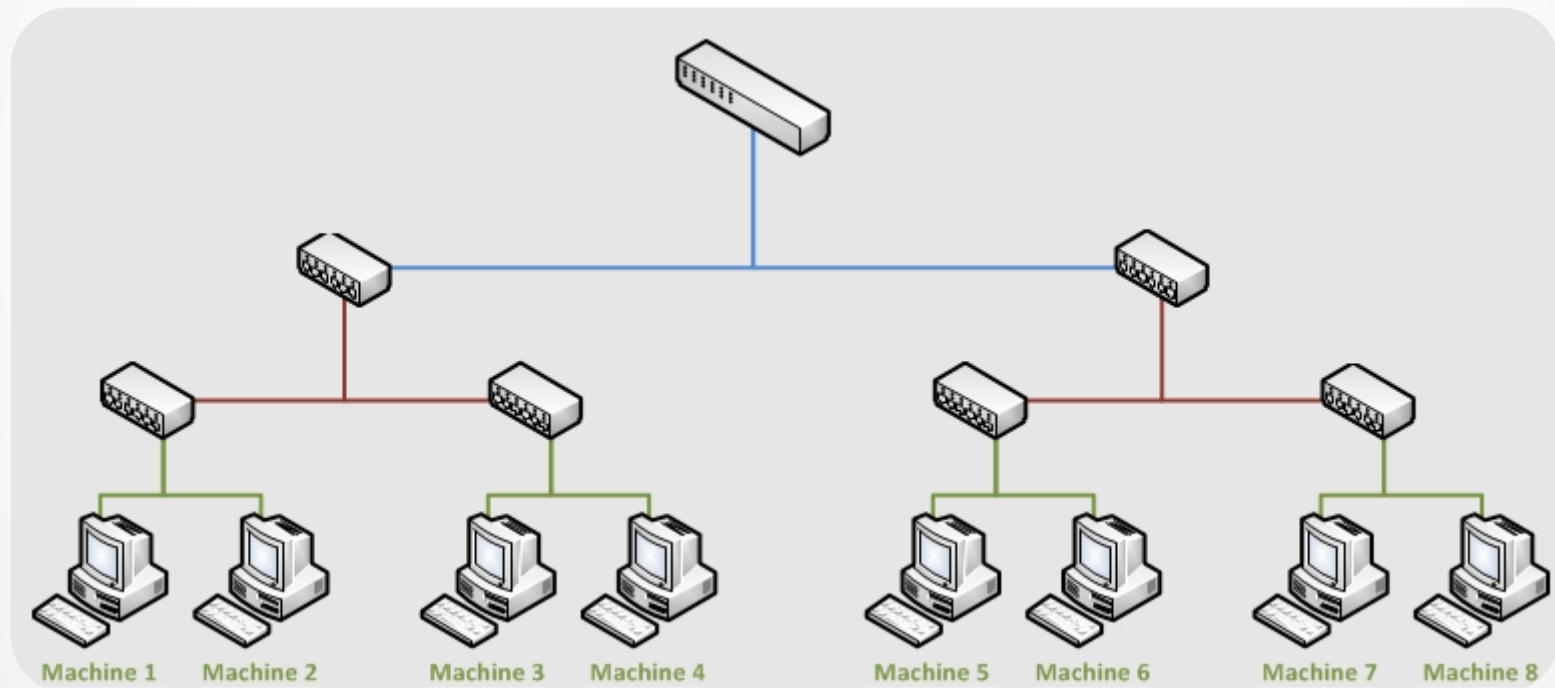


R103 : Réseaux locaux et équipements actifs.



Ressource R103 Réseaux locaux et équipements actifs	
Semestre	1
Heures	Formation encadrée 27h, dont 16h de TP
Compétence(s) ciblées, coefficient(s) et apprentissage(s) critique(s) couvert(s)	
RT1-Administrer Niveau 1 coef. 8	RT2-Connecter Niveau 1 coef. 4
AC0113 Configurer les fonctions de base du réseau local AC0115 Identifier les dysfonctionnements du réseau local AC0116 Installer un poste client	RT3-Programmer Niveau 1 coef. 0 AC0311 Utiliser un système informatique et ses outils
SAÉ concernée(s)	SAÉ11 Se sensibiliser à l'hygiène informatique et à la cybersécurité SAÉ12 S'initier aux réseaux informatiques SAÉ13 Découvrir un dispositif de transmission
Prérequis	R101 Initiation aux réseaux informatiques
Descriptif	<p>Cette ressource apporte le socle de connaissances et savoirs-faire pour les compétences de cœur de métier «Administrer les réseaux et l'Internet» (RT1). Elle vise à fournir à l'étudiant les connaissances et les compétences indispensables pour pouvoir concevoir, déployer et maintenir l'infrastructure réseau informatique de l'entreprise (Ethernet).</p> <p>La compétence RT1 est renforcée à travers la mise en place et la configuration de matériels actifs comme des commutateurs, la gestion de la sûreté de fonctionnement du réseau local Ethernet (spanning tree) et la participation à la sécurisation du système d'information dont il est le support (segmentation physique et virtuelle, VLAN). Ces deux compétences s'appuient sur la compréhension des mécanismes intrinsèques aux réseaux locaux Ethernet : adressage MAC, commutation/routage de niveau 2, ARP, passage d'un type de support physique à un autre, changements de débit.</p> <p>Pour la compétence «Connecter les entreprises et les usagers» (RT2), elle aborde les notions d'exploitation du câblage (brassage).</p> <p>Elle contribue aussi à la compétence «Créer des outils et applications informatiques pour les R&T» (RT3) à travers la découverte du poste client et de son environnement logiciel.</p>
Contenus	<ul style="list-style-type: none"> • Câblage réseaux. • Différentes topologies physiques et logiques. • Normalisation Ethernet 802 (802.1, 802.2, 802.3). • Commutation Ethernet : apprentissage des adresses MAC, diffusion, Broadcast. • Différents équipements actifs : commutateur, routeur. • Configuration d'un réseau segmenté en VLAN, lien multi-vlan, communication inter-vlan. • Redondance et détection de boucles dans un réseau commuté : STP, RSTP. <p>Sur chaque thème, faire le lien avec les notions de cybersécurité abordées en R101.</p>
Mots-clés	Réseaux locaux, Ethernet, commutateurs, routeurs, VLAN, 8021Q, 8021P, STP, RSTP.

Rappels : Equipement :

ses caractéristiques et paramètres d'identification



Carte réseau : interface réseau \Leftrightarrow débit maximum

Adresse MAC : Propre à chaque interface réseau

Adresse IP :

- Définie par l'utilisateur en fixe
- Via un serveur DHCP

- Commande en ligne windows : `ipconfig /all`
- Modification adresse IP windows :
=>Centre réseau et partage/Modifier paramètre de la carte/Propriété de la carte réseau/Protocol internet IPV4

- Commande en ligne linux : `ifconfig /all`
- Modification adresse IP linux : `nano /etc/network/interfaces`

Rappels : Equipement : ses caractéristiques et paramètres d'identification

```
C:\>ipconfig /all

Configuration IP de Windows

    Nom de l'hôte . . . . . : PORTABLE
    Suffixe DNS principal . . . . . :
    Type de noud . . . . . : Inconnu
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non

Carte Ethernet Connexion au réseau local:

    Statut du média . . . . . : Média déconnecté
    Description . . . . . : SiS 900-Based PCI Fast Ethernet Adapter
    Adresse physique . . . . . : 00-40-C8-51-85

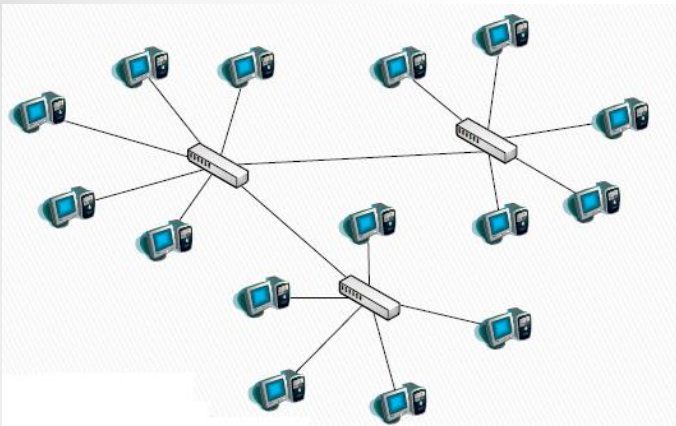
Carte Ethernet Connexion réseau sans fil:

    Suffixe DNS propre à la connexion :
    Description . . . . . : Realtek RTL8180 Wireless LAN (Mini-)
    Adresse physique . . . . . : 00-0F-66-C9-59-AA
    DHCP activé . . . . . : Oui
```

Numéro constructeur	Constructeur	Numéro constructeur	Constructeur
00-00-0C	Cisco	08-00-02	3Com-bridge
00-00-0F	Next	08-00-05	Symbolics
00-00-10	Sytek	08-00-06	Siemens Nixdorf
00-00-1D	Cabletron	08-00-07	Apple
00-00-2A	TRW	08-00-09	HP
00-00-5E	IANA	08-00-0A	Nestar systems
00-00-65	Network general	08-00-0B	Unisys
00-00-6B	MIPS	08-00-10	AT&T
00-00-77	MIPS	08-00-11	Tektronics
00-00-81	Synoptics	08-00-14	Excelan
00-00-89	Cayman systems	08-00-20	Sun

Rappels : L'interconnexion des équipements : Topologie physique et distance

Topologie Etoile étendue : la plus utilisée dans les réseaux locaux.

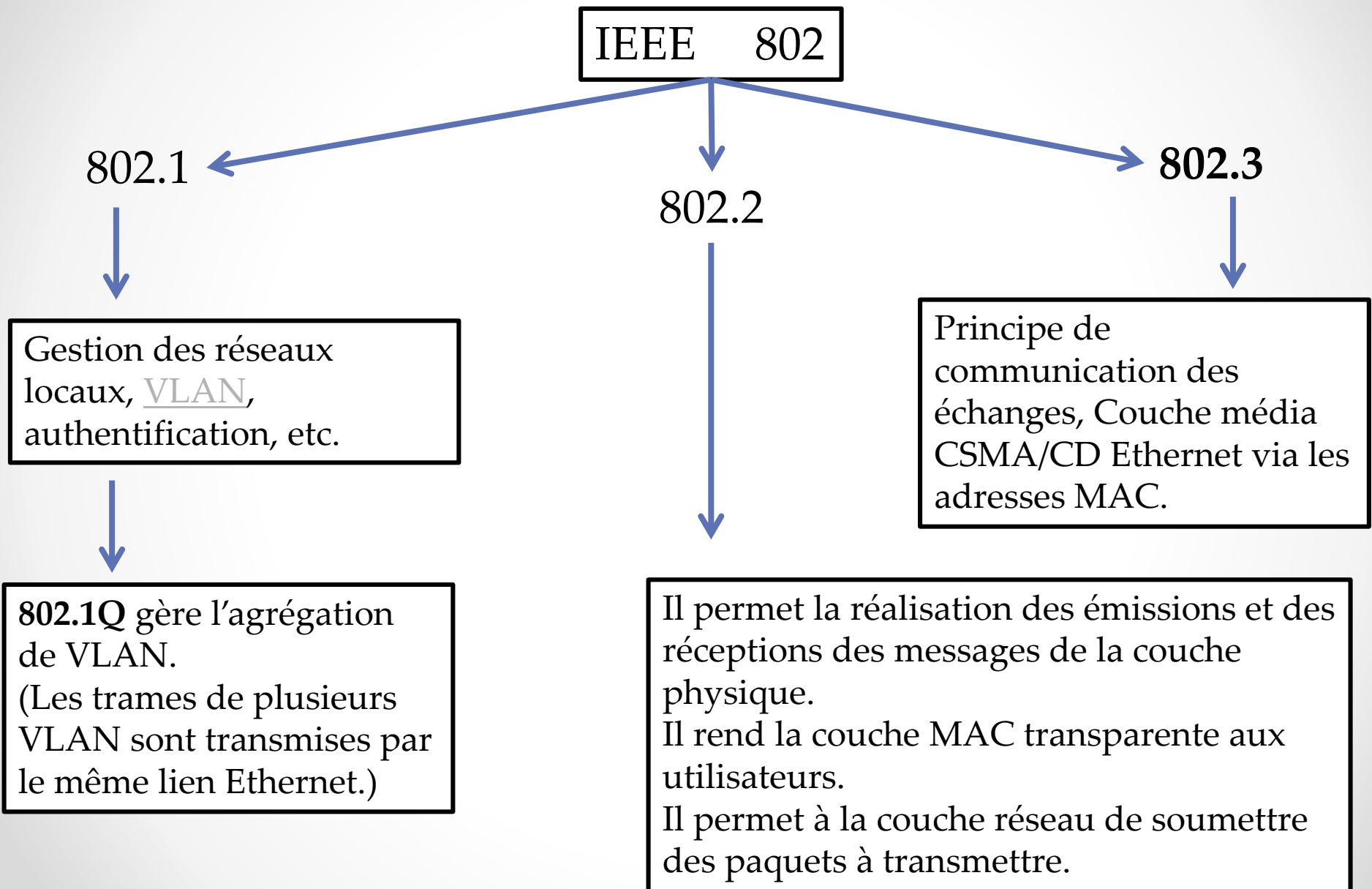


- Prise en compte des distances entre équipements :

Speed	Compatible Cable
10G	CAT6a (100m)
	CAT6 (55m)
	CAT5e (30m)
5G	CAT6 (100m)
	CAT5e (30m)
2.5G	CAT5e (100m)
1G	CAT5e (100m)
100M	CAT5 (100m)

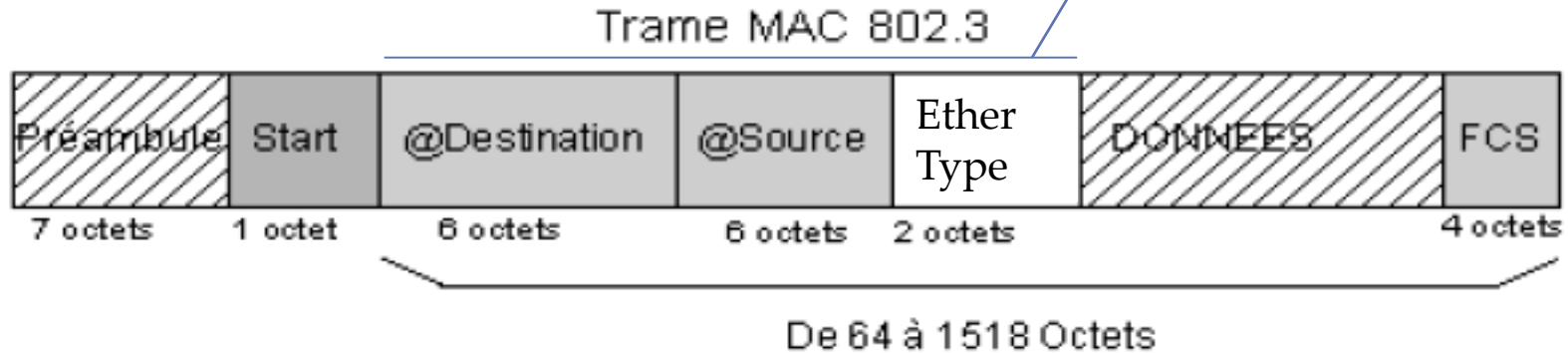
- Prise en compte des débits voulu (10/100/1000 Mbits/s voir 10Gbits/s)
- Prise en compte du nombre de machines
- Ethernet : Utilisation des adresses MAC des interfaces réseaux pour communiquer

La technologie Ethernet : Norme IEEE 802



La technologie Ethernet : Norme IEEE 802

Les trames Ethernet 802.3



Préambule : Permet la synchronisation des horloges de transmission. Il s'agit d'une suite de 1 et de 0 soit 7 octets à la valeur 0xAA.

Start : Il s'agit d'un octet à la valeur 0xAB. Il doit être reçu en entier pour valider le début de la trame

Frame Check Sequence : Ensemble d'octets permettant de vérifier que la réception s'est effectuée sans erreur.

