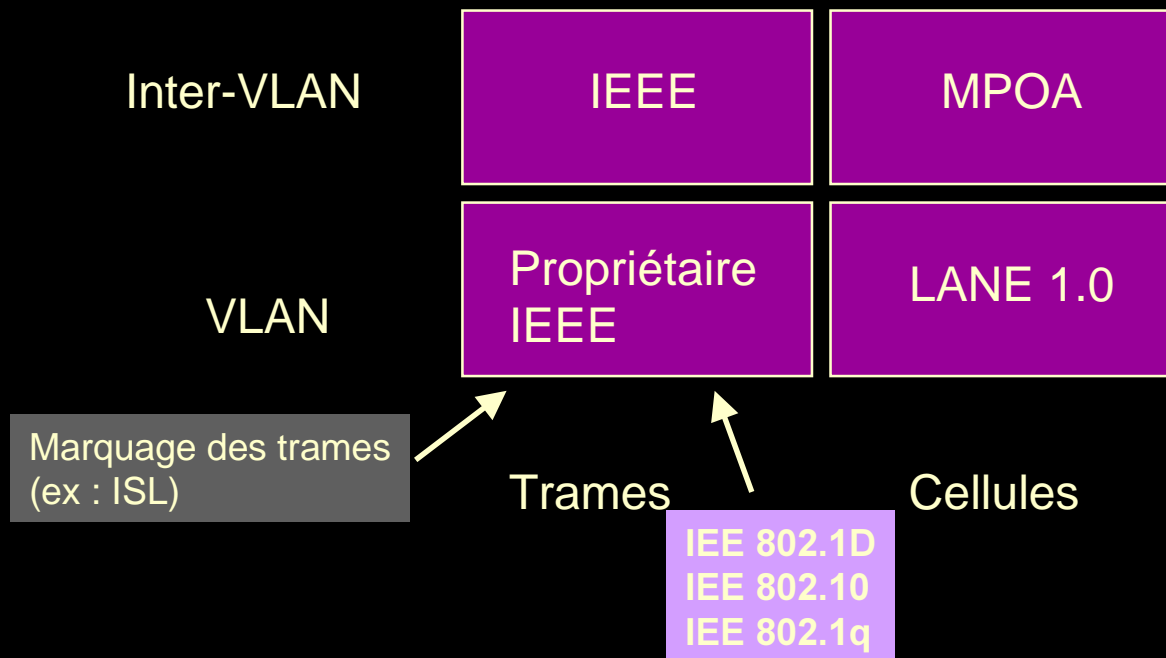
Evolutions

- Automatisation des déplacements, des ajouts, des changements
 - serveurs de configuration
 - enregistrement
 - base de données centralisée
 - requêtes de configuration des commutateurs basées sur les nouvelles adresses MAC enregistrées.
- Contrôle
 - services sur les VLANs liés aux applications
 - accès basé sur des règles centralisées
 - requiert de "l'intelligence" dans les équipements
- Réseaux de cellules ou de trames

Composants des VLANs

- Commutateurs
- Routeurs
- Serveurs
- Administration

VLAN et standards



Transparent Bridge

- Présence de ponts transparents aux stations.
- Toutes les décisions de routage, au niveau 2, sont exclusivement faites par les ponts.
- Un pont maintient une base de données pour l'aiguillage des trames : « Forwarding Data Base (FDB) »

IEEE 802.1D Transparent Bridge

Infos relatives aux stations actives
chaque entrée est associée à un *inactive timer*

