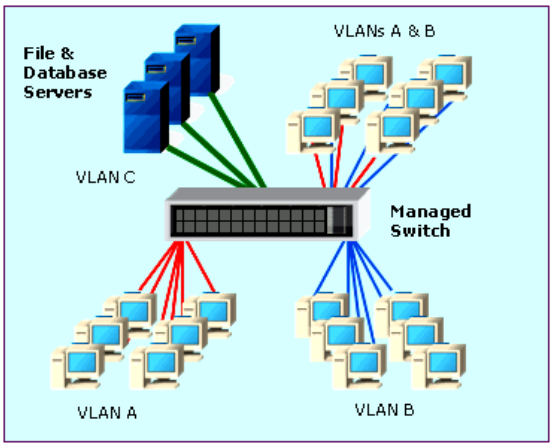
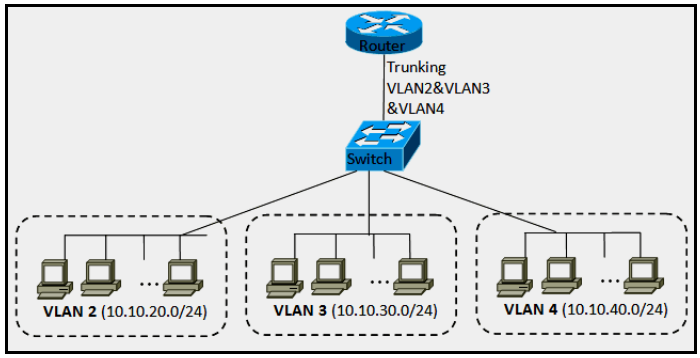
LA SEGMENTATION VIRTUELLE DES DOMAINES DE DIFFUSION : LES VLANs





Objectifs du COURS :

Ce cours traitera essentiellement les points suivants :

- rappels : le subnetting, le VLSM, les domaines de collision et de diffusion
- VLAN de niveau 1
- VLAN de niveau 2
- VLAN de niveau 3
- VLAN par protocole
- la norme IEEE 802.1Q
- exercices d'application

Quelques rappels :

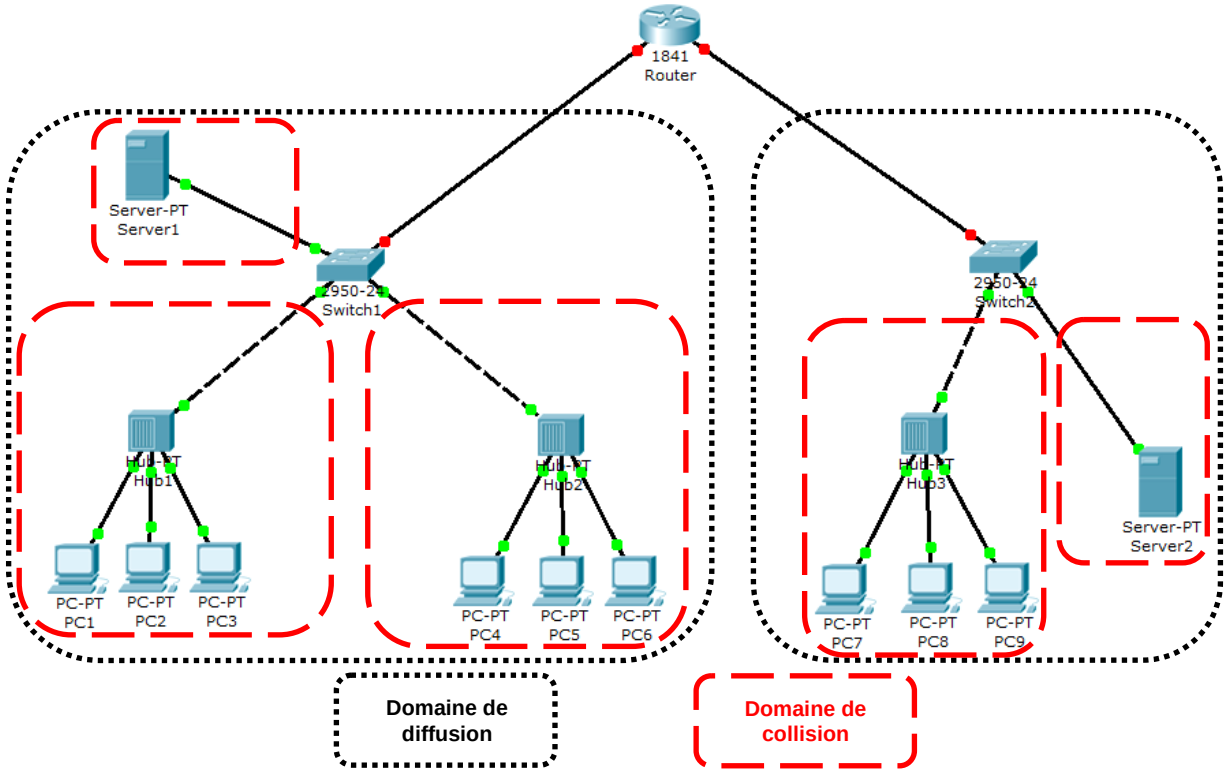
En classe de première, nous avons vu qu'il était intéressant de découper (segmentation logique) une classe d'adresse IP en sous-réseaux (classless) afin de compenser les problèmes de distribution de l'espace d'adressage IP, cloisonner les domaines de diffusion et limiter ainsi la propagation de code malveillant à l'aide de la technique appelée « **subnetting** ».