EtherType	Protocole
0x0800	IPv4
0x0806	ARP
0x809B	AppleTalk
0x8035	RARP
0x86DD	IPv6

Exemple de frame :

- Broadcast

ff	ff	ff	ff	ff	ff	ac	81	12	82	eb	29	08	06	00	01
08	00	06	04	00	01	ac	81	12	82	eb	29	c0	a8	02	7c
00	00	00	00	00	00	c0	a8	02	be						

- Unicast

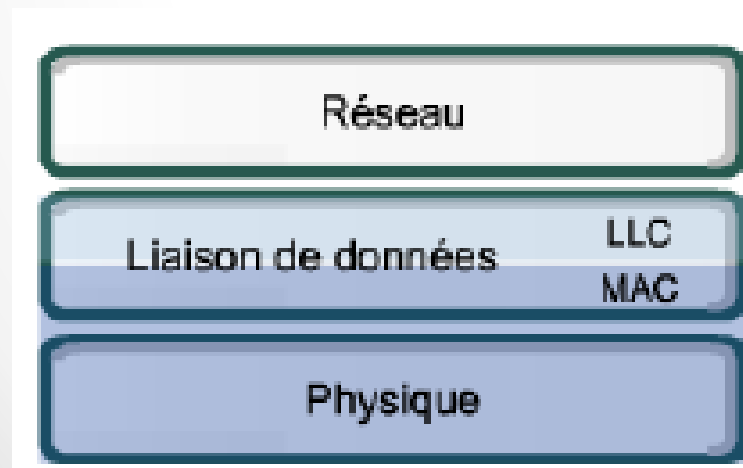
2c	d0	5a	15	f7	97	ac	81	12	82	eb	29	08	06	00	01
08	00	06	04	00	02	ac	81	12	82	eb	29	c0	a8	02	7c
2c	d0	5a	15	f7	97	c0	a8	02	be						

La technologie Ethernet : Norme IEEE 802

IEEE 802.2

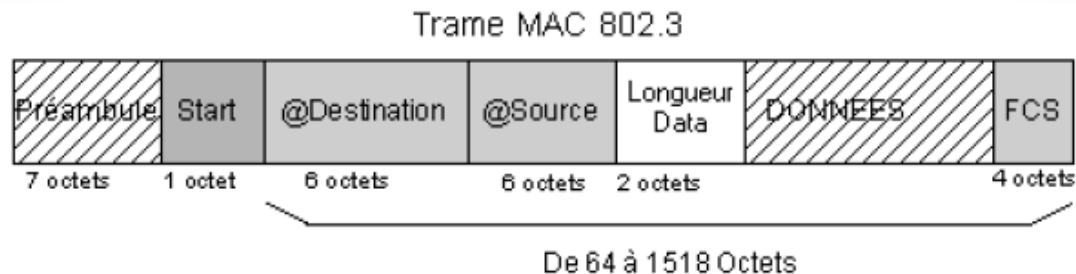
- Il permet la réalisation des émissions et des réceptions des messages de la couche physique.
- Il rend la couche MAC transparente aux utilisateurs.
- Il permet à la couche réseau de soumettre des paquets à transmettre.

Extrait modèle OSI :



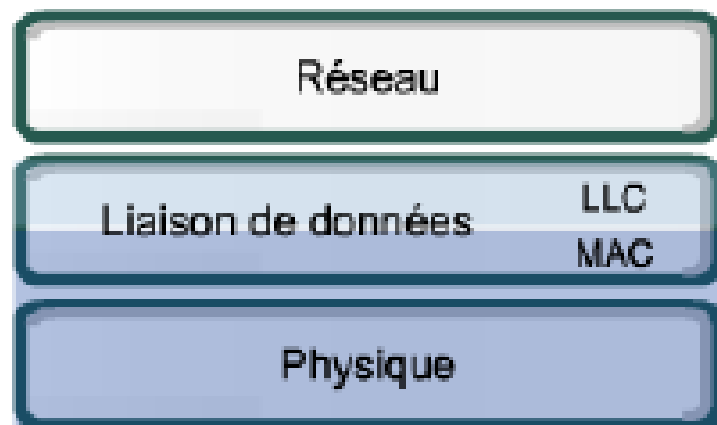
La technologie Ethernet : Norme IEEE 802

Principe de réception des trames destinées ou non, diffusion broadcast et unicast



- Si trame broadcast ? Exemple : FF:FF:FF:FF:FF:FF
- Si trame unicast ? Exemple : 80:C0:F6:A0:4A:B1

Extrait modèle OSI :



Adresse MAC : 2C-41-38-08-96-33

La technologie Ethernet : Utilisation des adresses MAC

- Dans un réseau Ethernet \Leftrightarrow échange via adresse MAC

Test connexion basic du PC0 vers PC1 : ping @_IP_PC

Premier test de communication :

- Envoie frame depuis le PC0 à l'ensemble du réseau : requête ARP
- Réponse du PC1 : réponse ARP

Renseignement table ARP du PC 0 et PC1

- Envoie frame depuis le PC0 test de la connexion : requête ICMP
- Réponse du PC1 : réponse ICMP

Second test de communication :

- Envoie frame depuis le PC0 vers PC1: requête ICMP
- Réponse du PC1 : réponse ICMP

La technologie Ethernet : Utilisation des adresses MAC

- Commande ping 10.0.0.1,
- arp -a,
- arp -d

```
C:\Users\Administrateur>arp -a

Interface : 10.205.205.80 --- 0xc
  Adresse Internet    Adresse physique    Type
  10.250.250.12       bc-30-5b-d7-14-2a   dynamique
  10.250.250.101      00-22-64-8a-8c-e1   dynamique

C:\Users\Administrateur>ping 10.0.0.1

Envoi d'une requête 'Ping' 10.0.0.1 avec 32 octets de données :
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.0.0.1:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
^C
C:\Users\Administrateur>arp -a

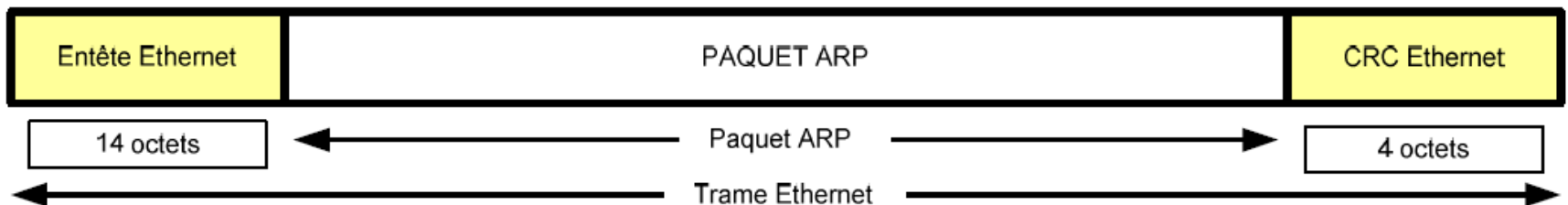
Interface : 10.205.205.80 --- 0xc
  Adresse Internet    Adresse physique    Type
  10.0.0.1            00-0a-f7-86-09-71   dynamique
  10.250.250.12       bc-30-5b-d7-14-2a   dynamique
  10.250.250.101      00-22-64-8a-8c-e1   dynamique
  10.250.250.141      00-e0-b1-d1-7c-ab   dynamique
```

La technologie Ethernet : Notion d'encapsulation

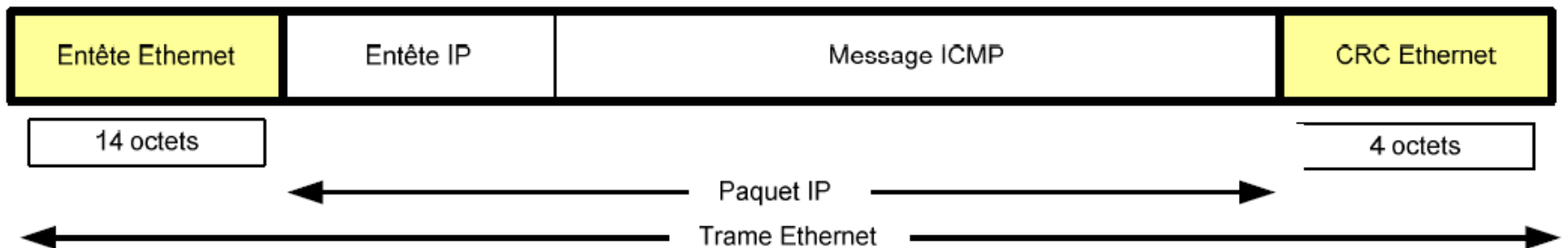
- Chaque couche “encapsule/intègre” la couche supérieure,
- Chaque couche possède ses propres structures de données
- Permet d'acheminer, de router, de démultiplexer ... (Ex : adresse postale)

Exemple :

Paquet ARP :



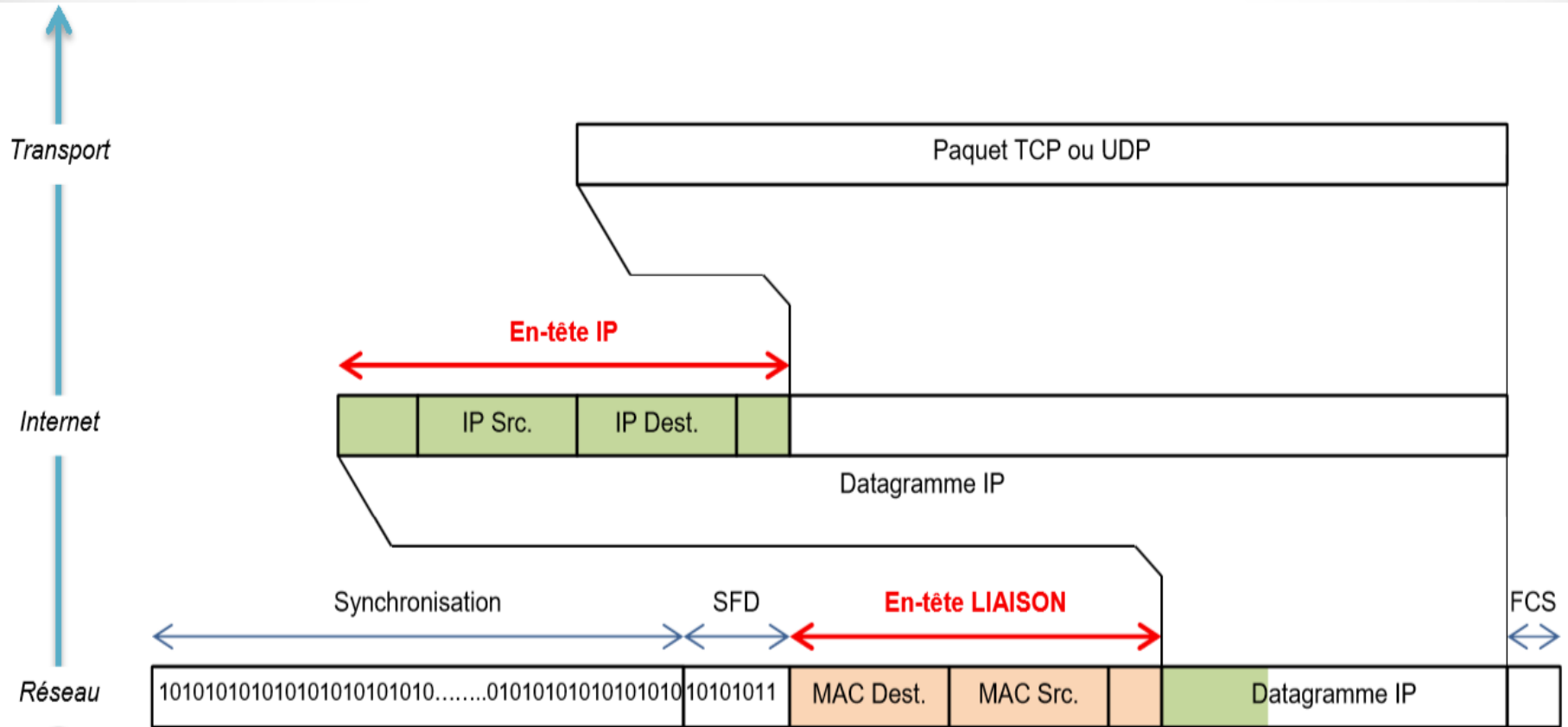
Message ICMP :



La technologie Ethernet : Notion d'encapsulation

C'est la trame que l'on rencontre dans la plupart des réseaux locaux actuels.

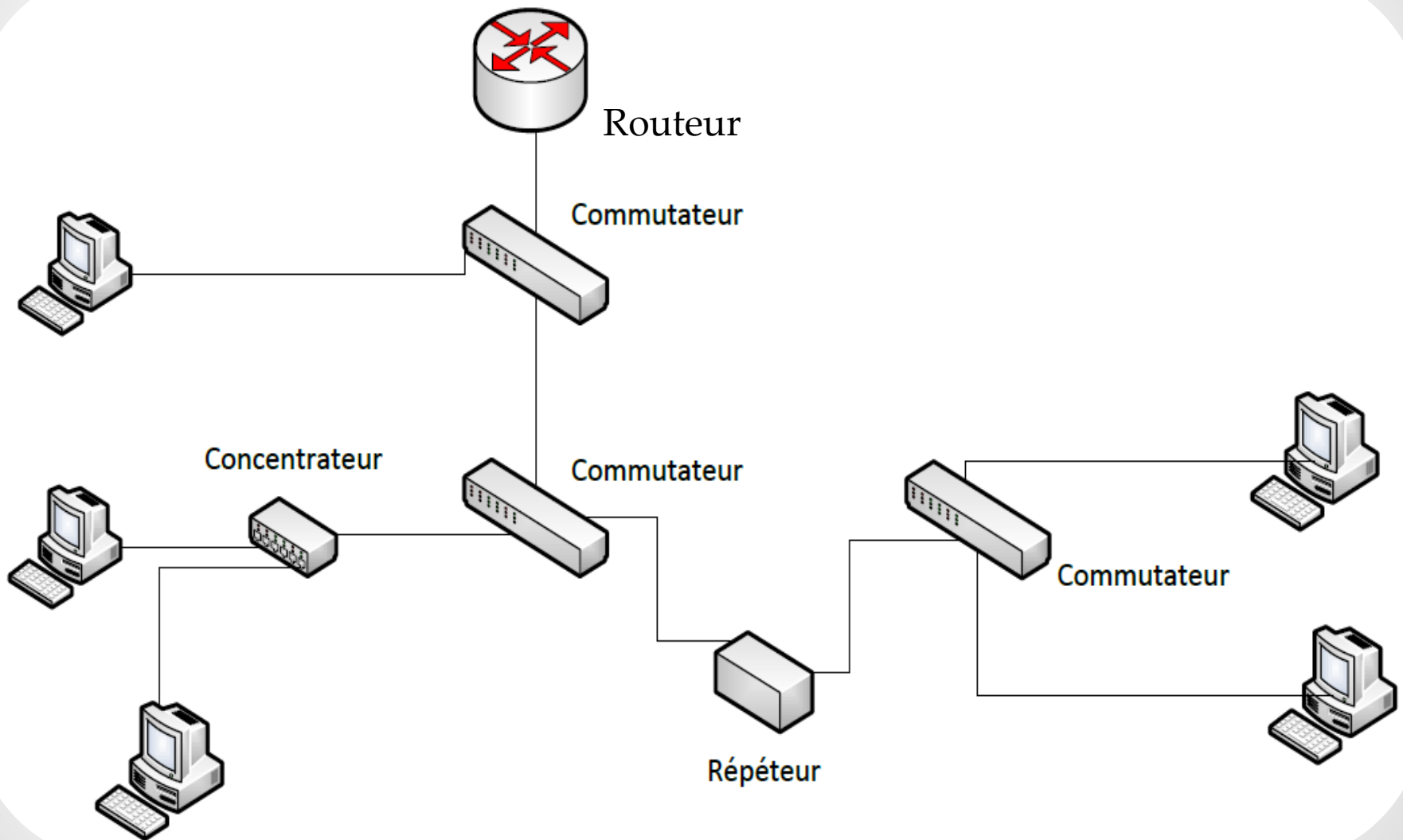
Schéma de la structure



Ce sont ces informations qui circulent sur le réseau

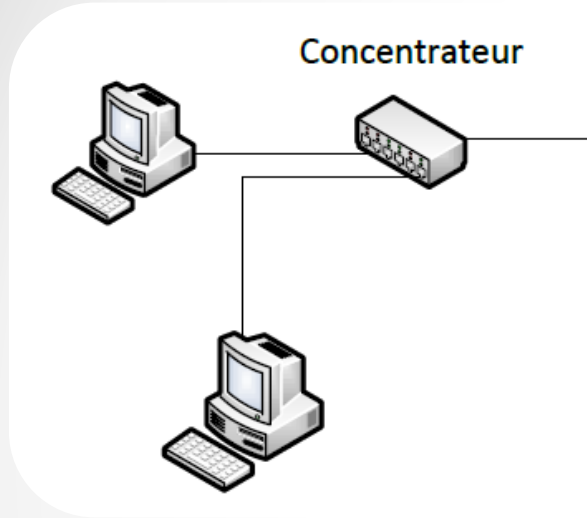
L'inter connexion des équipements : Matériel

Une topologie LAN complète :



L'inter connexion des équipements : Matériel

Les concentrateurs (hub) (matériel obsolète) :



- Il ne fait que récupérer le signal pour le retransmettre sur tous ses ports
- Le réel problème de ce type de concentrateur, c'est justement le renvoi des données vers tous les équipements.
- Ils sont remplacés par les switchs dans tous les réseaux actuels.