Forwarding Data Base

@ station	port
1	1
2	1
3	2
4	2
5	2
6	2

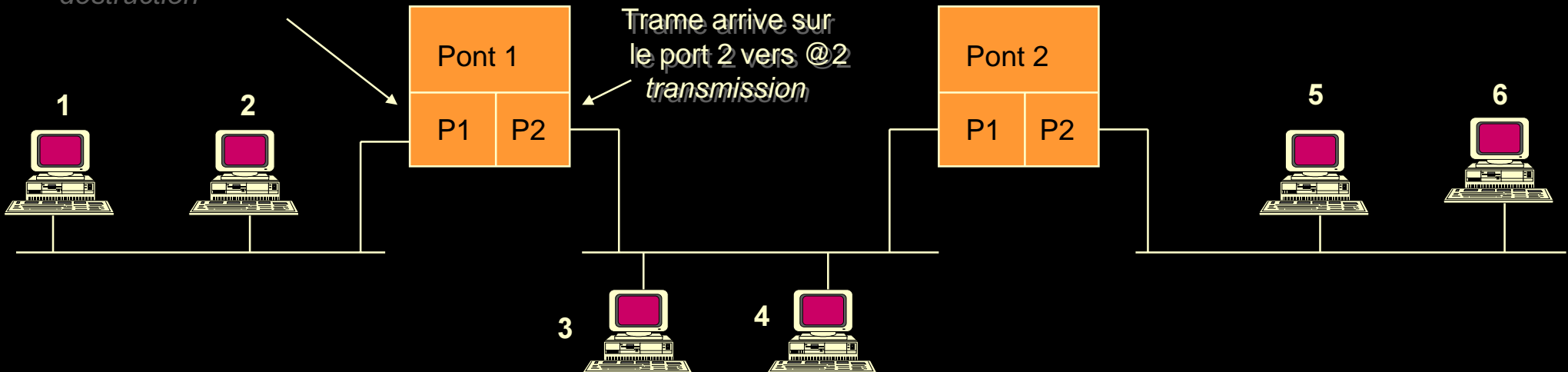
Forwarding Data Base

@ station	port
1	1
2	1
3	1
4	1
5	2
6	2

Indique le port de sortie

Trame arrive sur le port 1 vers @2
destruction

Trame arrive sur le port 2 vers @2
transmission



Transparent Bridge

- Autoapprentissage

- à la mise en service : FDB vide

- réception d'une trame

- @ source et le port d'arrivée dans la FDB

- port de transmission inconnu : copie de la trame sur tous les autres ports (mécanisme de *flooding*)

- tous les segments sont concernés

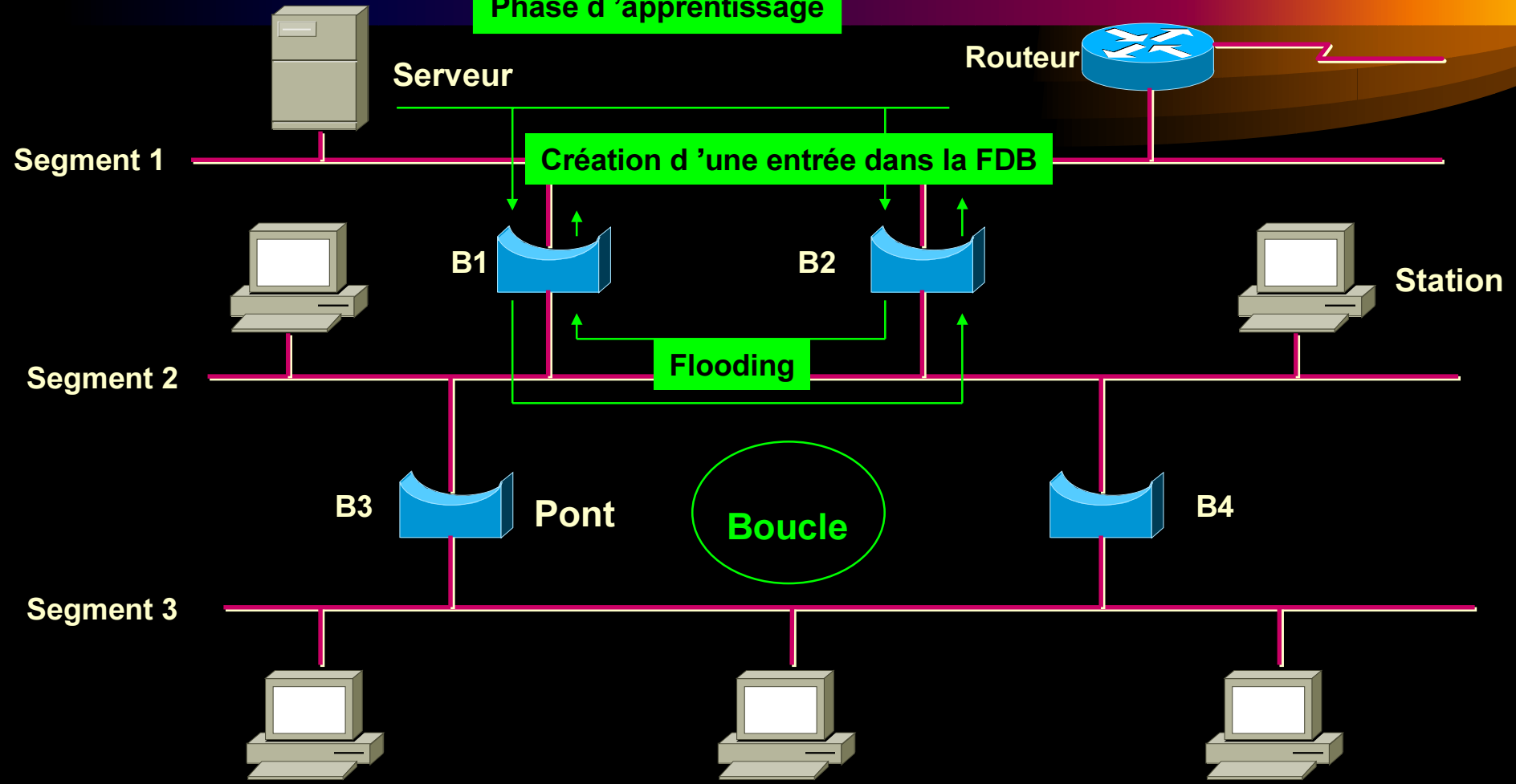
=> convergence rapide du processus (spanning tree)