Puis nous avons vu une autre méthode appelée « **VLSM** » qui en plus de la précédente va permettre d'avoir des sous-réseaux avec des nombres d'hôtes différents grâce aux masques à longueur variable.

Un **domaine de collision** désigne une partie du réseau dans laquelle toutes les trames sont vues par tous les équipements. Il comprend les bus et les « hubs » ou concentrateurs et est limité par les « switchs » ou commutateurs et les routeurs.

Un **domaine de diffusion** désigne la partie du réseau dans laquelle les trames de « broadcast » sont vues par tous les équipements.
Il est constitué des bus, des « hubs » et des « switchs », il est limité par les routeurs.
Les domaines de collisions appartiennent au même domaine de diffusion.

L'utilisation d'un routeur permet de segmenter les domaines de collision et de diffusion. Cependant, ce mode d'interconnexion n'est pas sans inconvénients. Les sous-réseaux sont définis physiquement par les « hubs », si bien que les utilisateurs sont groupés géographiquement : l'organisation logique du sous-réseau est donc définie par sa géographie. Par ailleurs, la mobilité d'une machine d'un sous-réseau à l'autre implique un changement d'adresse si bien que le plan d'adressage est difficile à gérer.



Remarques :

Les hubs (ou concentrateur) sont devenus aujourd'hui obsolètes et ont laissé place au switch (ou commutateur) permettant ainsi de réduire la taille des domaines de collision.
Les machines actives utilisant une liaison partagée (avec hub par exemple) se répartissent le débit binaire.

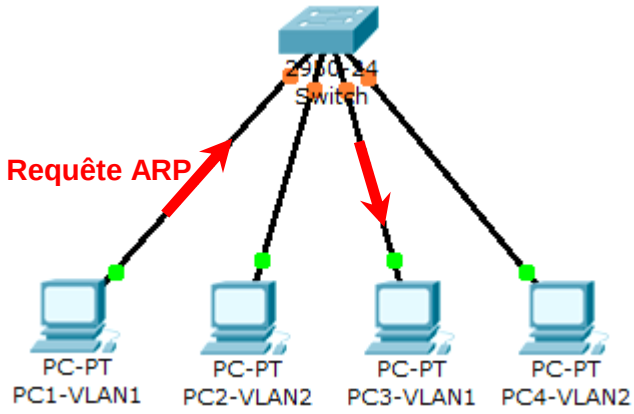
Les **réseaux locaux virtuels** résolvent plusieurs problèmes communs sur les réseaux locaux :