L'inter connexion des équipements : Matériel

Les commutateurs administrables (switch) :

Les commutateurs fixes :



Les commutateurs empilables :



Les commutateurs modulaires :

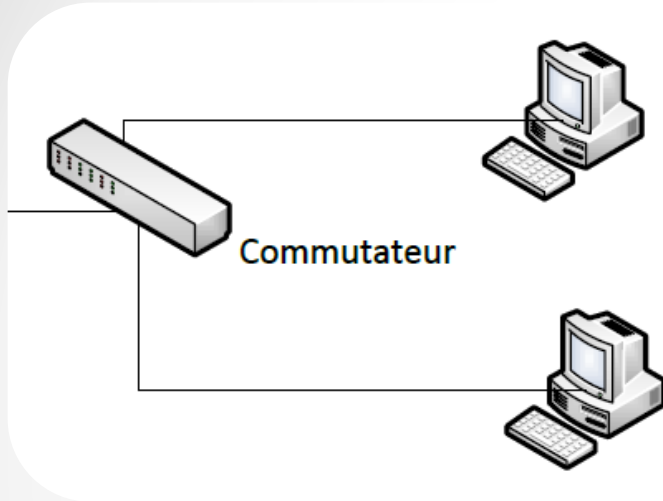


Possibilité de STACK pour :

- Simplifier l'administration (l'ensemble des switchs apparaissent pour l'administrateur comme un seul switch),
- Améliorer la bande passante entre les switchs,
- Améliorer la redondance en cas de panne.

L'inter connexion des équipements : Matériel

Les commutateurs (switch) :

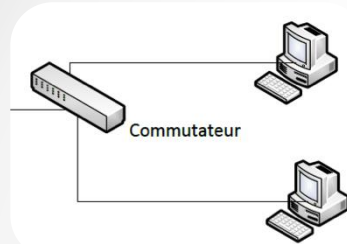


- Il permet d'aiguiller les communications.
- Dispose de phases d'apprentissages. Qui est connecter au port FA0/1, FA0/2...?
- Pendant les communications (hors apprentissage), si une trame est destinée au PC2, il l'envoi uniquement au PC2.
- Cela grâce aux adresses MAC des ordinateurs.
- • Différent type d'interface Ethernet RJ45 ou fibre optique via module SFP



L'inter connexion des équipements : Matériel

Les commutateurs administrables (switch) :

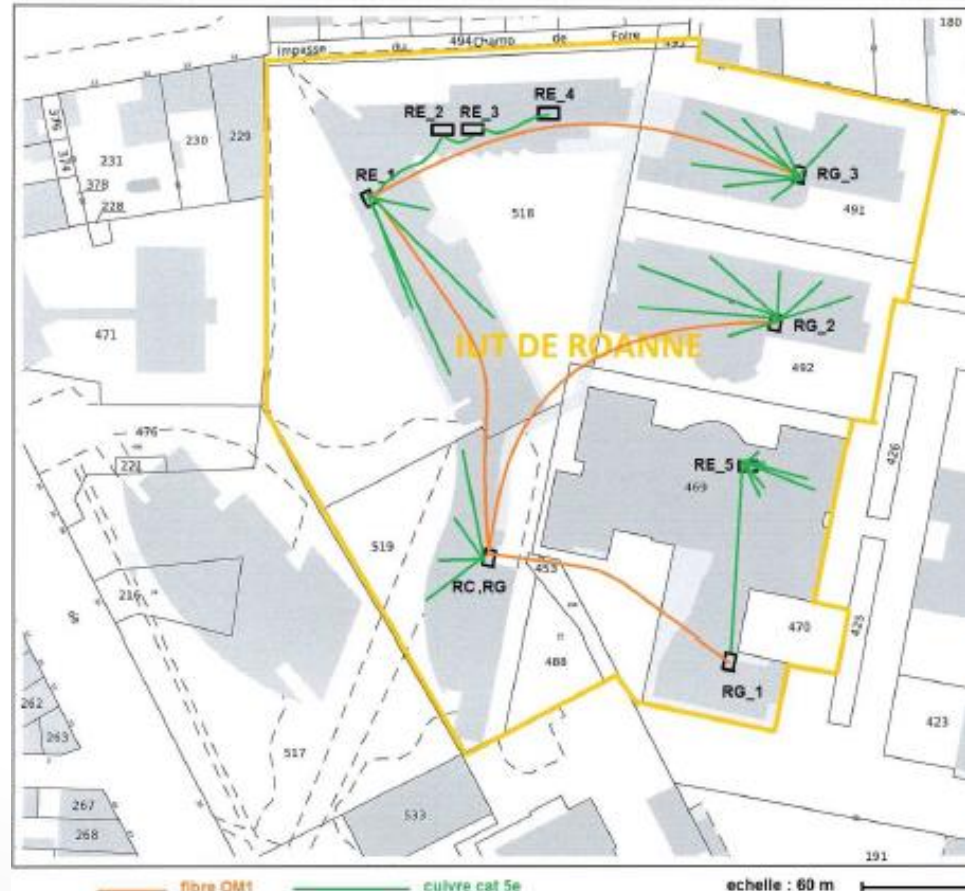


- Permet aussi la création de VLAN.

- VLAN : Réseau local virtuel : Permet de séparer les domaines de diffusion dans un réseau local.

Exemple IUT : Isole une partie administration, d'une partie étudiant, d'une partie service info.

Création de 4 VLANs



L'inter connexion des équipements : Matériel

Les commutateurs administrables (switch) :

Le commutateur dispose d'une table MAC faisant le lien entre numéro de port et adresse MAC du poste connecté au bout.

1) L'apprentissage peut se réaliser :

- Si l'adresse MAC source et destination est connue
- Si l'adresse MAC source est inconnue et celle de destination est connue
- Si l'adresse MAC source est connue et celle de destination est inconnue

2) L'inondation ou « flooding ».

La trame reçue est retransmise sur l'ensemble des ports du commutateur à l'exception du port d'arrivée de la trame.

Deux commutateurs peuvent être mis en cascade, dans ce cas plusieurs @MAC de destination sont mémorisées pour un même port .

L'inter connexion des équipements : Matériel

Les commutateurs administrables (switch) :

3) L'horodatage.

Les adresses MAC, les plus anciennes sont supprimées de la table MAC pour éviter une saturation mémoire.

4) Fonction de filtrage.

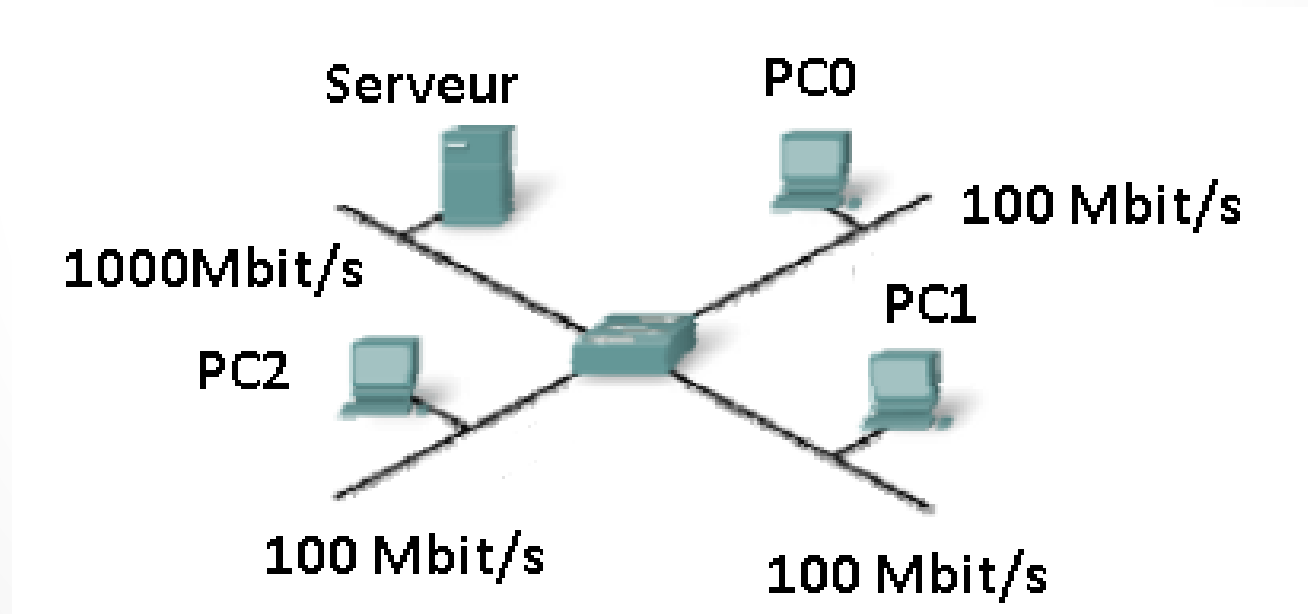
- Abandon d'une trame endommagée.
- Suppression des trames issues ou à destination d'une machine du réseau.

L'inter connexion des équipements : Matériel

Les commutateurs administrables (switch) :

5) Commutation asymétrique.

- fournit des connexions commutées entre des ports de débits différents.

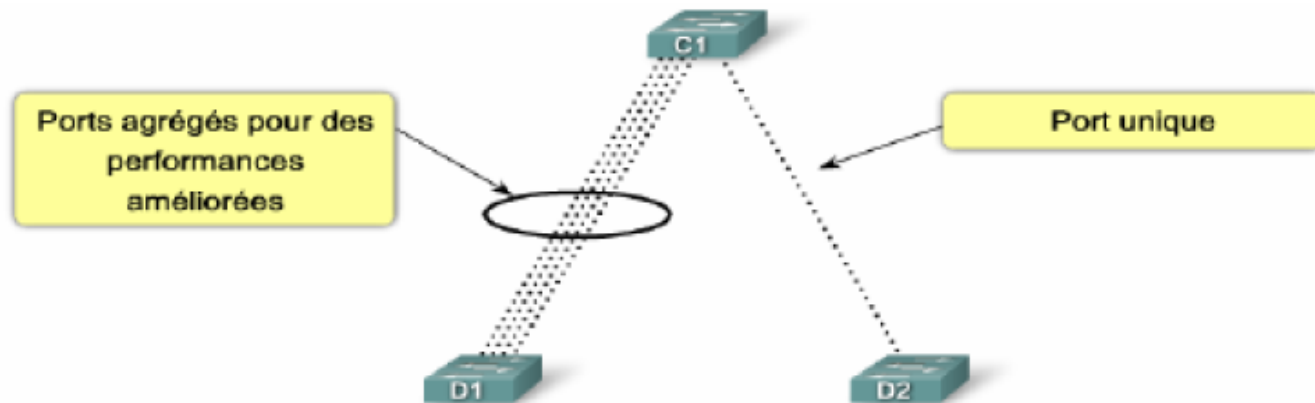


L'inter connexion des équipements : Matériel

Les commutateurs administrables (switch) :

6) Agrégation de lien.

Pour augmenter le débit de transfert, on peut réaliser une association de port du commutateur.



7) Redondance de lien.

L'inter connexion des équipements : Matériel

Les commutateurs administrables (switch) : Configuration du matériel.

Deux possibilités :

- prise de contrôle à distance grâce au LAN (TELNET, SSH ou WEB)
- interface en ligne de commande sur le port console



méthode d'accès local : Via port console

Permet la configuration via logiciel communication.
Putty ou hyper terminal sous windows ou
minicom sous linux.

- Utile lors de la configuration initiale du périphérique
- procédures de reprise après sinistre et dépannage lorsque l'accès distant est impossible.

L'inter connexion des équipements : Matériel

Modes de commande des commutateurs

Mode de commande	Pour accéder au mode	Invite de commutateur affichée	Pour quitter le mode
Mode d'exécution utilisateur	Ouvrir une session	Switch>	Utiliser la commande logout.
Mode d'exécution privilégié.	À partir du mode utilisateur, entrer la commande enable .	Switch#	Pour quitter le mode utilisateur, utiliser la commande disable, exit ou logout.
Mode de configuration globale	En mode privilégié, entrer la commande configure terminal .	Switch(config)#	Pour quitter le mode privilégié, utiliser la commande exit ou end, ou appuyez sur Ctrl-z.
Mode de configuration d'interface	En mode de configuration globale, entrer la commande interface type numéro comme par exemple interface fastethernet 0/1 .	Switch(config-if)#	Pour quitter le mode de configuration globale, utiliser la commande exit .

Exemple de configuration Switch(config)#hostname *nom*

L'inter connexion des équipements : Matériel

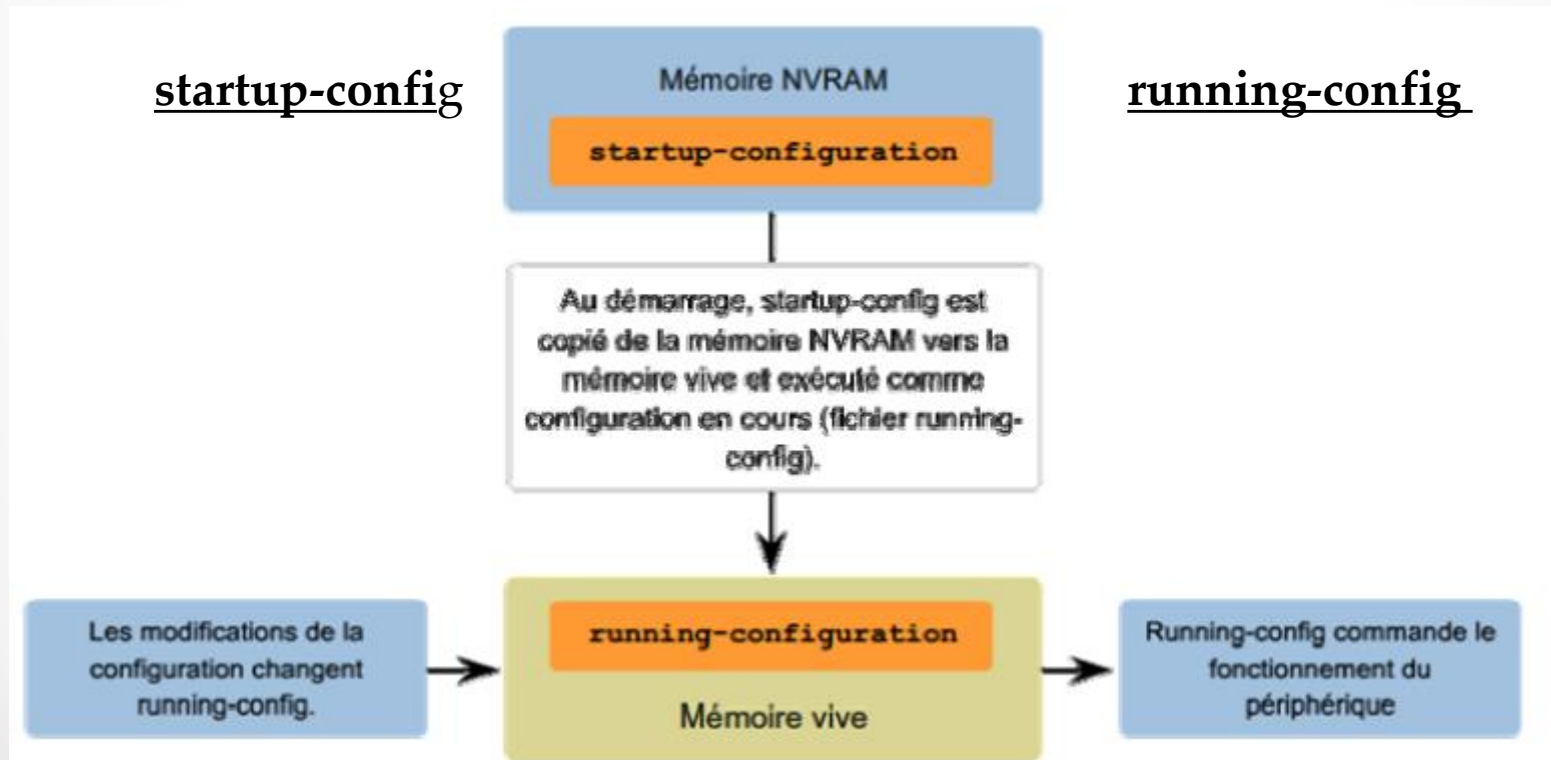
Les commutateurs administrables (switch) : Configuration du matériel.