IEEE 802.1D

Les boucles

Phase d'apprentissage



Solution au problème du bouclage : Algorithme du spanning Tree

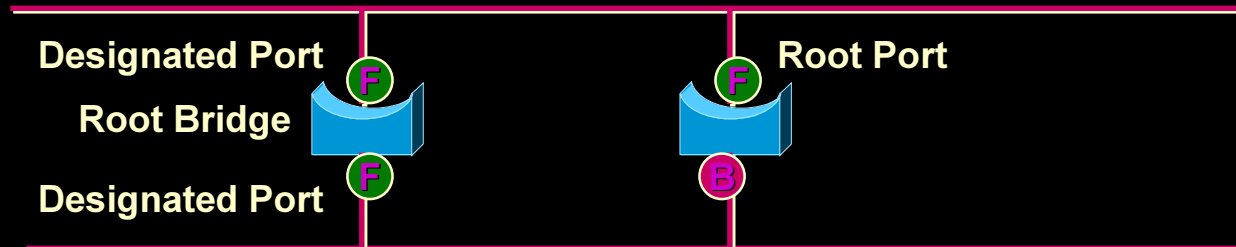
Spanning Tree

Concepts

- **BPDU**
 - Bridge protocol Data Unit
- **Bridge Types**
 - Root Bridge
 - Designated Bridge
- **Port Types**
 - Root Port
 - Designated Ports
- **Port States**
 - Blocking
 - Listening
 - Learning
 - Forwarding

Spanning Tree



Segment 1



Segment 2



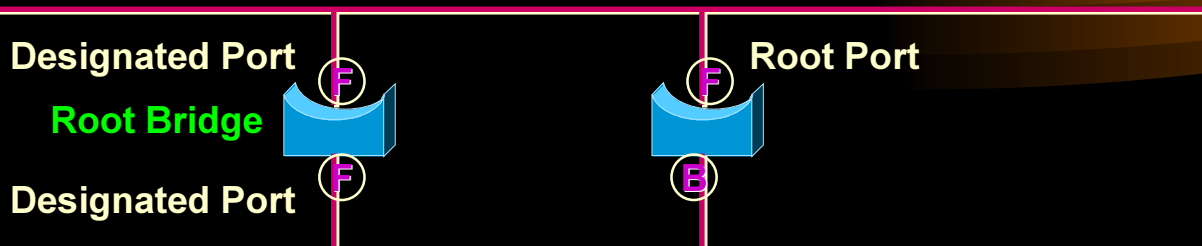
Segment 3

 Blocked Port  Forwarding Port

Spanning Tree

Root Bridge

Segment 1



Segment 2



Segment 3

(B) Blocked Port (F) Forwarding Port

- Un par réseau
- Processus d'élection
- Confirmé/Elu à intervalle régulier
- Configure les timers des autres ponts
- Tous les autres ponts calculent le chemin le plus court vers le « root bridge » (« least root path cost »)

