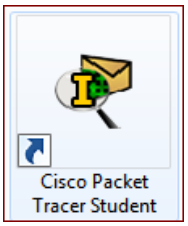
Exolab PACKET-TRACER de mise en pratique des VLAN et de découverte des sous-interfaces et de VTP



Description du thème

Propriétés	Description
Intitulé long	*Activité Packet-Tracer de mise en pratique :* • du transport des VLAN - protocole 802.1q *et de découverte :* • du routage inter-VLAN avec des sous-interfaces de routeur ; • du déploiement des VLAN avec le protocole VTP. Maquette à construire intégralement.
Formation concernée	BTS Services Informatiques aux Organisations
Matière	**SISR2** Conception des infrastructures réseaux
Présentation	Cette activité a pour but de mettre en pratique des connaissances acquises sur le transport des VLAN et sur le routage Inter-vlan, d'introduire l'usage des sous-interfaces et du protocole VTP dédié au déploiement automatique des VLAN.
Notions	**Activités** A3.2.1 Installation et configuration d'éléments d'infrastructure **Savoir-faire** • Configurer une maquette ou un prototype pour valider une solution • Configurer les éléments d'interconnexion permettant de séparer les flux
Transversalité	**SI5** **D3.3 - Administration et supervision d'une infrastructure** · A3.3.1 Administration sur site ou à distance des éléments d'un réseau, de serveurs, de services et d'équipements terminaux
Prolongement	**SISR5 :** • Sécuriser une infrastructure réseau • Contrôler et améliorer les performances du réseau
Pré-requis	Une connaissance de base de l'outil Packet Tracer pour créer la maquette et les notions suivantes : VLAN, trunk 802.1Q.
Outils	Packet Tracer Student 6.2.0
Mots-clés	Packet Tracer, Activité, Maquette, Cisco, Sous-interface, port 802.1Q, trunk, tagged, étiquette, Routage, inter-vlan, VTP
Durée	4 heures
Niveau de difficulté	Facile (7/10) *avec une maîtrise préalable de Packet Tracer et une connaissance des VLAN et du routage.*
Auteur(es)	Eve-Marie Gallot, Denis Gallot, avec la collaboration d'Apollonie Raffalli, Cécile Nivaggioni et Pascal Moussier. Relecture Gaëlle Castel
Version	v 1.0
Date de publication	Avril 2016
Contenu du package	Document présentant les objectifs et les paramétrages demandés. Fichiers .pkt correspondant aux corrigés de l'activité pour chacune des parties. Corrigé complet.

Objectifs

Étudier le transport des VLAN et en particulier visualiser l'étiquette ou tag qui identifie le VLAN dans les trames transportées sur un port étiqueté d'un commutateur.
Sur Windows, il est difficile de visualiser ces informations car beaucoup de cartes réseau ne gèrent pas les VLAN et retirent l'étiquette de VLAN dans les trames. Certaines cartes le font par défaut, la plupart non et quelques unes peuvent le faire en activant le « tagging » des VLAN dans la base de registre. Donc en pratique, une analyse de trame effectuée sur la plupart des postes sur Windows ne permet pas de visualiser le tag de VLAN, contrairement à un poste sur Linux ou sous Mac OS ou au mode simulation de Packet Tracer qui autorise la visualisation des tags de VLAN dans les trames.

Étudier le transport des VLAN et en particulier visualiser l'étiquette ou tag qui identifie le VLAN dans les trames transportées sur un port étiqueté d'un commutateur.

Étudier le routage inter-VLAN en utilisant des sous-interfaces d'un routeur.

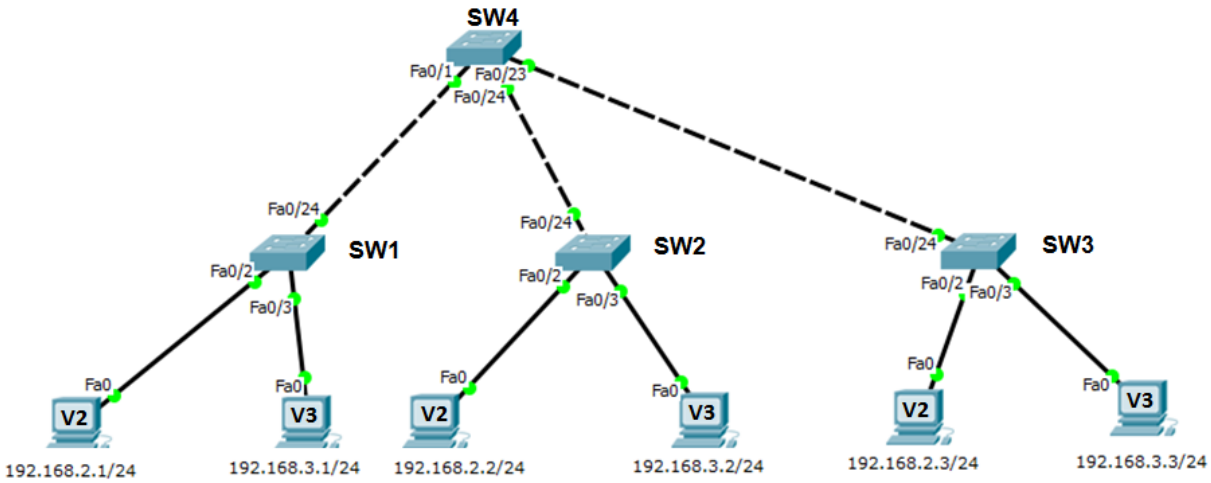
1ère partie - transport des VLAN et Routage inter-VLAN