- Les méthodes d'accès pour la configuration des commutateurs :

Méthode d'accès à distance : SSH ou TELNET

Possibilité de modifier les paramètres du commutateur via les protocoles **Telnet** ou **SSH** en étant connecté sur le réseau Ethernet via adresse IP.

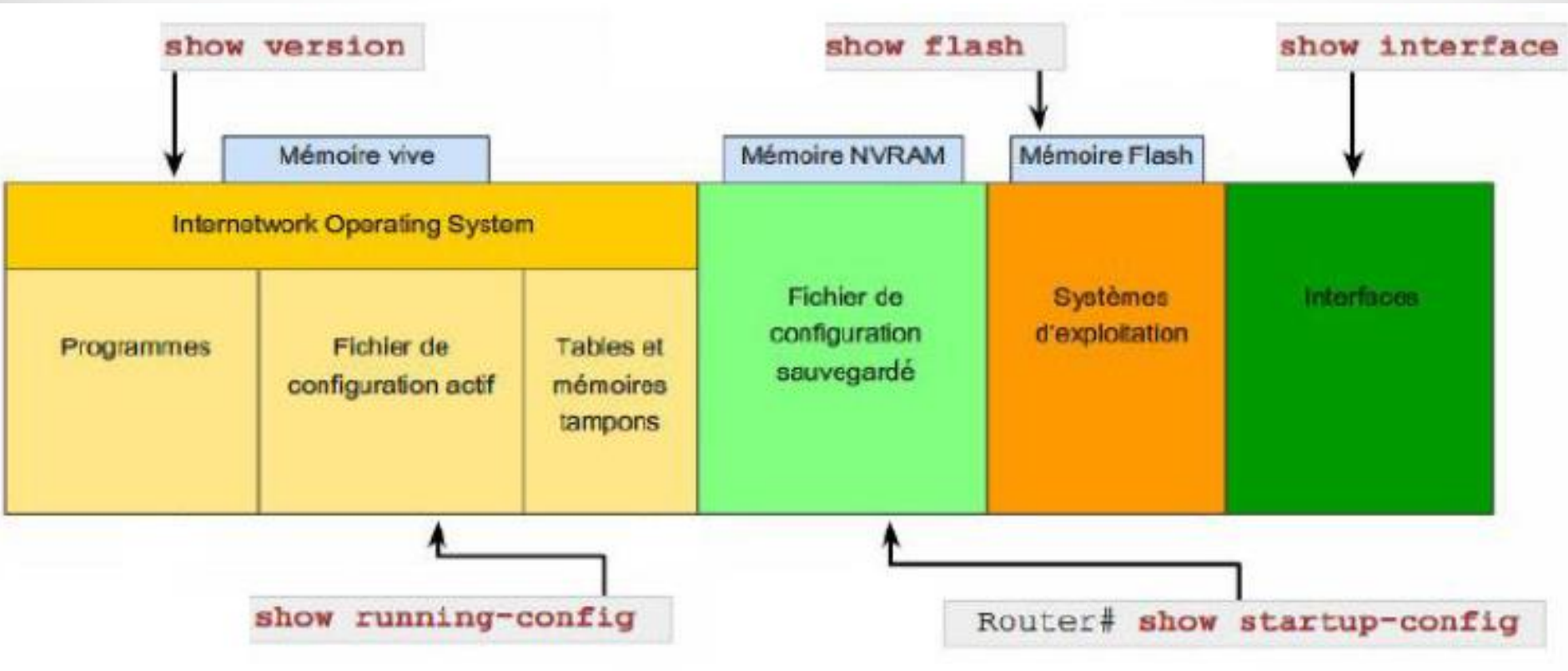
Mise en mémoire de la configuration :



- Sauvegarde configuration copy running-config startup-config

L'inter connexion des équipements : Matériel

La commande show : donne des informations sur le commutateur.



`show mac-address-table` : affiche un tableau représentant les adresses MAC en fonction des ports du commutateur

L'inter connexion des équipements : Matériel

```
Switch(config)#line console 0
```

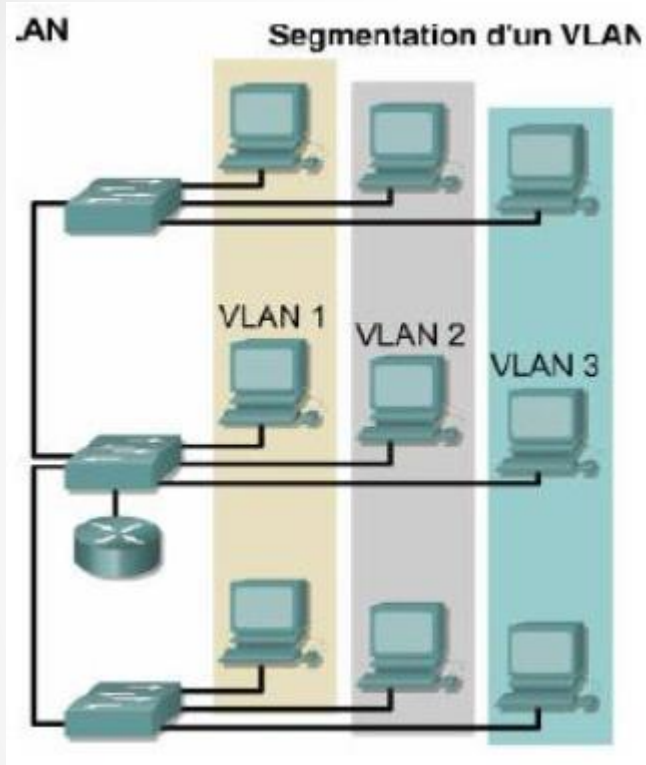
```
Switch(config-line)#password motdepasse
```

```
Switch(config-line)#login
```

```
Switch(config-line)#exit
```

```
Switch(config)#enable secret motdepasse
```

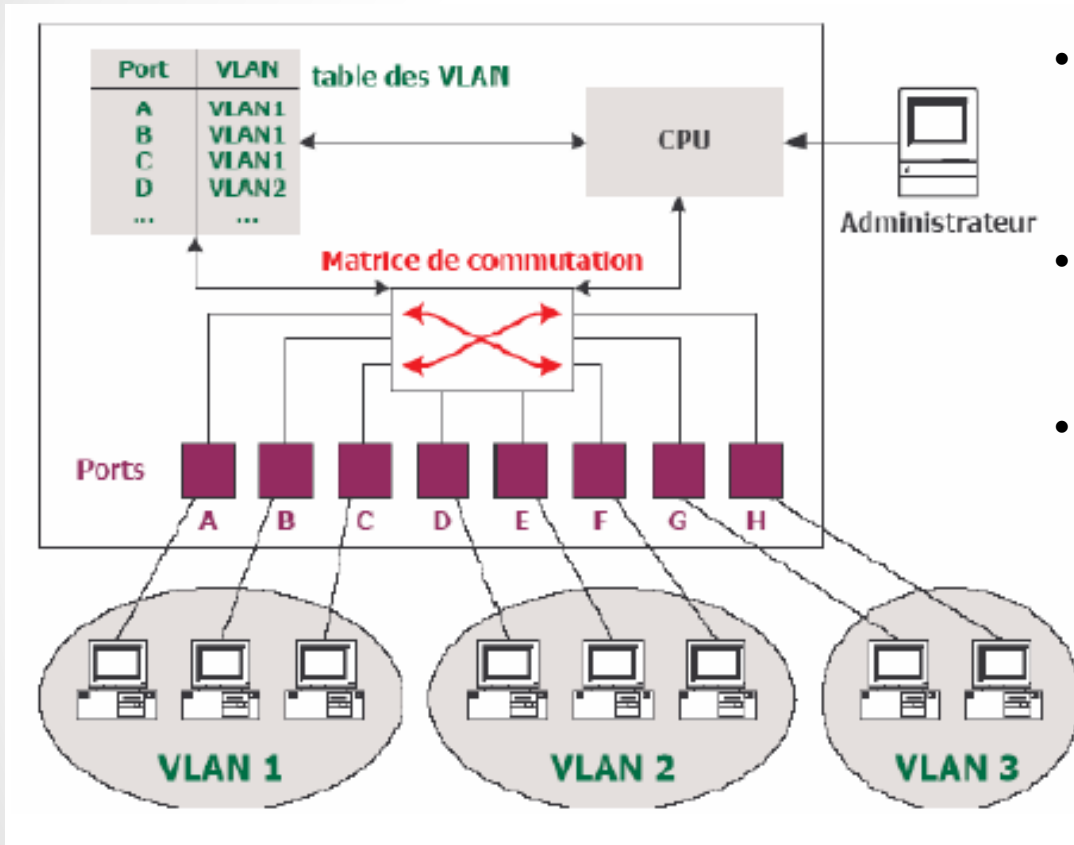
Les VLANs : une segmentation logiciel du réseau.



- Ces réseaux permettent de définir des domaines de diffusions restreints,
- Ils optimisent la bande passante, en réalisant des réseaux disjoints.
- Le principe d'un VLAN, est qu'une trame issue d'une machine appartenant à un VLAN, ne puisse pas être transmise à une autre machine n'appartenant pas au même VLAN.

Les VLANs : une segmentation logiciel du réseau.

VLAN statiques :

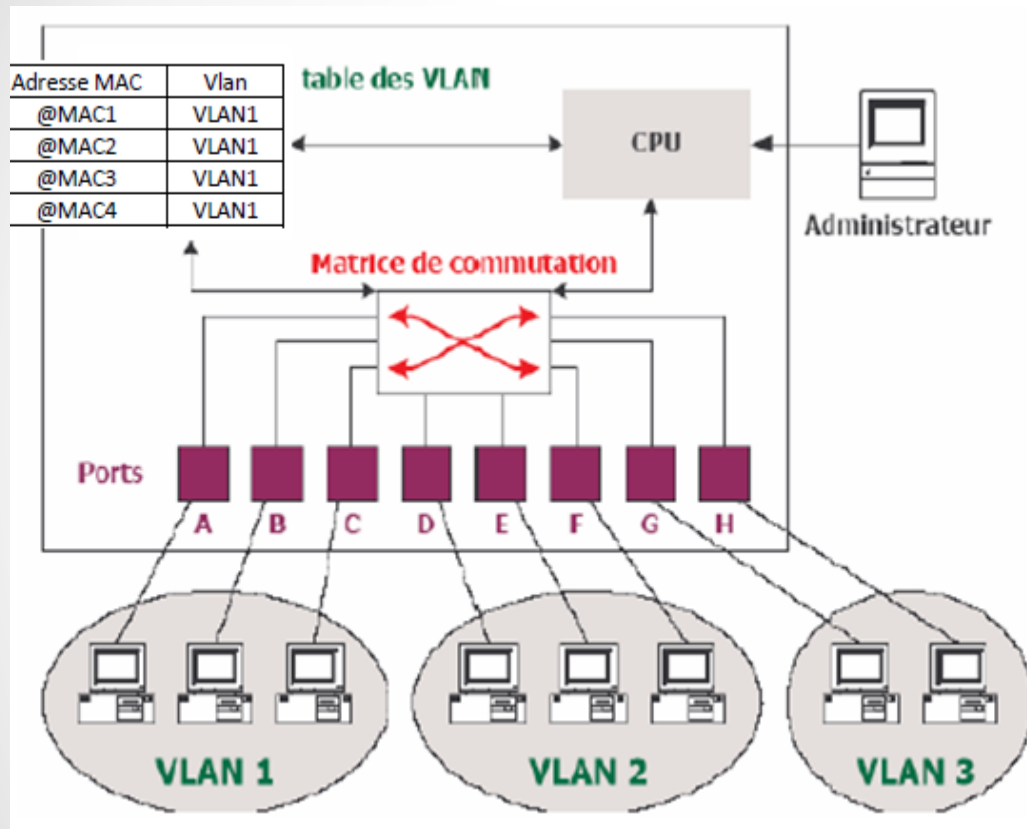


- une table VLAN, décrivant quel port de celui-ci appartient à quel VLAN.
- port configuré en mode **PORT ACCESS**
- En cas de déplacement d'une machine du parc informatique (d'une pièce à l'autre), une reconfiguration du commutateur est nécessaire.

la trame envoyée de la station source, n'est en aucun cas modifiée lors du passage dans le switch avec des ports en mode ACCESS (norme 802.3).

Les VLANs : une segmentation logiciel du réseau.

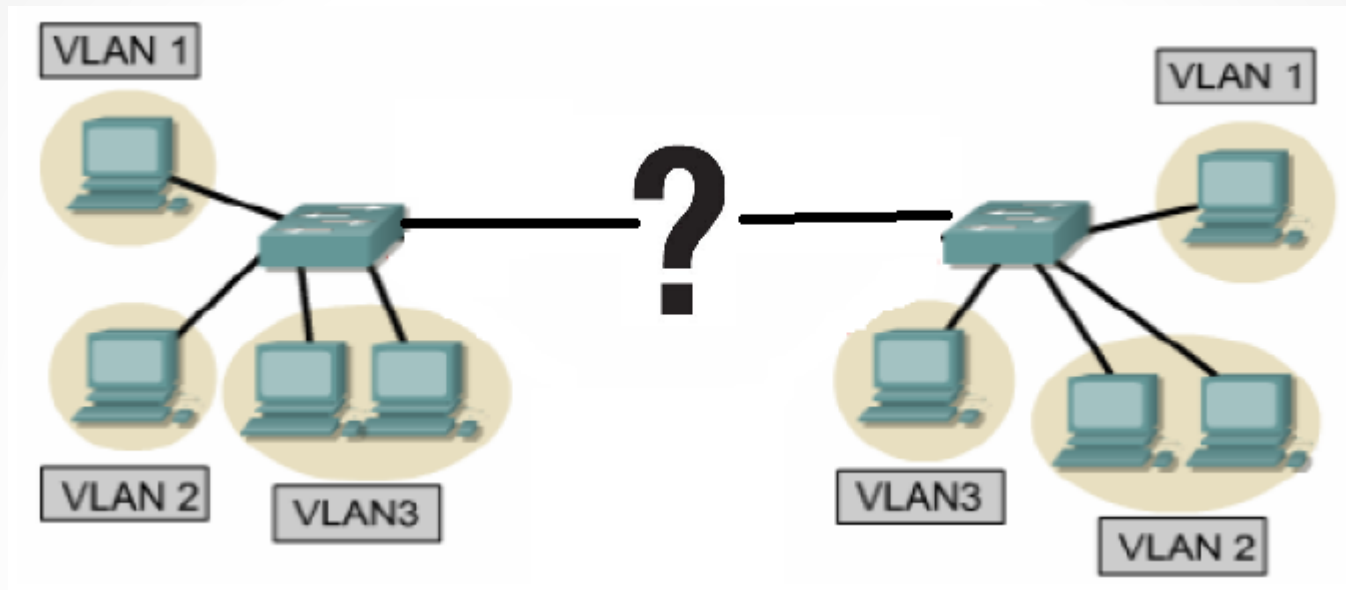
VLAN Dynamique:



- une table VLAN, décrivant quelle adresse MAC appartient à quel VLAN.
- port configuré en mode **PORT ACCESS**
- En cas de déplacement d'une machine du parc informatique (d'une pièce à l'autre), aucune reconfiguration du commutateur est nécessaire.

la trame envoyée de la station source, n'est en aucun cas modifiée lors du passage dans le switch avec des ports en mode ACCESS (norme 802.3).

Les VLANs : VLAN sur plusieurs commutateurs.



- Problème, on affecte des ports à 1 seul VLAN en Mode Access.
- Comment interconnecter deux commutateurs, et garder la notion de VLAN.

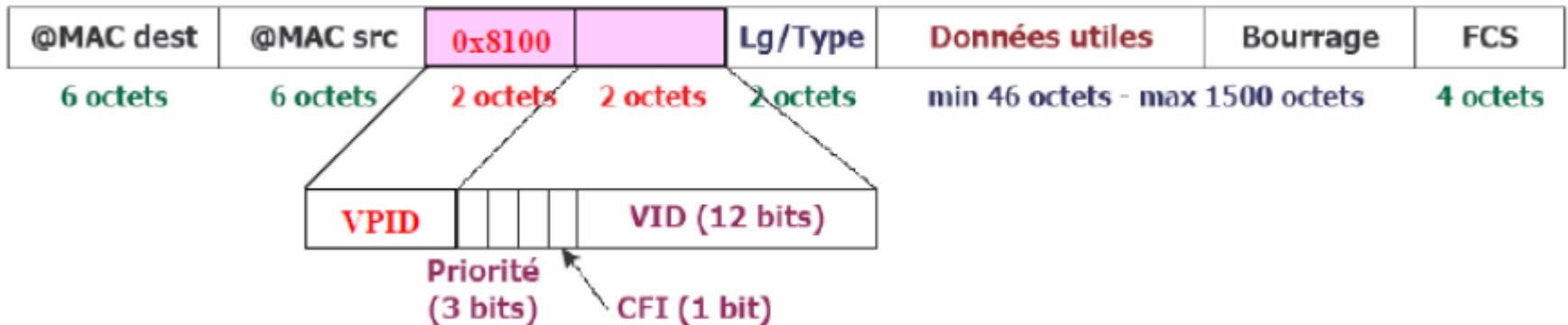
Première méthode : On crée un chemin de transfert pour chaque VLAN.