Spanning Tree

Root Port

Segment 1



Segment 2



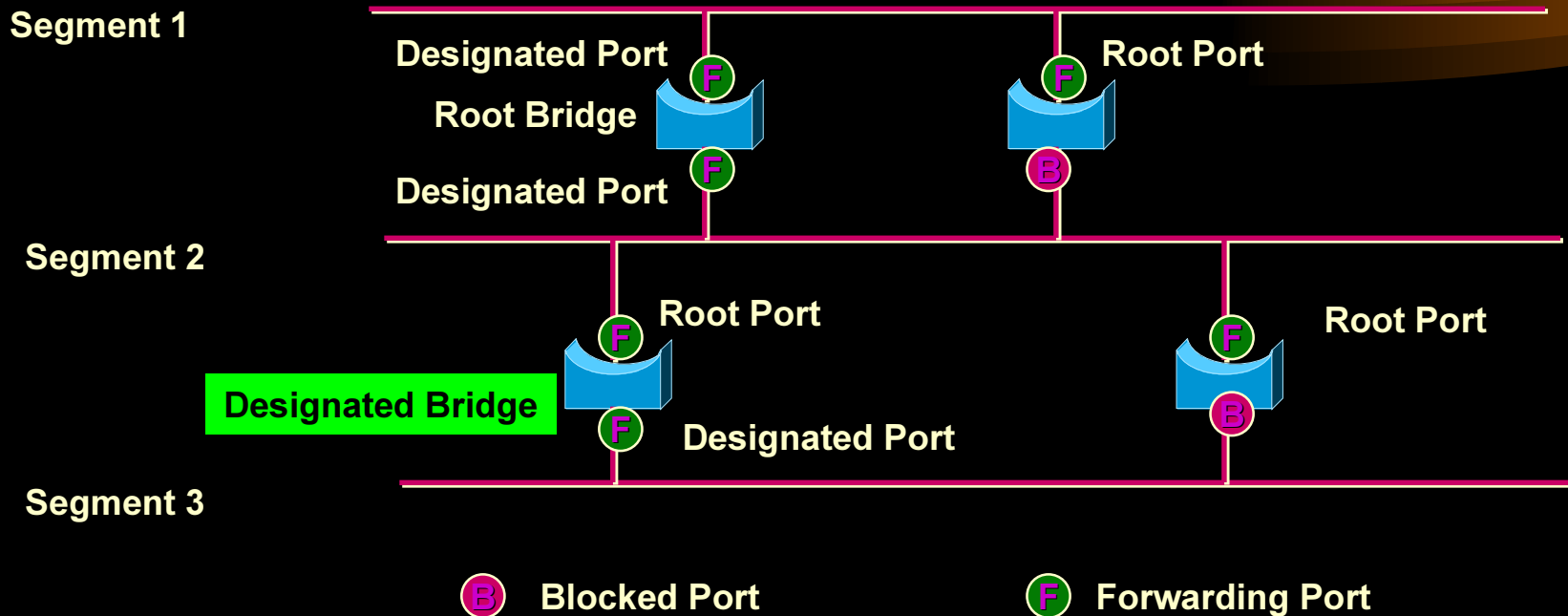
Segment 3

(B) Blocked Port (F) Forwarding Port

- Un port pont
- Port au « least root path cost »
- Il reçoit toutes les BPDU envoyées par le « root bridge »
- Etat du port : jamais bloquant

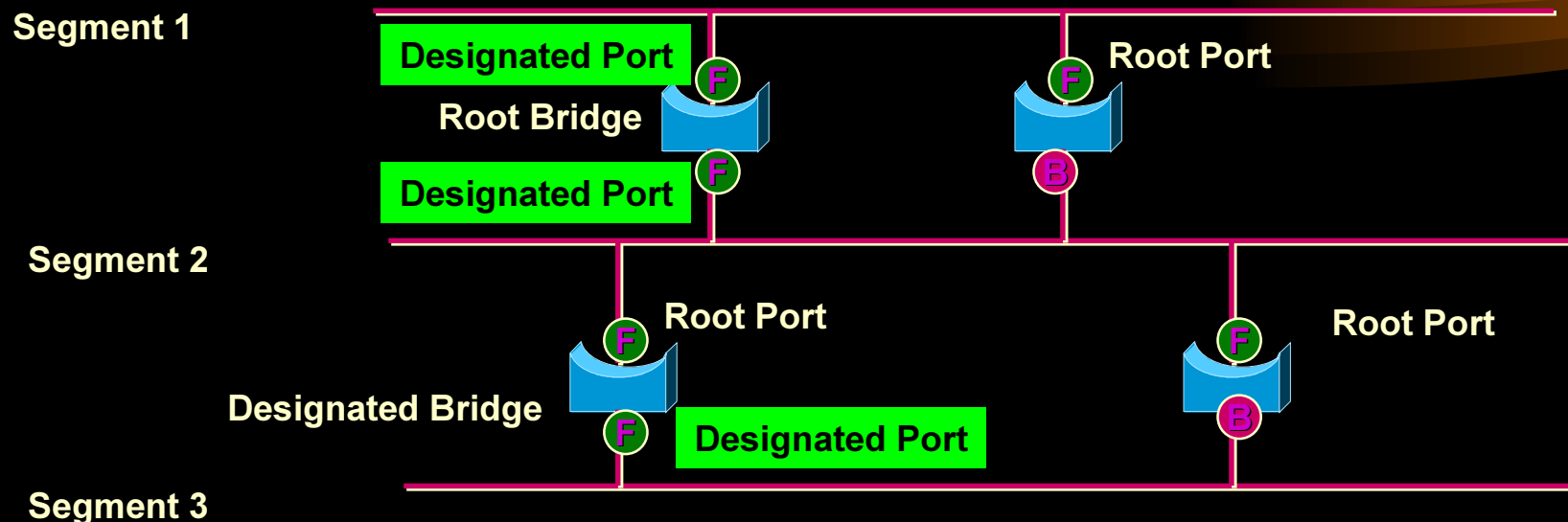
Spanning Tree

Designated Bridge



- Au moins un par segment : transmet les trames sur chaque segment
- Le root bridge est toujours « Designated bridge » pour le segments qu 'il connecte
- Toujours le pont avec le plus court chemin vers le « root bridge »