- beaucoup d'utilisateurs sont aujourd'hui mobiles et la situation géographique d'un utilisateur n'a pas forcément de lien avec son appartenance logique : deux collaborateurs situés aux deux extrémités de l'entreprise peuvent souhaiter appartenir au même domaine de diffusion, donc au même LAN qui devient ainsi virtuel car il n'a plus de réalité géographique. Il n'est plus nécessaire de reconfigurer sa machine pour changer de VLAN ;
- les trafics de diffusion sont généralement importants. Les protocoles ARP et DHCP y ont recours et beaucoup de serveurs en génèrent pour décrire leurs services. Or la plupart des trames de

« broadcast » n'intéresse qu'un nombre restreint de machine. Sur les réseaux en mode diffusion (bus ou étoile avec hub), ce type de trafic gaspille le débit binaire, augmente la latence et consomme inutilement de la puissance de calcul ;
- enfin, à l'intérieur d'un domaine de diffusion, le trafic peut être visualisé par toute station dont la carte réseau supporte le « promiscuous mode » ou encore en utilisant un « sniffer » tel que « WireShark » par exemple. Des problèmes de confidentialités peuvent donc exister.

Un VLAN redéfinit les domaines de diffusion de façon à regrouper les utilisateurs de manière logique ou à économiser le débit binaire, améliorer la confidentialité des données et faciliter la gestion de la mobilité. Il est implémenté sur un « switch » et réalise un domaine « logique » de diffusion.

Dans l'exemple ci-dessous, les machines « PC1 à PC4 » sont connectées au même switch sur lequel sont définis deux VLANs : VLAN1 contenant PC1 et PC3, et VLAN2 contenant PC2 et PC4. Lorsque PC1 émet une trame de diffusion, requête ARP par exemple, celle-ci est transmise uniquement vers les machines du VLAN1, donc ici à PC3.
Les machines PC2 et PC4 ignorent le trafic du VLAN1.



Les VLANs peuvent être construits à l'image de l'organisation de l'entreprise.
Dans l'exemple, on peut imaginer que le VLAN1 est attribué au service Production et le VLAN2 au service Administration. Les trafics des deux services de la société sont isolés, même si leurs machines sont reliées à un même switch.

VLAN DE NIVEAU 1

Dans un VLAN de niveau 1, aussi appelé VLAN par port, l'appartenance d'une machine à un VLAN est définie par le port auquel elle est connectée. Le switch est équipé d'une table « port/VLAN » remplie par l'administrateur qui précise le VLAN affecté à chaque port. Dans cette situation toutes les machines reliées à un même port (cas de l'Ethernet partagé) doivent appartenir au même VLAN.
C'est une contrainte qu'il faut gérer lorsque le réseau s'agrandit.

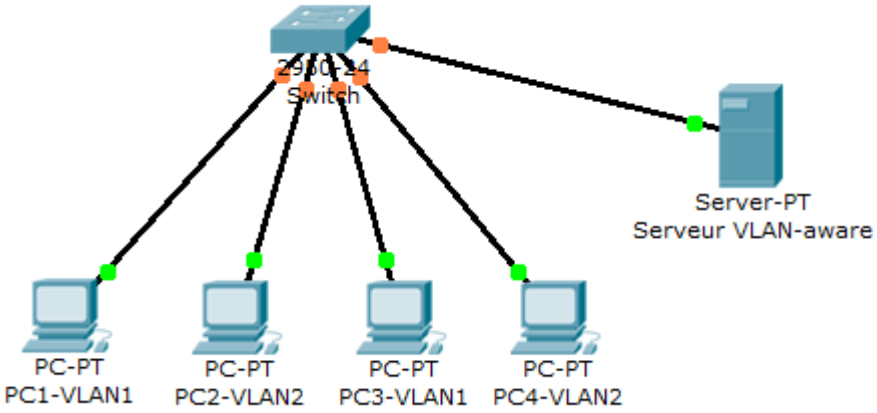


Table	
Port	**VLAN**
1	1
2	2
3	1
4	2
5	1 ; 2

Si l'on souhaite faire appartenir un port à plusieurs VLAN, il est alors nécessaire de procéder à du **marquage** de trames. Les machines doivent être « **VLAN-aware** » et être capable de rajouter dans l'en-tête Ethernet de la trame un marqueur (tag) identifiant le VLAN auquel elle appartient.