Seconde méthode : On réalise une agrégation de VLAN.

Les VLANs : L'agrégation de VLAN.

Pour l'agrégation de VLAN, on parle de TAGGED TRAME de la norme 802,1Q

Trame IEEE 802.1Q

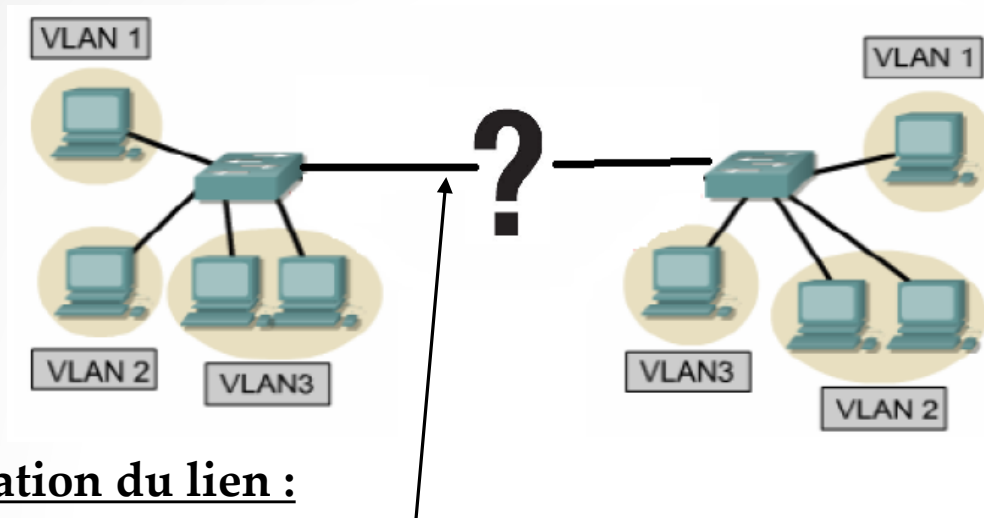


Le champ VPID : on lui donne la valeur 0x8100 ce qui permet de définir l'utilisation d'un protocole VLAN.

Le champ CFI : Canonical Format Identifier, placé à zéro dans les réseaux locaux.

Le champ VID : Identifiant du VLAN

Les VLANs : L'agrégation de VLAN, les VLANs natifs.



Configuration du lien :

Agrégation des VLAN 2 à 3 avec le VLAN natif 1.

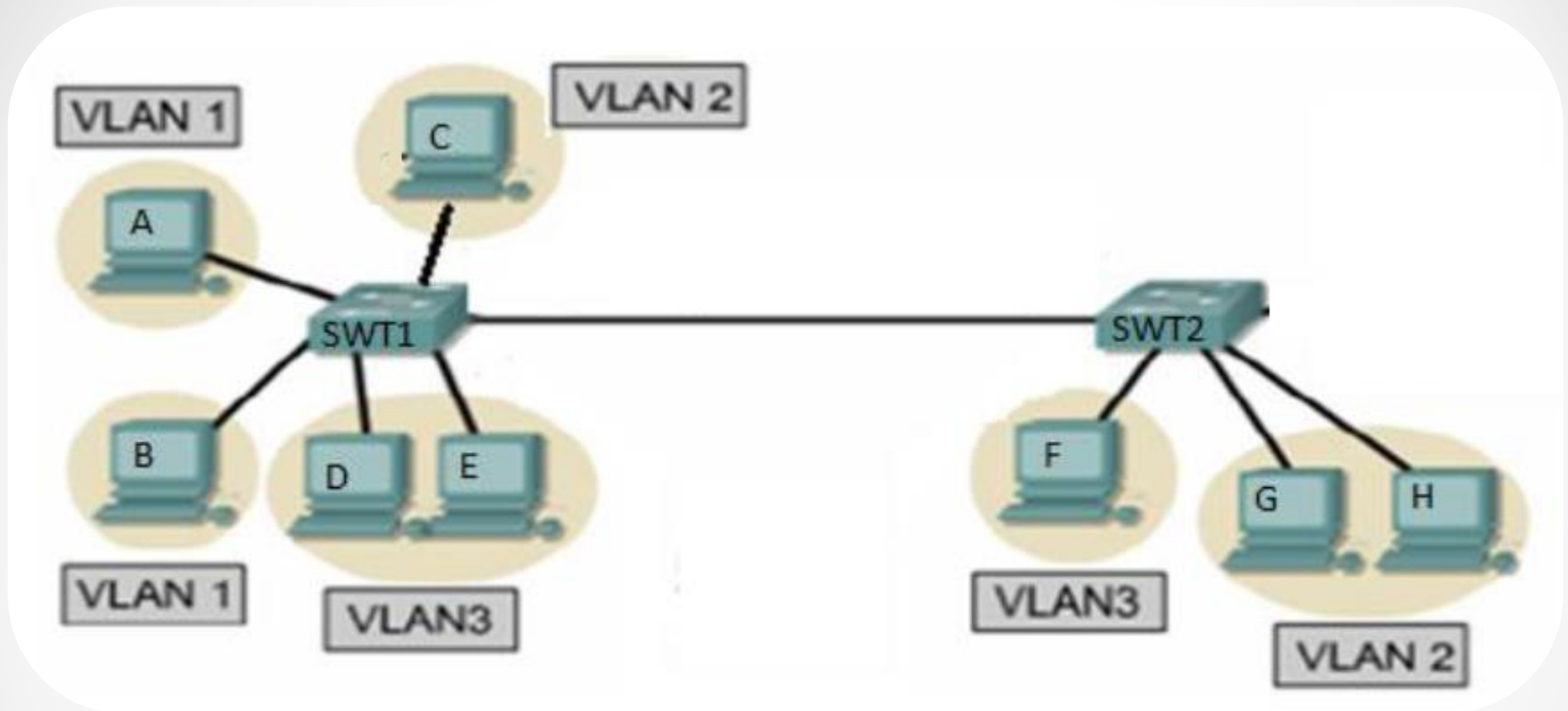
Pour information :

DTP pour **Dynamic Trunking Protocol**, est un protocole **propriétaire** Cisco donc ne fonctionnant qu'entre switchs Cisco!

Le principe est très simple, lorsqu'un port TRUNK monte (up), des annonces DTP sont envoyées.

- Si le port est connecté à un switch voisin, ce dernier va recevoir l'annonce DTP et y répondre. Des deux côtés, l'activation du Trunk s'effectue;
- Si le port est connecté à un pc, ce dernier ne répondra pas à l'annonce car il ne comprend pas le protocole. Sur le port du switch, le Trunk n'est pas activé et donc reste en mode **Access**.

Les VLANs : Synthèse



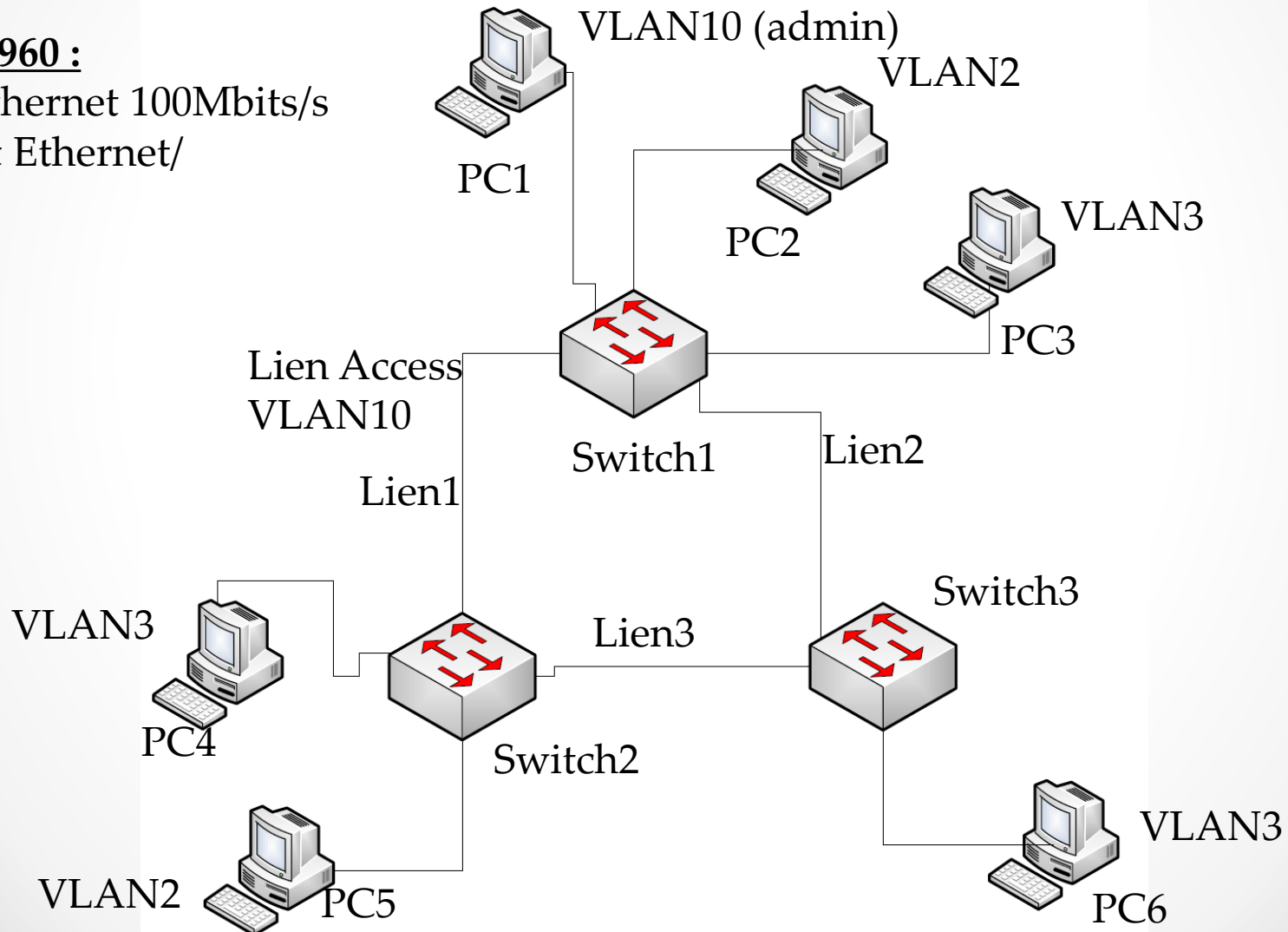
Quelle norme pour le lien entre les deux SWITCH ?

Les VLANs : Réalisation d'une configuration

Proposer une configuration optimum afin que les PC d'un même VLAN puisse communiquer en eux. (numéro port, type, vlan...)

Switch 2960 :

24 FastEthernet 100Mbits/s
2 Gigabit Ethernet/



Les VLANs, création de VLAN

Création d'un VLAN avec affectation en mode Access

1) Création du nom de VLAN.

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	Comml# configure terminal
Créer un VLAN. « id_vlan » est le numéro de VLAN à créer. Passe en mode de configuration de VLAN pour l'ID de VLAN du VLAN.	Comml(config)# vlan id_vlan
(Facultatif) Spécifier un nom de VLAN unique pour identifier le VLAN. Si aucun nom n'est entré, le numéro de VLAN, complété par des zéros, est ajouté au mot « VLAN », comme par exemple VLAN0020.	Comml(config-vlan)# name nom_vlan
Revenir au mode d'exécution privilégié. Vous devez terminer votre session de configuration pour que la configuration soit enregistrée dans le fichier vlan.dat et pour qu'elle soit appliquée.	Comml(config-vlan)# end

Les VLANs, création de VLAN

Création d'un VLAN avec affectation en mode Access

2) Affectation du VLAN au port concerné

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer en mode de configuration globale.	Comml# configure terminal
Entrer dans l'interface pour affecter le réseau local virtuel.	Comml(config)# interface id_interface
Définir le mode d'appartenance du port à un réseau local virtuel.	Comml(config-if)# switchport mode access
Affecter le port à un réseau local virtuel.	Comml(config-if)# switchport access vlan id_vlan
Repasser en mode d'exécution privilégié.	Comml(config-if)# end

NB : L' id_interface peut être obtenu par une commande « show interfaces »
par exemple :

Switch>enable				
Switch#show ip interface brief				
Interface	IP-Address	OK?	Method	Status Protocol
FastEthernet0/1	unassigned	YES	manual	down down
FastEthernet0/2	unassigned	YES	manual	down down
FastEthernet0/3	unassigned	YES	manual	down down

3) Vérification avec un show vlan.

• Configuration pour un commutateur cisco

1. Création des Vlan.

Switch> enable

Passer en mode privilégié

Switch# vlan database

Switch(vlan)# vlan 2 name peda

Crée le VLAN nommé peda avec le numéro (VID) 2.

Switch(vlan)# vlan 3 name admin

Crée le VLAN nommé admin avec le numéro (VID) 3.

Switch(vlan)# exit

2. Affectation des ports (ports 1 à 4 : VLAN 2 - ports 9 à 12 VLAN 2).

Switch# configure terminal

Switch(config)# interface fastEthernet 0/1

paramétrage du port n°1

Switch(config-if)# switchport mode access

pas de tag sur ce port (access)

Switch(config-if)# switchport access vlan 2

affectation du port au vlan 2

Switch(config-if)# exit

Switch(config)# interface fastEthernet 0/9

paramétrage du port n°9

Switch(config-if)# switchport mode access

pas de tag sur ce port (access)

Switch(config-if)# switchport access vlan 3

affectation du port au vlan 3

Switch(config-if)# exit

Remarque : Pour configurer plusieurs interfaces en même temps:

Switch(config)# interface range fastEthernet 0/1 - 4

configure les ports 1 à 4

Ne fonctionne pas avec tous les IOS

3. Création du lien taggé ou trunk (port 24 -> Routeur)

Switch(config)# interface fastEthernet 0/24

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk encapsulation dot1q

Switch(config-if)# exit

paramétrage du port n°24

ce lien sera taggé (trunk)...

...au format 802.1Q (Commande inutile sur Cisco 2950 et +)

4. Quelques commandes utiles.

En mode utilisateur privilégié (enable) :

Switch# show vlan

Voir la configuration des VLAN.

Switch# show conf

Voir la configuration de démarrage.

Switch# show run

Voir la configuration en cours

Switch# show ip int brief

Voir le statut des ports

Switch# show interface trunk

Voir les ports taggués (ne fonctionne pas sur tous les IOS)

Switch# erase flash :vlan.dat

Supprime tous les vlans.

En mode de configuration vlan (vlan database) :

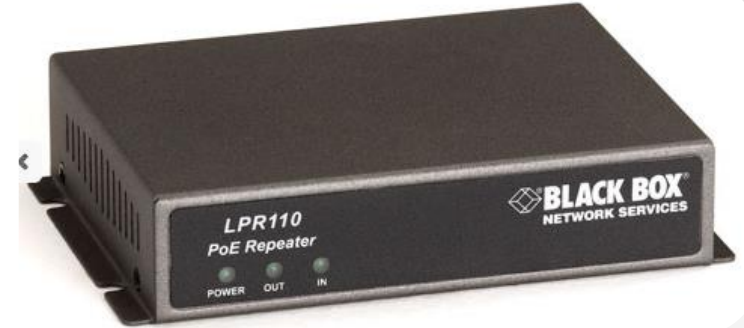
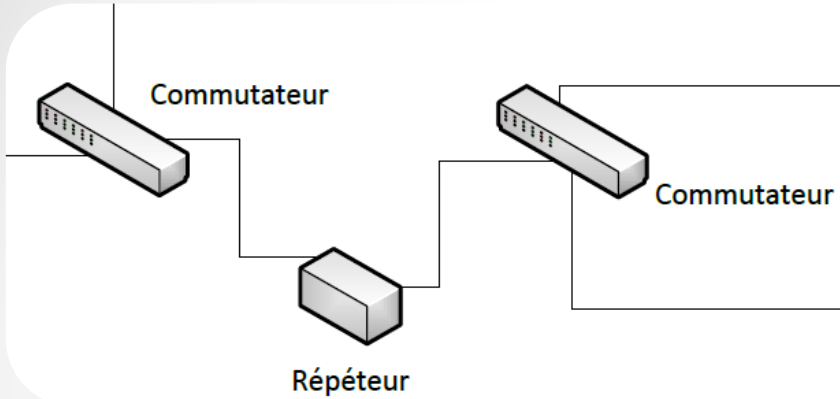
Switch(vlan)#no vlan id

Supprimer le VLAN de numéro id.