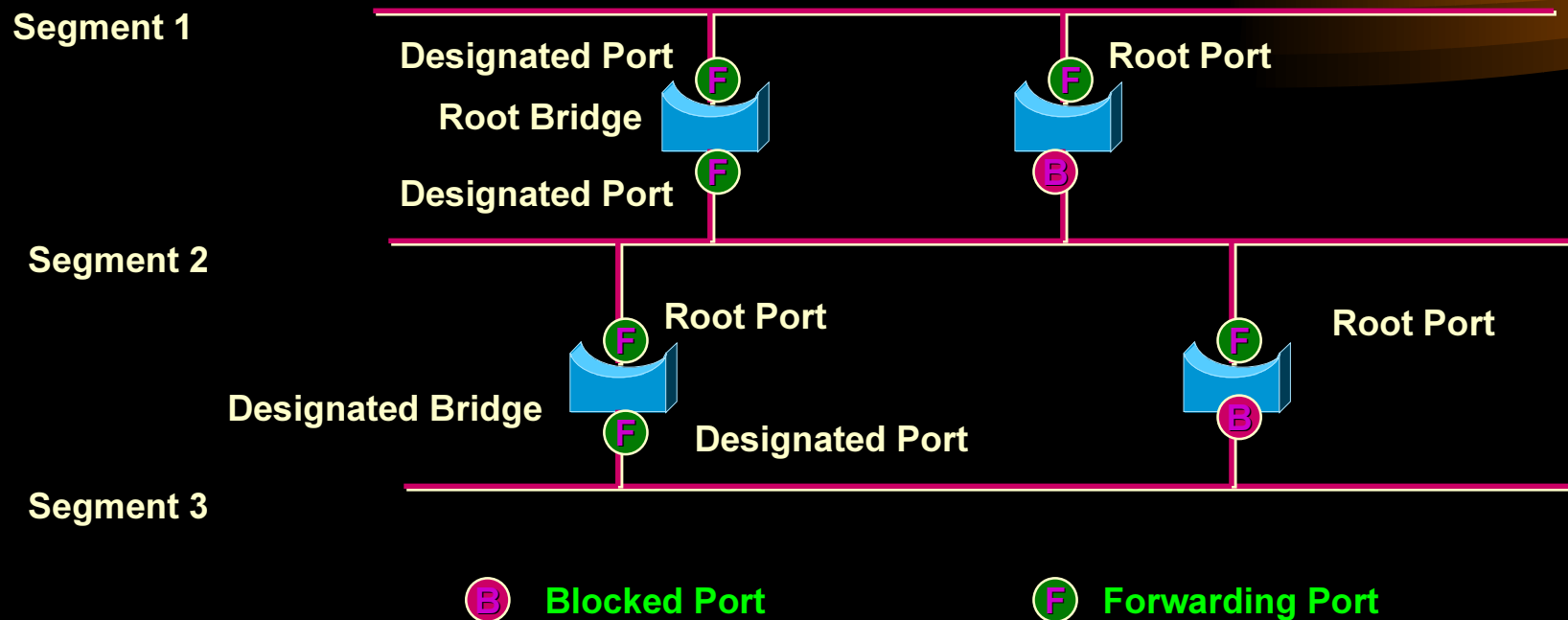
Designated port



- Port connectant le « Deignated Bridge » au segment, choisi
- Tous les trafics qui sortent du segment
- Transmission de BPDU vers les autres ponts
- Jamais dans un état bloquant

Spanning Tree

Port States



- Blocking : Pas de trafic à travers ce port, reçoit seulement les BPDU
- Listening : Pas de trafic à travers ce port, stoppe les BPDU reçues
- Learning : Pas de trafic à travers ce port, construit sa FDB
- Forwarding : Trafic utilisateur, transmission et réception de BPDU

Spanning Tree

Paramètres de configuration

- Paramètres réseau

- Hello interval

- Fréquence à laquelle un « designated port » envoie des BPDU, 2 s par défaut.

- Forward delay

- Passage de l'état « listening, learning » à l'état « forwarding », 15 s par défaut

- Max age

- Pseudo TTL pour les BPDU

- Bridge priority (per bridge)

- Intervalle 1-32768, valeur par défaut 32768

- Paramètres liés au port

- Port cost

- Coût de transmission d'une trame sur un segment

- Path cost

- coût total vers le « root bridge »

- lors de l'envoi d'une BPDU, le « port cost » du port précédent qui a reçu la BPDU est ajouté

- Par défaut : 1000/Débit en Mbps

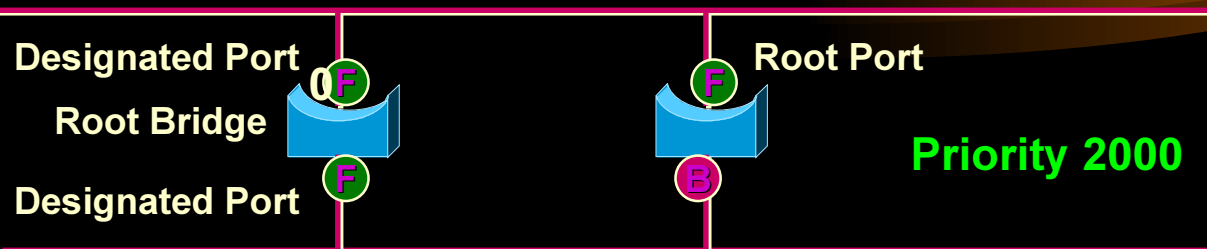
- 10 Base T = 100, 100 Base FX, FDDI = 10, ATM = 6