Dans l'exemple le serveur appartient aux deux VLANs. Il rajoute à ses trames un marqueur indiquant à quel VLAN elle est destinée. Les autres machines n'ont pas besoin de gérer le tag. Lorsque le switch reçoit une trame marquée du serveur, il trouve les ports de sortie et y réémet la trame à laquelle il a enlevé le marqueur.
Si le serveur souhaite diffuser une même information aux deux VLANs, il doit générer deux trames : l'une portant le marqueur du VLAN1, l'autre portant le marqueur du VLAN2.

Le VLAN de niveau 1 est simple à mettre en place mais présente quelques inconvénients :

- l'extension est difficile ;
- si une machine doit changer de VLAN (déplacement logique), il faut réaffecter manuellement le port ;
- si une machine est physiquement déplacée sur le réseau, il faut désaffecter son ancien port et réaffecter son nouveau port, ce qui nécessite deux manipulations de la part de l'administrateur.

VLAN DE NIVEAU 2

Les VLAN de niveau 2 sont aussi nommés VLAN par adresse MAC. Dans cette méthode, l'adresse MAC d'une machine est affectée à un VLAN. En pratique, c'est encore le port qui est affecté à un VLAN, mais de manière dynamique. En effet, l'administrateur saisit dans la table du switch le couple adresse MAC/VLAN. Lorsque le switch découvre sur quel port est connecté la machine, il affecte dynamiquement le port au VLAN. Il gère donc une deuxième table, la table port/VLAN. Cette structure permet également de définir plusieurs VLAN par port à condition d'utiliser le marquage.

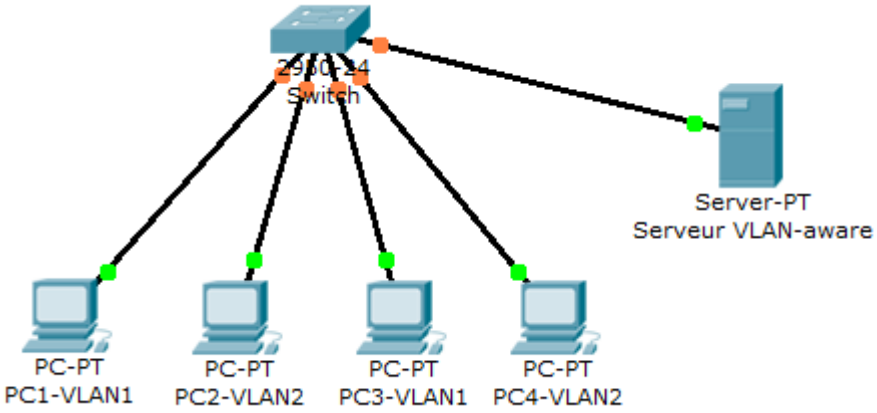


Table créée dynamiquement	
Port	**VLAN**
1	1
2	2
3	1
4	2
5	1 ; 2

Table construite par l'administrateur	
VLAN1	**VLAN2**
@ MAC PC1	@ MAC PC2
@ MAC PC3	@ MAC PC4

Ce procédé présente plusieurs avantages. Lorsqu'une machine change de VLAN, il suffit de modifier l'entrée correspondante de la table d'adresse/VLAN ; la table port/VLAN sera mise à jour dynamiquement. En outre, ce fonctionnement est bien adapté aux équipements mobiles, puisque la reconfiguration du port se fera sans intervention manuelle de l'administrateur en cas de déplacement physique.