Pour quitter un mode : **Ctrl Z**

L'inter connexion des équipements : Matériel

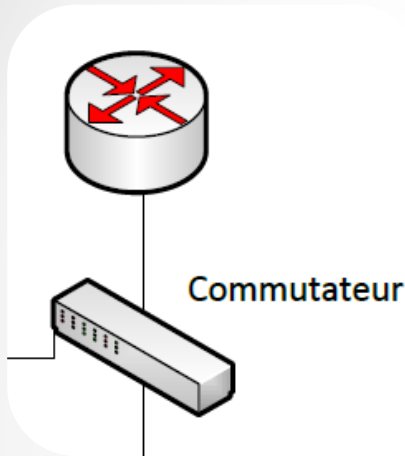
Les répéteurs :



Un **répéteur** est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau.

L'inter connexion des équipements : Matériel

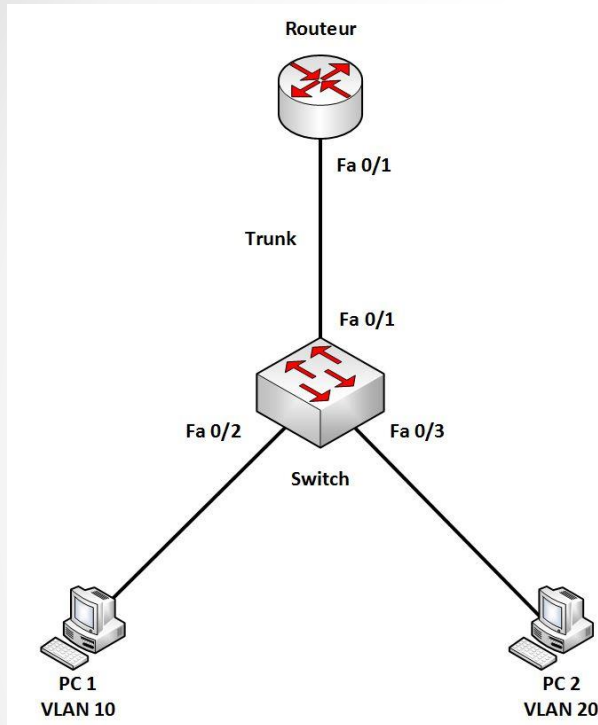
Les routeurs:



- Un **routeur** est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux IP
- Réalise l'interconnexion entre la partie WAN et la partie LAN.
- Permet une communication inter VLAN.

Commutation Inter-VLAN : utilisation d'un routeur.

Prenons l'exemple suivant :



Nous avons deux PC, dans deux VLAN distincts. Pour communiquer d'un VLAN à un autre, il est **obligatoire de passer par un routeur.**

Dans la configuration utilisant un seul lien parfois appelée « Router On A Stick », il faut créer un trunk entre le switch et le routeur.

Tous les messages allant d'un VLAN à un autre, passeront par ce trunk.

On configure sur FA0/1 du routeur **des sous-interfaces** correspondantes à chaque VLAN.

Cela a un avantage et un inconvénient.

Avantage, un seul port est nécessaire sur le switch et le routeur. Même si le routeur permet de connecter 20 VLAN entre eux.

Inconvénient, cela crée un goulot d'étranglement. Tout le trafic inter-VLAN allant d'un port à un autre du switch, devra remonter jusqu'au routeur par ce lien.

```
Switch-1(config)#interface fastEthernet 0/1
Switch-1(config-if)#switchport mode trunk
Switch-1(config-if)#switchport trunk native vlan 99
Switch-1(config-if)#switchport trunk allowed vlan 10,20
```

Concernant le routeur, il faut commencer par activer l'interface voulue :

```
Router(config)#interface fastEthernet 0/1
Router(config-if)#no shutdown
```

Il faudra ensuite créer des sous-interfaces.

Le numéro de la sous interface n'a pas d'importance, mais il est préférable d'en choisir un représentatif du numéro de VLAN.

```
Router(config)#interface fastEthernet 0/1.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.254 255.255.255.0
```

```
Router(config)#interface fastEthernet 0/1.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.254 255.255.255.0
```

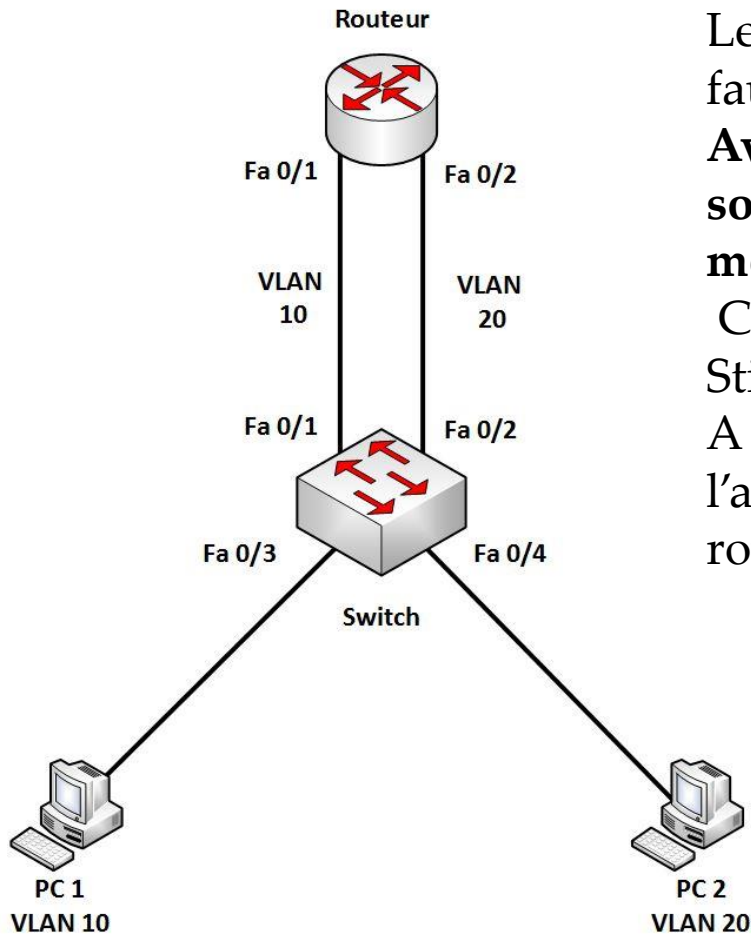
Il n'est pas nécessaire de créer le VLAN natif sauf si l'on souhaite le router:

```
Router(config)#interface fastEthernet 0/1.99
Router(config-subif)#encapsulation dot1Q 99 native
```

Retenons que cette solution est simple à mettre en place, et ne nécessite pas de switch de niveau 3.

Le routage inter-VLAN sera vu plus en détail dans le cours routage M2103

Une deuxième solution existe :



Les performances seront meilleures, mais il faudra un port par VLAN.

Avec plus de deux ou trois VLAN, cette solution se révèle très vite impossible à mettre en place.

C'est pourquoi la solution « Router On A Stick » est préférée.

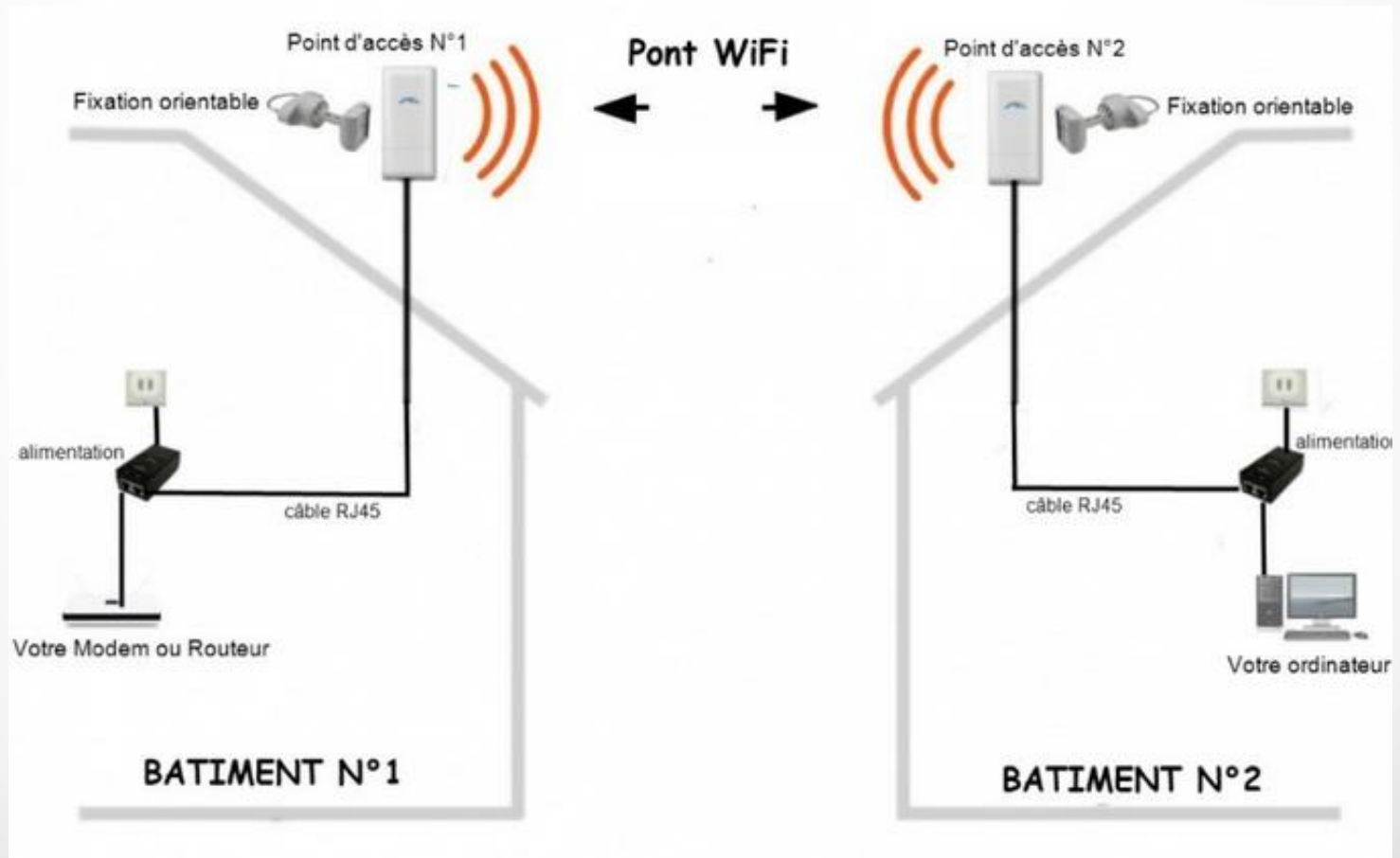
A noter que rien n'empêche de faire de l'agrégation de lien entre le switch et le routeur.

L'interconnexion des équipements : Matériel

Les ponts :

Permet de relier deux bâtiments distants aux réseaux local sans passer par le WAN.

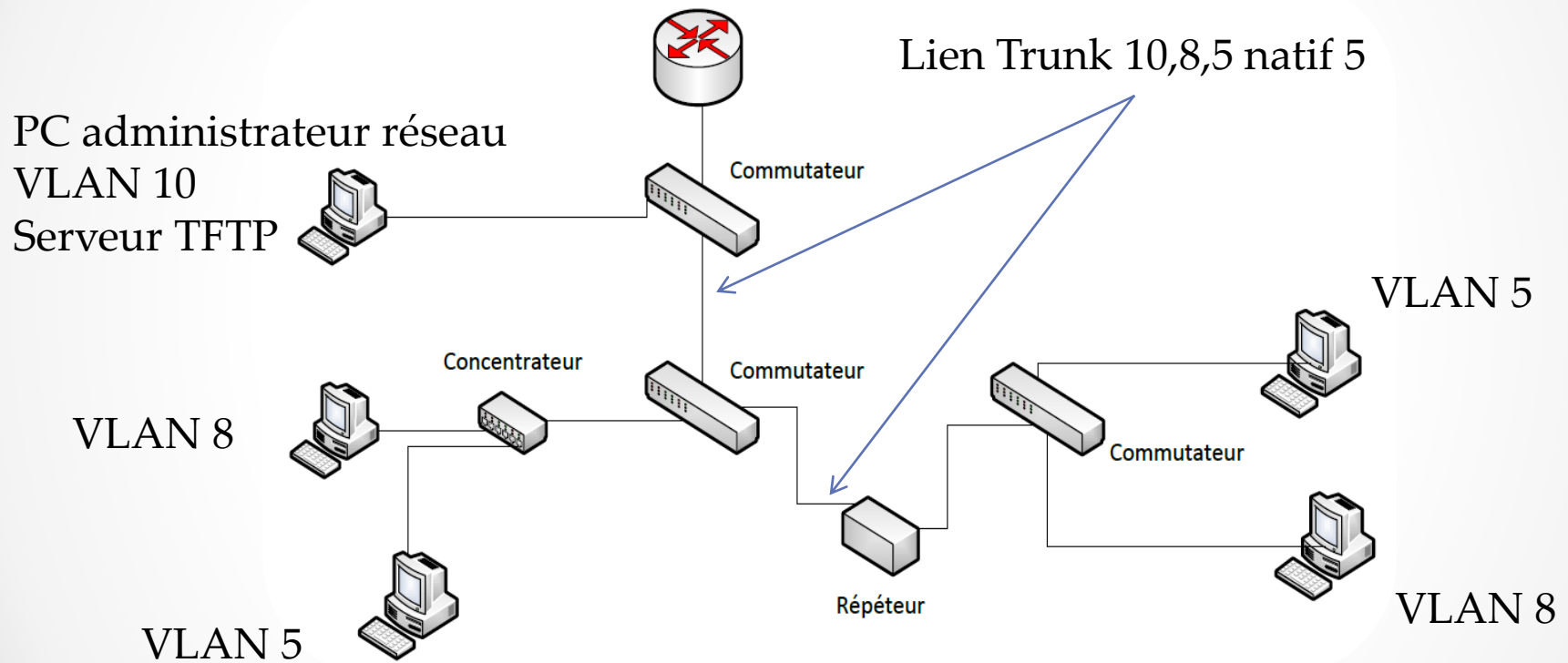
Exemple : Pont wifi.



Fonctionnalités liées aux commutateurs (Switch)

Les commutateurs, TFTP.

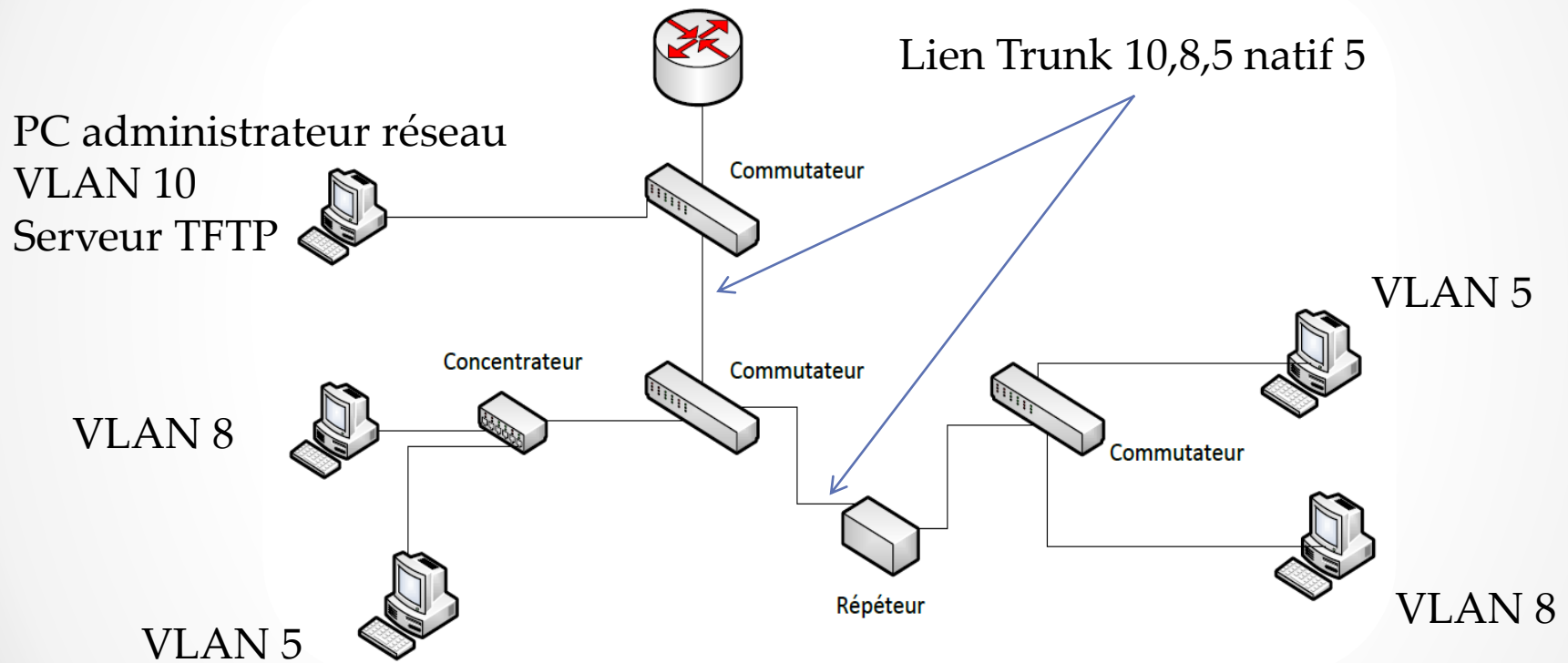
Sauvegarde de la configuration de démarrage sur le serveur TFTP



```
#copy system:running-config tftp://192.168.10.252/config_BX_JJ_MM_AA
```

Les commutateurs, TFTP.