- Port priority

Spanning Tree

Segment 1

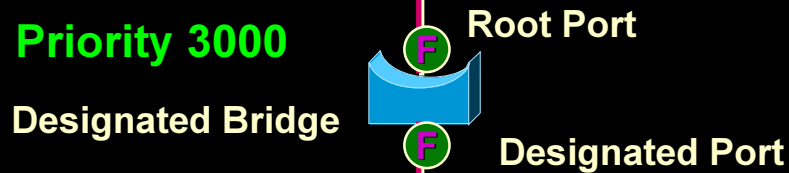
Priority 1000



Priority 2000

Segment 2

Priority 3000



Priority 32768

Segment 3

(B) Blocked Port

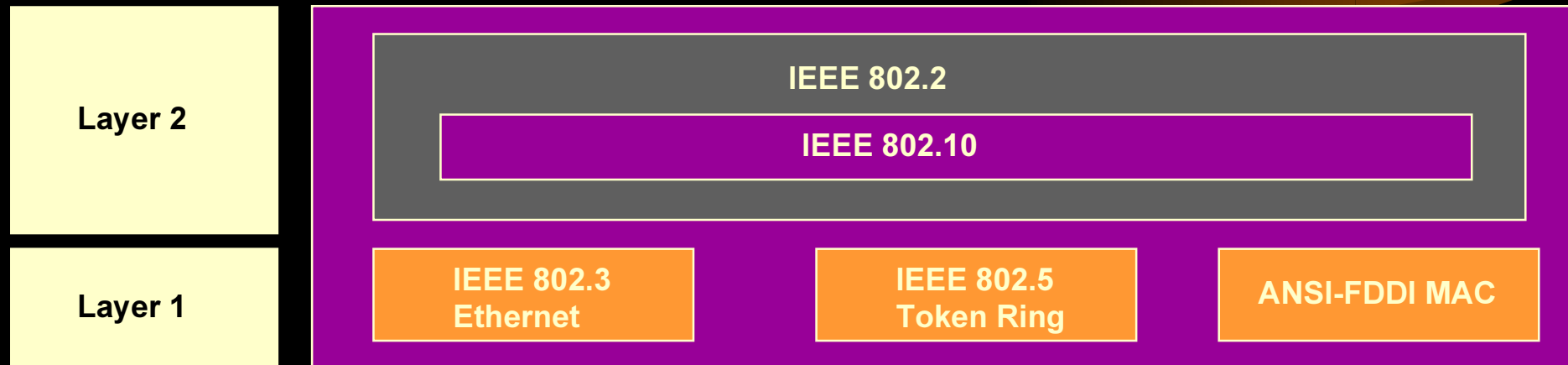
(F) Forwarding Port



All ports have a cost of 100

- Messages de changement de topologie
- En direction du « root bridge »
- Envoyés à chaque transition d'un port dans l'état « forwarding ».

IEEE 802.10



- IEEE 802.10 correspond aux besoins de segmentation du trafic et de sécurité dans les réseaux LAN/MAN
 - à la base, gestion des Groupes Fermés d'Abonnés
- Indépendance vis à vis des équipements intermédiaires
- Son utilisation semble être limité à FDDI

IEEE 802.1p

- Extension de IEEE 802.1D pour le support dans les LANs "bridgés"
 - Classes de trafic
 - priorisation du trafic dans les commutateurs
 - permettre le trafic temps réel dans les commutateurs
 - la priorité est alloué
 - au niveau MAC sur le protocole (ex 802.3)
 - au niveau des adresses MAC des entités
 - pas de QoS, pas de contrôle de flux
 - Filtrage dynamique du multicast
 - protocole GARP
 - Generic Attribute Registration Protocol*
 - identique à IGMP mais au niveau 2
 - Internet Group Management Protocol*

Virtual Bridged Local Area network

- Standard VLAN pour des LAN commutés/bridgés
- Construit sur IEEE 802.1D et IEEE 802.1P
- Marquage des trames
 - Etiquette implicite
 - Pas d'étiquette dans la trame
 - Appartenance d'une trame à un VLAN basée sur son contenu (@MAC,@IP) et le port
 - Etiquette explicite
 - Etiquette dans la trame
- Supporte la priorisation
- Draft Standard P802.1Q/D11