Cependant plusieurs inconvénients demeurent :

- le switch doit procéder à une analyse de l'adresse MAC, ce qui rend le VLAN de niveau 2 plus lent que le VLAN par port ;
- l'administrateur doit procéder à la saisie des adresses MAC : la procédure est longue et les erreurs sont probables ;
- enfin, les switchs sur le réseau doivent procéder à l'échange de leurs tables adresse/VLAN, ce qui peut provoquer une surcharge sur le réseau.

VLAN DE NIVEAU 3

Dans les VLAN de niveau 3, aussi nommé VLAN de sous-réseau, l'adresse IP est affectée a un VLAN. Par exemple, le VLAN1 contient les machines d'adresse 10.1.x.x, le VLAN2 celles d'adresses 10.2.x.x. Comme dans le VLAN de niveau 2, l'administrateur remplit une table d'adresse/VLAN. Lorsque le switch identifie le port auquel appartient la machine, il l'affecte a son VLAN. Le VLAN de niveau 3 est plus lent que le VLAN de niveau 2 car le switch doit accéder aux informations de la couche réseau.

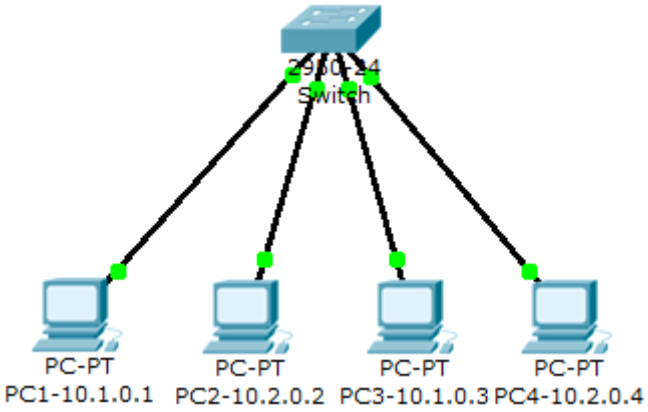


Table créée dynamiquement	
Port	**VLAN**
1	1
2	2
3	1
4	2

Table construite par l'administrateur	
VLAN1	**VLAN2**
@ IP 10.1.x.x	@ IP 10.2.x.x

VLAN PAR PROTOCOLE

Une dernière catégorie de VLAN est constituée des VLANs par protocole dans lesquels l'appartenance au VLAN dépend du protocole utilisé par la machine. Les protocoles considérés sont des protocoles de niveau 3 ou supérieur un VLAN VoIP pour le protocole H.323 par exemple, ou encore par SSID dans le cas du WiFi.
Évidemment, les performances de ces VLANs sont dégradés en raison de l'analyse des niveaux 3 ou supérieurs qu'ils nécessitent.

LA NORME IEEE 802.1Q

La norme IEEE 802.1Q est utilisée pour étendre la portée des VLANs sur plusieurs switchs. Elle est basée sur le marquage explicite des trames : dans l'en-tête de niveau 2 de la trame est ajoutée un « tag » qui identifie le VLAN auquel elle est destinée, on parle alors de VLANs « taggés ». Le format de la trame est donc modifiée, ce qui peut entraîner des problèmes de compatibilité avec les switchs ne supportant pas les VLANs et des soucis de taille maximale de trame sur le réseau. Il faut noter que seuls les switchs ajoutent et enlèvent les « tags » dans les trames. Les machines n'ont donc pas à gérer le marquage qui leur est inconnu.

Trois types de trames sont définis :

- les **trames non étiquetées** (untagged frame) ne contiennent aucune information sur leur appartenance à un VLAN ;
- les **trames étiquetées** (tagged frame) possèdent un marqueur qui précise à quel VLAN elles appartiennent ;
- les **trames étiquetées avec priorité** (priority-tagged frame) sont des trames qui possèdent en plus un niveau de priorité défini selon la norme IEEE 802.1P.