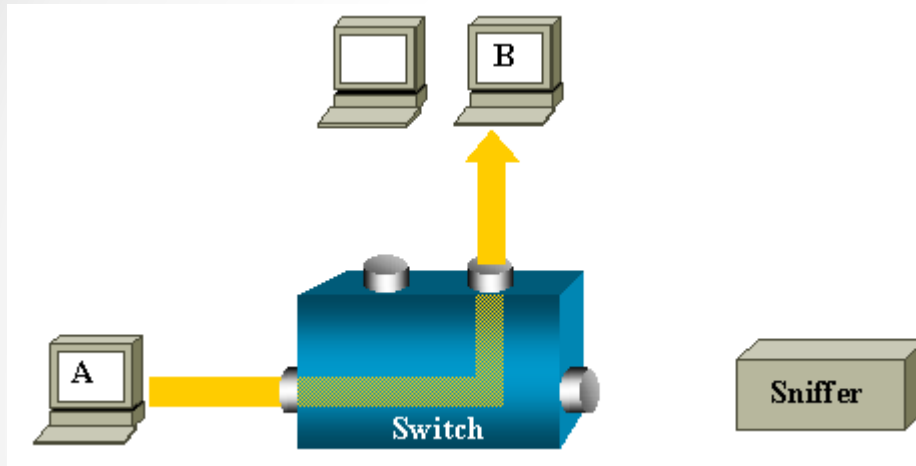
Restauration d'une configuration du commutateur



Condition minimum de configuration?

```
Switch# copy tftp://192.168.20.252/binome_X-config system:running-config |  
startup-config
```

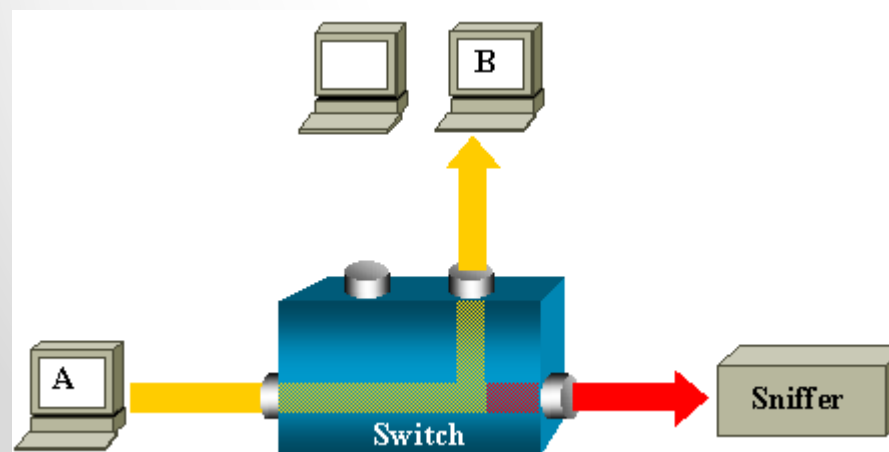
Les commutateurs, Le monitoring



Sans Monitoring :

Le sniffer ne reçoit rien,
l'adresse mac de destination
n'est pas la
sienne

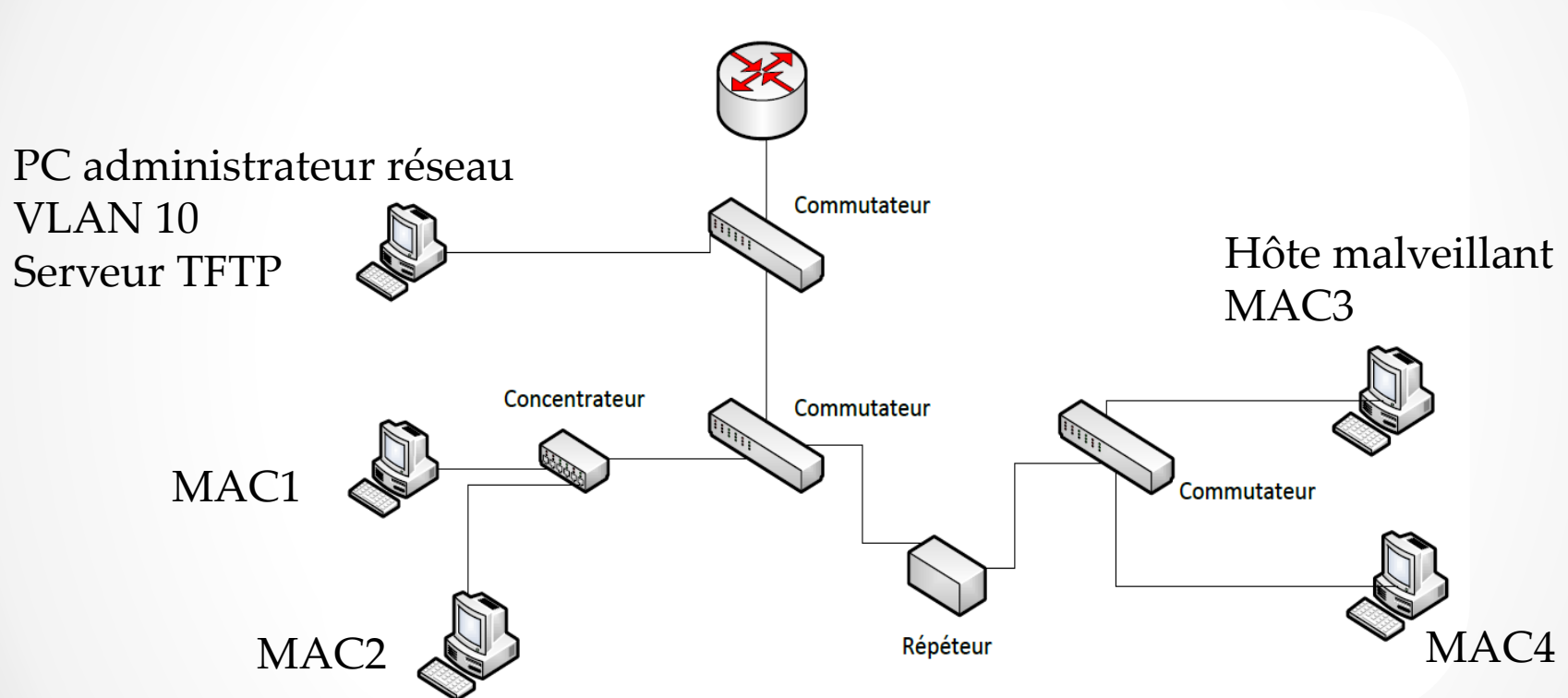
Avec Monitoring :



```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source
interface fastethernet0/11- 12
Switch(config)# monitor session 1
destination interface fastethernet0/13
encapsulation replicate
```

Les commutateurs.

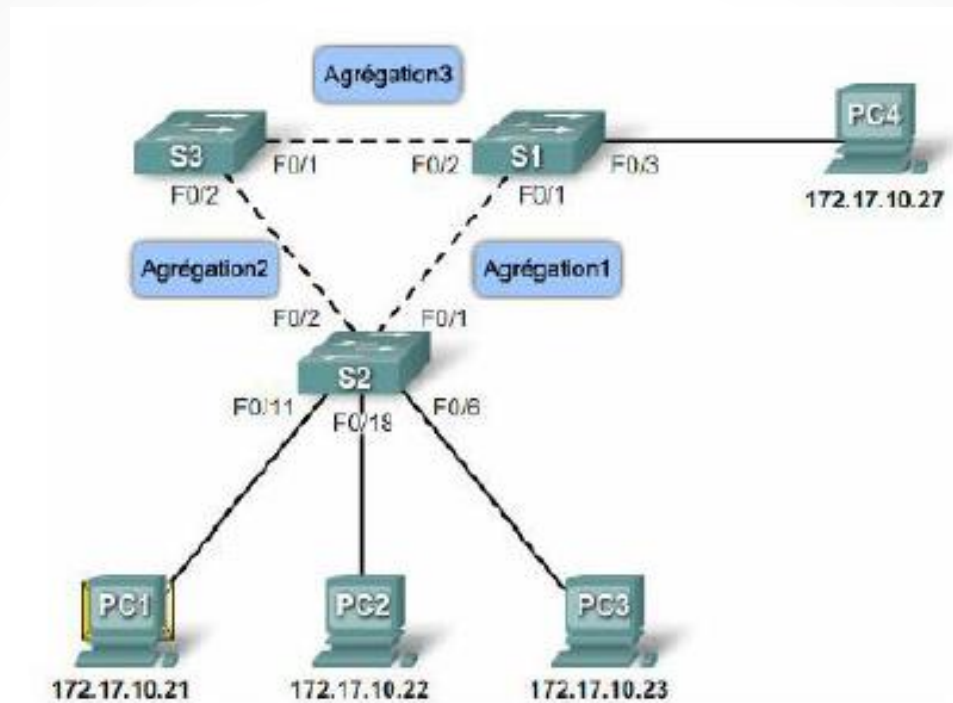
Recherche d'un hôte « malveillant »



Identification adresse MAC hôte malveillant

Recherche de celui-ci à l'aide de la commande `show mac-address-table`

Les commutateurs (switch) et la redondance.



Le PC1 envoie une trame au PC4. Deux chemins sont envisageables

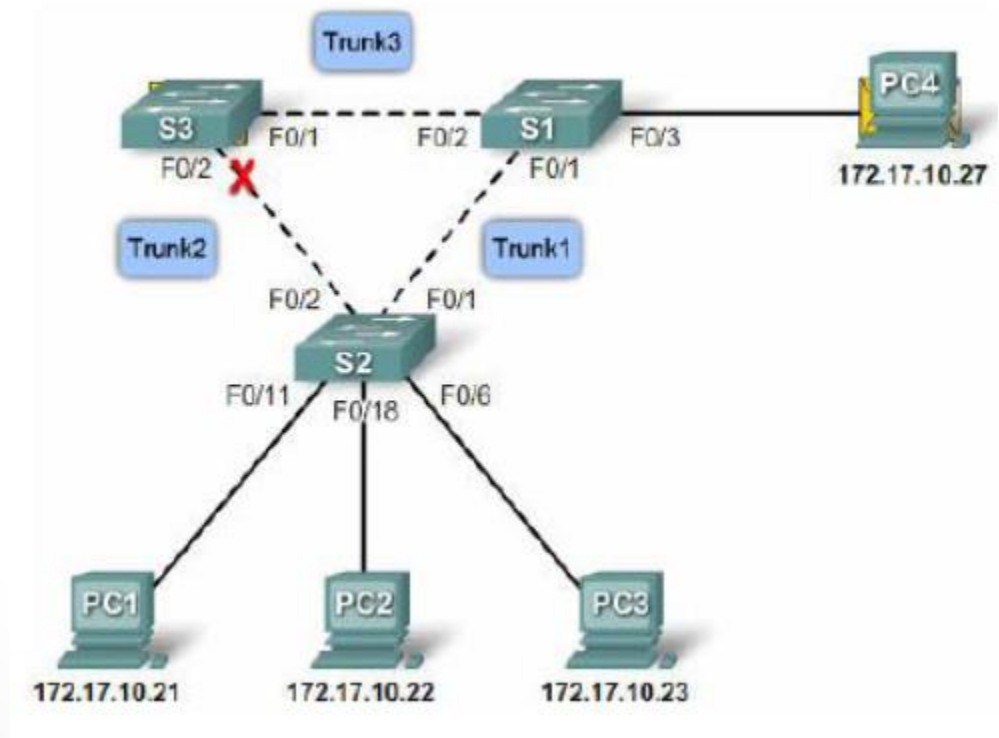
➤ Tempête de broadcast.

- ⇒ Risque de saturation du réseau
- ⇒ Risque de destruction des composants du commutateur (mémoire...)

Le Spanning Tree Protocol : STP.

Ce protocole appartient à la norme 802.1d,

- Permet de déterminer une topologie de réseau sans aucun lien de redondance. Cela même si des liens de câblage imposent des redondances.
- désactiver ou non les ports des commutateurs

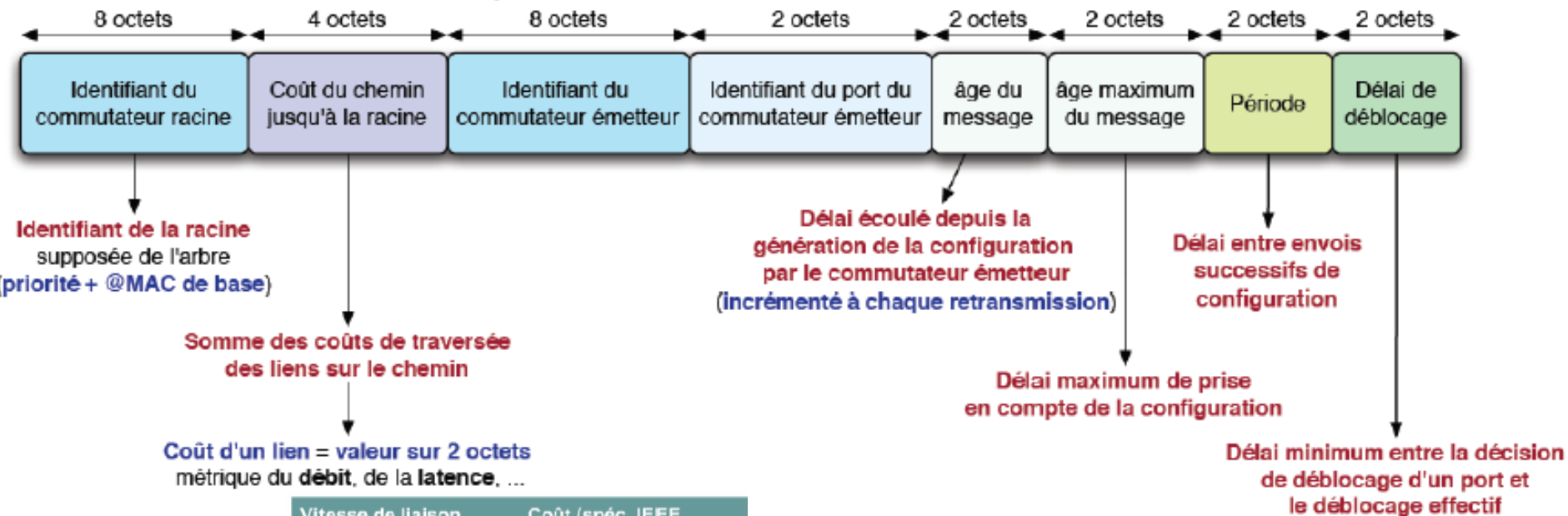


Le Spanning Tree Protocol : STP.

➤ Les trames BDPU.

Les trame BDPU sont des trames envoyées en multicast à l'ensemble des commutateurs du réseau, et uniquement eux.

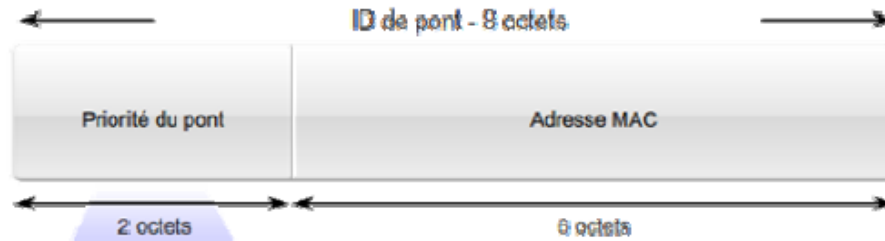
01-80-C2-00-00-00	MAC source	longueur	DSAP 0x42	SSAP 0x42	Cde 0x03	BDPU	FCS
-------------------	------------	----------	-----------	-----------	----------	------	-----



Vitesse de liaison	Coût (spéc. IEEE révisée)
10 Gbits/s	2
1 Gbits/s	4
100 Mbits/s	19
10 Mbits/s	100

Le Spanning Tree Protocol : STP.