Virtual Bridged Local Area network

- Trame IEEE 802.3



Tag Header

User Priority

VID

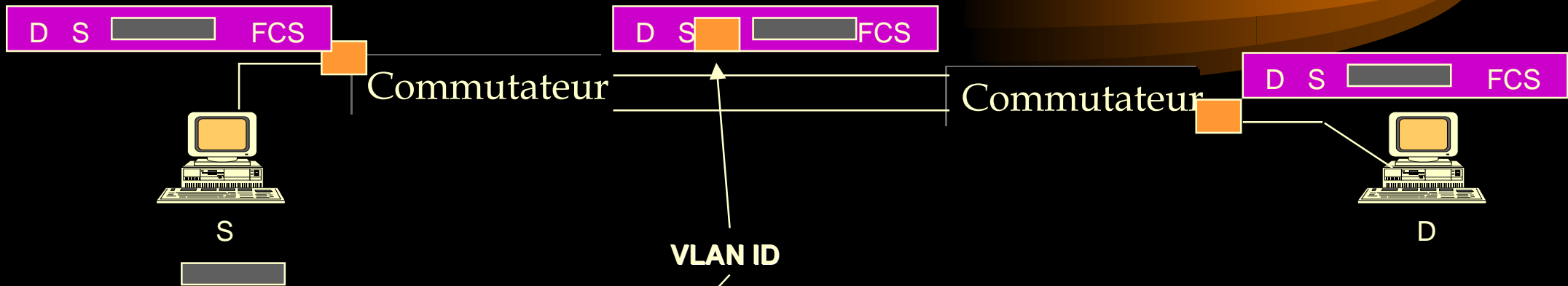
12 bits = 4096 identificateurs

VID VLAN Identifier

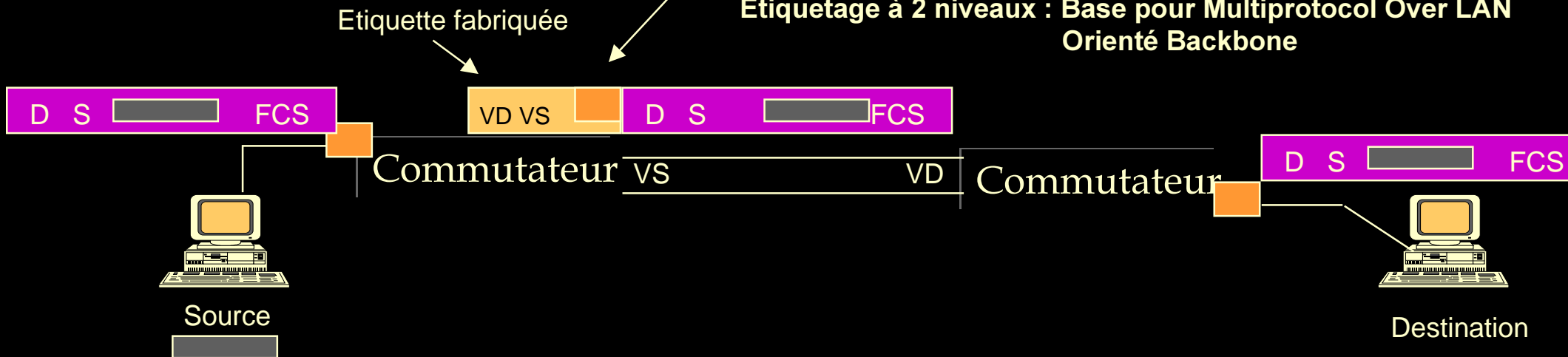
CFI Canonical Format Indicator

Etiquette explicite

Etiquetage à 1 niveau : simple marquage des trames



Etiquetage à 2 niveaux : Base pour Multiprotocol Over LAN Orienté Backbone



Règles de design des VLAN

- Questions ?
 - nombre d'utilisateurs ?
 - plan du campus
 - les utilisateurs qui partagent des données sont-ils géographiquement proches ?
 - plan de câblage du campus
 - les changements sont-ils le fait de départements ou d'utilisateurs isolés ?
 - quel est le trafic sur le campus ?
 - les ressources sont centralisées ou distribuées ?
 - applications multimédia en perspectives ?

Le "backbone"



- Choix de la technologie
 - Fast ethernet
 - Gigabit ethernet
 - ATM 155 Mbps, 622 Mbps (PNNI Phase 1)
- Ne doit jamais être saturé
 - règle des 80/20
 - garantir un bon temps de réponse aux applications
- Liens multiples
 - répartition de charge
 - redondance
- Evolution et stabilité
 - Spanning Tree par VLAN

Les "broadcasts"