Format de la trame IEEE 802.1Q :

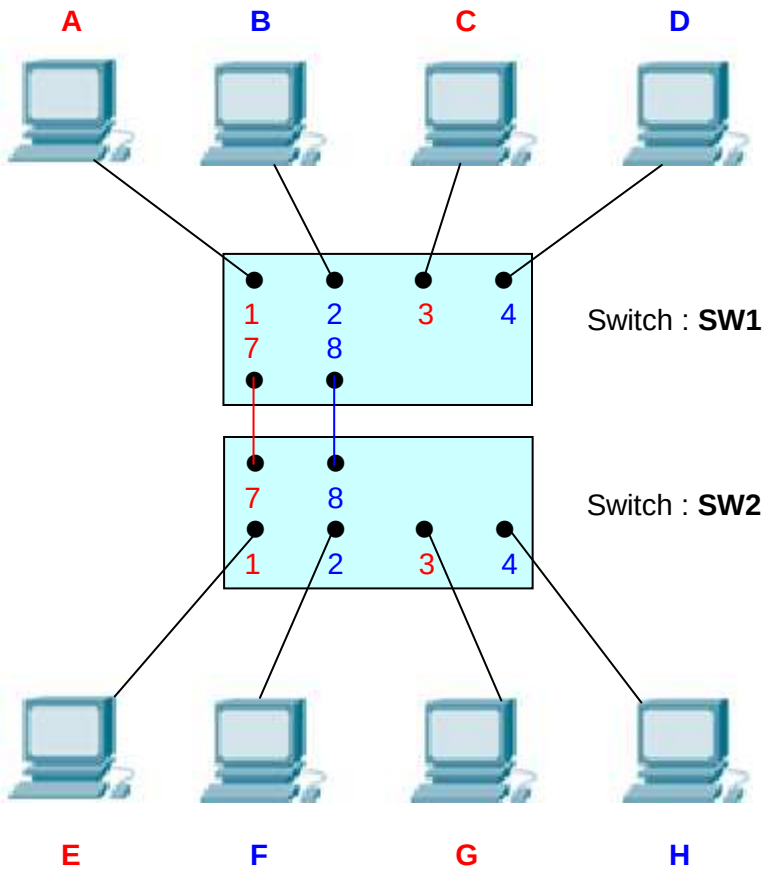
16 bits	3 bits	1 bit	12 bits
Tag Protocol Identifier (TPID)	Priority Code Point (PCP)	Canonical Format Indicator (CFI)	VLAN IDentifier (VID)
	Tag Control Information (TCI)		

- le champ TPID à une valeur fixe, 0x8100 qui identifie une trame de type 802.1Q ;
- le champ TCI est constitué de trois parties :
  - le champ Priority indique le niveau de priorité de la trame et est utilisé lorsque que le champ VID est nul ;
  - le champ CFI indique que le format est standard (Ethernet) ou non ;
  - le champ VID contient l'identifiant du VLAN auquel appartient la trame.

Les VLANs peuvent être déclarés manuellement ou dynamiquement. Dans la déclaration dynamique, l'administrateur définit les VLANs sur un switch et un seul. Le protocole : Mutiple VLAN Registration Protocol (MVRP) permet la diffusion de ces informations aux autres switchs du réseau.

EXERCICES D'APPLICATION

Soit le LAN comportant des VLANs de niveau 1 ci-dessous.



On suppose dans un premier temps que les VLANs sont non taggés. L'administrateur souhaite faire appartenir les machines aux VLANs comme ci-dessous :

- machines A,C, E, G : **VLAN1** (sur le port 7 des switchs)
- machines B, D, F, H : **VLAN2** (sur le port 8 des switchs)

Il complète en conséquence les tables port/VLAN des deux switchs.
On considère que les switchs et les machines viennent d'être mis sous tension. Ainsi les tables MAC/port sont vides.

Question 1 :

Pourquoi a-t-on mis en place deux liens entre les switchs ?

Comme il n'y a pas de marquage, il faut donc un lien pour le trafic issu du VLAN1, et un lien pour le trafic issu du VLAN2.
Les machines d'un même VLAN mais placées sur des switchs différents peuvent ainsi communiquer.