➤ Election du ROOT BRIDGE (point central du réseau).



Chaque commutateur compare sa priorité avec celle des autres commutateurs, reçus dans les trames BDPU.

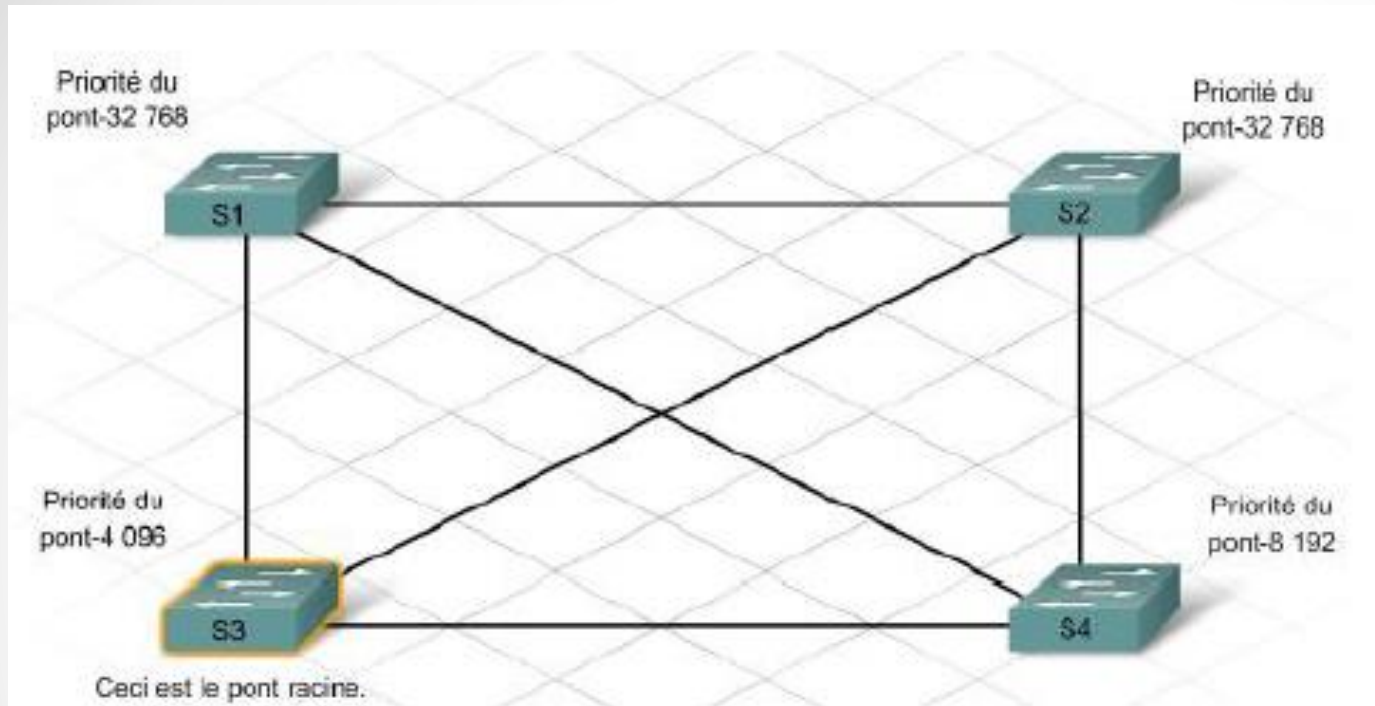
- ⇒ Le commutateur ayant la plus faible priorité, s'attribue le rôle de root bridge.
- ⇒ Si chaque commutateur a la même priorité (32767 par défaut), c'est le commutateur ayant l'adresse MAC, la plus faible qui devient le root bridge.

Le Spanning Tree Protocol : STP.

➤ Election du ROOT BRIDGE (point central du réseau).

Un pont racine est déterminé pour chaque instance Spanning Tree. Il est possible d'avoir plusieurs ponts racine distincts. Par contre si tous les ports de tous les commutateurs sont membres du même VLAN (VLAN 1), il n'y aura qu'une seule instance Spanning Tree

Le Spanning Tree Protocol : STP.



⇒ **Port racine (Root Port) :**

Le port qui fournit le chemin au coût le plus bas vers le « pont racine »

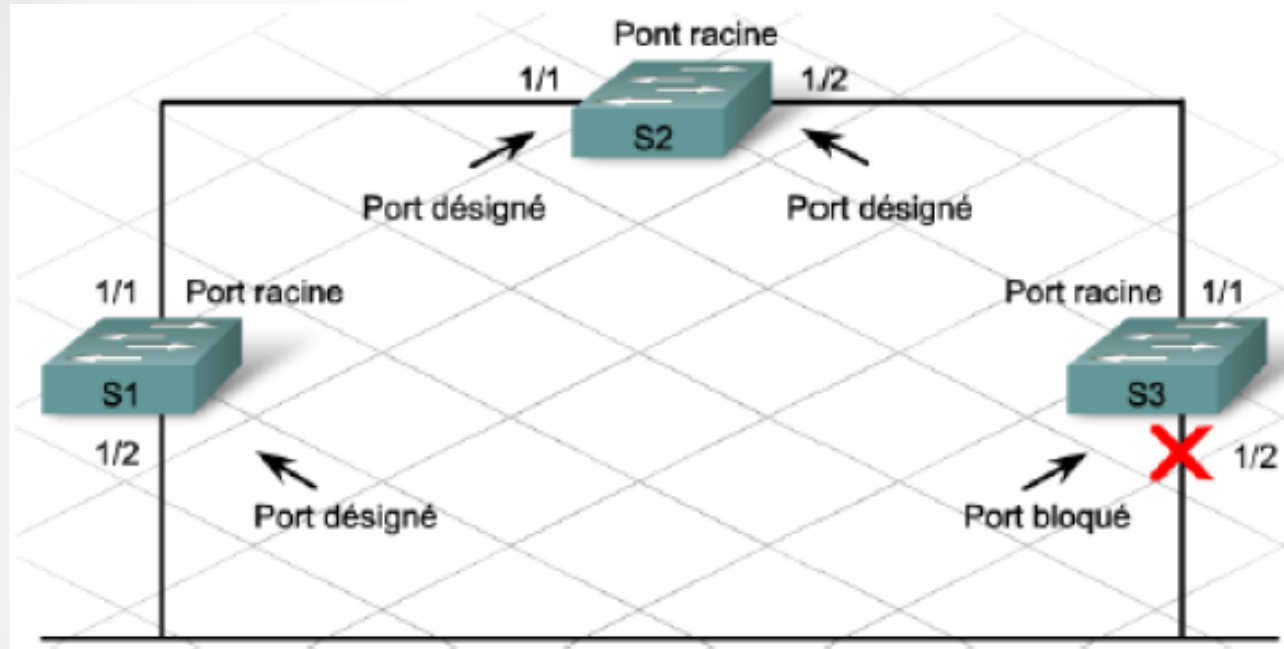
⇒ **Port désigné (Designated Port) :**

Un port désigné est un port qui transfère le trafic au « pont racine ».

Port bloqué :

Un port bloqué ne transfère pas de trafic.

Le Spanning Tree Protocol : STP.



⇒ **Port racine (Root Port) :**

Le port qui fournit le chemin au coût le plus bas vers le « pont racine »

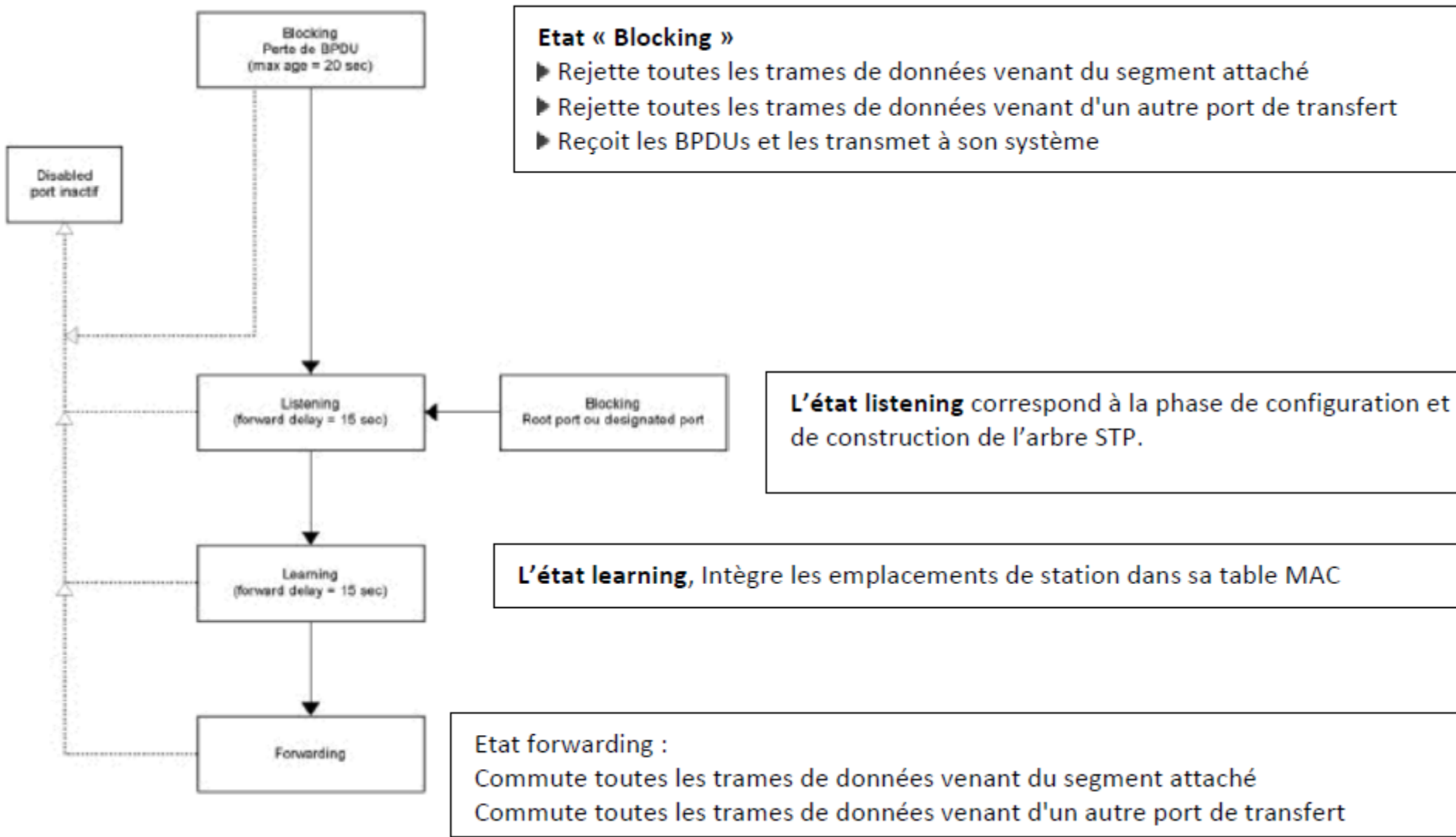
⇒ **Port désigné (Designated Port) :**

Un port désigné est un port qui transfère le trafic au « pont racine ».

Port bloqué :

Un port bloqué ne transfère pas de trafic.

Le Spanning Tree Protocol : STP.



Le Protocol Spanning Tree se remet en route et stoppe donc le trafic pendant une période maximale de 50s.

Le STP fonctionnement et évolution.

Ce temps pouvant être considéré comme long dans certaines structures de réseau (avec l'intégration de la voix et l'image dans les réseaux), il existe alors un autre protocole plus rapide RSTP (15 secondes).

Comment observer la topologie créée par le protocole STP (chez cisco)?

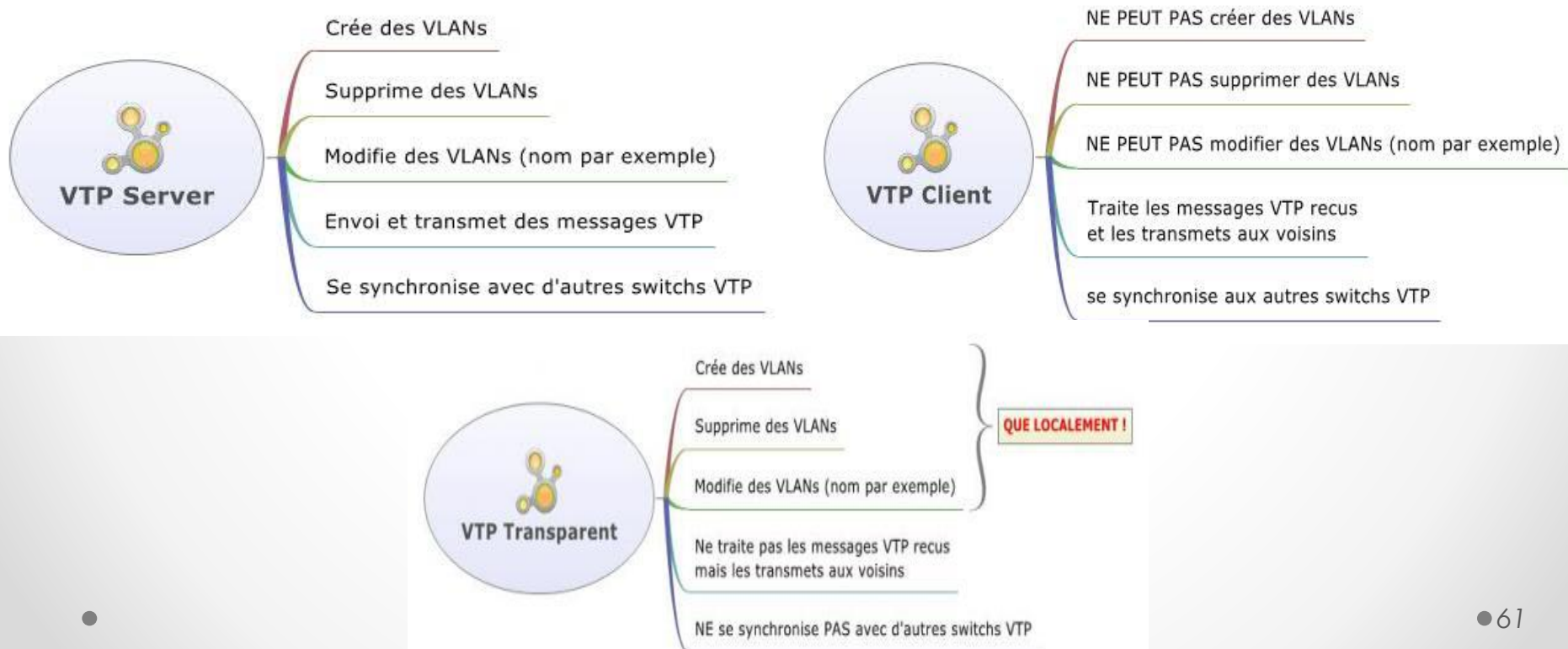
La commande : **Show spanning-tree**

Le STP et les Vlan.

Dans le cas d'un réseau disposant de VLAN, Il va exister une topologie STP liée à chaque VLAN

Le VLAN Trunking Protocol: VTP.

- C'est un protocole propriétaire Cisco de niveau 2. De part sa simplicité et sa puissance, l'IEEE a sorti un protocole similaire afin de permettre cette fonctionnalité entre switches de constructeurs différents: GVRP (GARP VLAN Registration Protocol). La norme est IEEE 802.1ak
- Le switch possède 3 modes VTP: client, transparent ou server (actif par défaut):
 - VTP Server: switch qui crée les annonces VTP
 - VTP Client: switch qui reçoit, se synchronise et propage les annonces VTP
 - VTP Transparent: switch qui ne traite pas les annonces VTP



Le VLAN Trunking Protocol: VTP.

A chaque création/suppression/modification de VLAN, une variable appelée RN – Revision Number – s'incrmente (initialement 0 puis 1 puis 2 puis 3...). A chaque création/suppression/modification de VLAN, le switch Server envoie un message VTP avec la nouvelle valeur du RN.

Les autres switch compare le RN reçu du switch Server avec le RN qu'ils stockent en local, si ce dernier est plus petit alors les switch se synchronisent avec le Server et récupèrent la nouvelle base de données des VLANs.