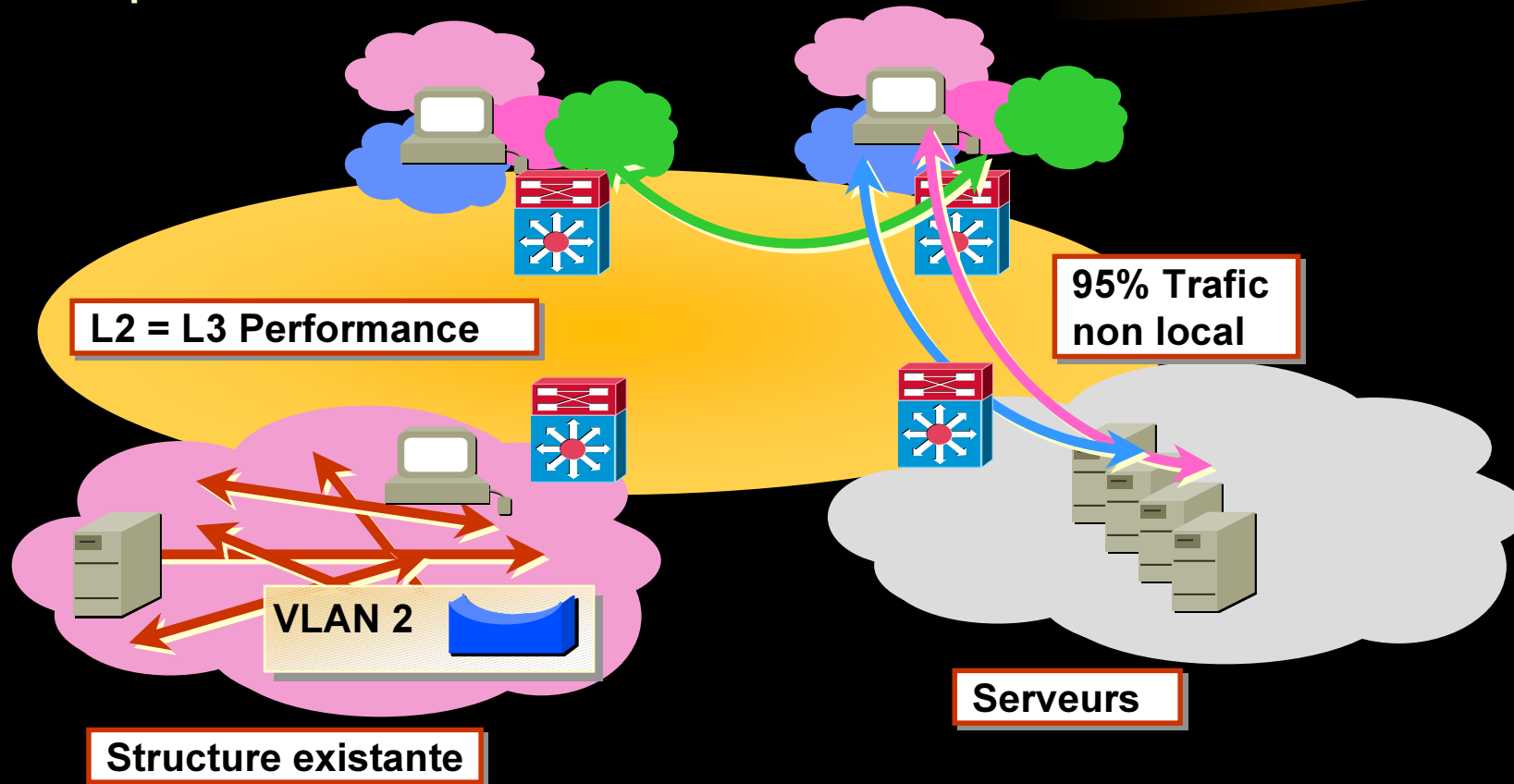
- Les broadcasts et les multicasts interrompent tous les matériels sur le réseau
 - traitement au niveau du CPU
- Taille d'un domaine de broadcast
 - IP < 500 stations
 - la classe C est un moyen pratique de limitation
 - IPX < 300 stations
 - Appletalk < 200 stations

Accès à des serveurs d'applications

- Serveurs centralisés géographiquement
 - liaisons haut-débit
- Les groupes de travaux, les services sont séparés logiquement avec des serveurs dédiés.
- Liens haut-débit pour interconnecter les VLANs
 - Le routage et la sécurité se font au niveau 3
- Architecture indépendante des technologies
 - LAN, ATM

Campus Architecture VLAN

- Commutateurs multi-niveaux L2-L3
- Contrôle par « Access Lists »
- Services haute-performance



Architecture VLAN

- Les utilisateurs sont membres d'un VLAN donné, indépendamment des déplacements physiques.
- Chaque VLAN peut avoir un jeu de règles de sécurité pour l'ensemble de ses membres.
- Aujourd'hui, le trafic est principalement local, les performances des commutateurs de niveau 3 ne sont pas requises.

Administration des VLANs

- Disposer d'outils graphiques
 - "Drag & drop" pour la configuration des ports
 - Suivi de configuration par VLAN
 - à travers le réseau
 - topologie par VLAN
 - Mise en oeuvre et configuration centralisées
 - Configuration des liens redondants basée sur des chemins préférentiels
 - Outils pour "régler" le réseau
 - problème de la visibilité dans les réseaux commutés



Administration des VLANs

Analyse de trafic
 Surveillance active
 Défaillances
 Rapports d'activité

RFC 2222