Question 2 :

La machine A émet une trame à destination de la machine C. On rappelle que les tables MAC/port sont vides. Quelles sont les machines qui reçoivent la trame ? Expliquer.

SW1 consulte sa table port/VLAN et apprend que la trame provient du VLAN1. SW1 ne sait pas sur quel port se trouve la machine C car sa table MAC/port est vide. Donc SW1 émet la trame sur les ports de VLAN1, c'est-à-dire les ports 3 et 7.

SW2 consulte sa table port/VLAN et apprend que la trame provient du VLAN1. SW2 ne sait pas sur quel port se trouve la machine C car sa table MAC/port est vide. Donc SW2 émet la trame sur les ports de VLAN1, c'est-à-dire les ports 1 et 3.

Les machines qui reçoivent la trame sont : C, E, G.

Question 3 :

On considère maintenant que les tables MAC/port sont remplies. La machine A émet de nouveau une trame vers la machine C. Quelle(s) machine(s) reçoi(en)t la trame ?

Seule la machine C reçoit la trame.

Question 4 :

La machine A émet une trame en « broadcast ». Quelles sont les machines qui reçoivent la trame ?

Toutes les machines du VLAN1 reçoivent la trame : A, C, E, G.

Question 5 :

La machine A émet une trame pour la machine H. Expliquer comment est traité la trame ?

SW1 consulte sa table port/VLAN et constate que le port 1 appartient au VLAN1. Il consulte sa table MAC/port et constate que la machine H est accessible par le port 7.
SW1 consulte sa table port/VLAN et constate que le port 7 appartient au VLAN2, donc il détruit la trame.

Question 6 :

Quelle modification doit-on réaliser pour permettre le trafic entre deux machines appartenant au même VLAN mais connectées à des switchs différents reliés par un seul lien (7/SW1-8/SW2) ?

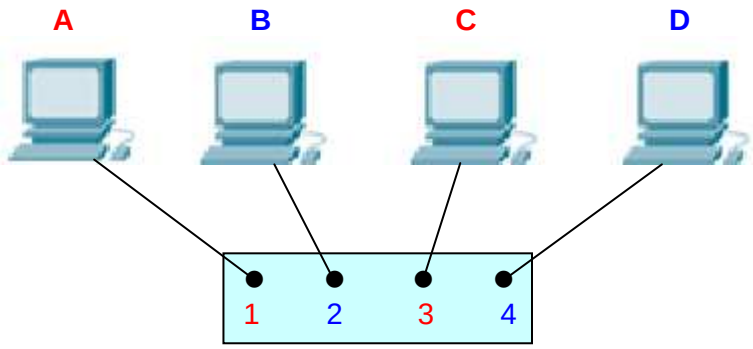
Il faut rajouter du marquage explicite : le port 7/SW1 et le port 8/SW2 doivent suivre la norme 802.1Q.

Exemple pour une trame de A vers E :

SW1 consulte sa table port/VLAN et constate que E est sur le port 7.
SW1 marque la trame et l'émet sur le port 7.
La trame arrive sur le port 8 de SW2.
SW2 lit la marque et apprend que la trame appartient au VLAN1.
SW2 consulte sa table MAC/port et apprend que E est sur le port 1.
SW2 consulte sa table port/VLAN et constate que le port 1 appartient au VLAN1.
SW2 émet la trame sur le port 1.

Soit le LAN ci-dessous sur lequel on souhaite implémenter deux VLANs de niveau 2.

- machines A,C : **VLAN1**
- machines B, D : **VLAN2**



Question 7 :

Quelle table l'administrateur doit-il compléter ?

L'administrateur doit compléter manuellement la table MAC/VLAN.

Question 8 :

Quelle table est construite dynamiquement et à quel moment ?

La table Port/VLAN sera construite dynamiquement par le switch dès qu'il aura pris connaissance des affectations adresses MAC aux ports.