Phase 1 – Transport des VLAN

L'architecture de départ à modéliser comporte 2 réseaux IP associés chacun à un VLAN selon le plan d'adressage suivant :

Réseau	N° de VLAN	Nom de VLAN	Adresse réseau	Adresse de passerelle
Production	2	production	192.168.2.0/24	192.168.2.254
Ventes	3	ventes	192.168.3.0/24	192.168.3.254

Le schéma physique est le suivant :



Sur chaque PC, il est indiqué son VLAN d'appartenance : V2 pour le VLAN 2 et V3 pour le VLAN 3.

Travail à faire

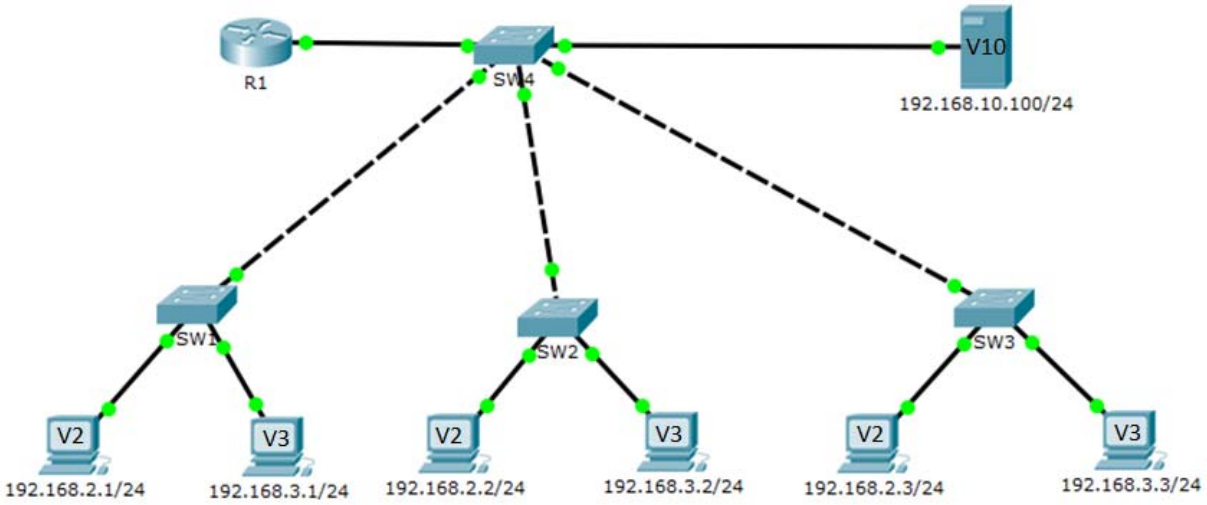
- Modéliser la maquette de départ sur Packet Tracer, configurer chaque poste, puis paramétrer les VLAN sur chaque commutateur.
- Visualiser, en mode simulation, les étiquettes de VLAN dans les trames, (en testant par exemple la connectivité entre postes d'un même VLAN).

Phase 2 – Routage inter-VLAN

Les services Production et Ventes doivent pouvoir partager des ressources hébergées sur un serveur. Ce dernier a pour adresse IP 192.168.10.100/24 et est associé à un nouveau VLAN dont les caractéristiques sont les suivantes :

Réseau	N° de VLAN	Nom de VLAN	Adresse réseau	Adresse de passerelle
Serveurs	10	serveurs	192.168.10.0/24	192.168.10.254

Afin de permettre la communication entre les services Production et Ventes avec le serveur « ressources », il est nécessaire de mettre en place du routage inter-VLAN.
Nous utiliserons dans cet Exolab la méthode « router-on-a-stick » détaillée en **annexe1**.
Pour cela, un routeur 1841 « R1 » est ajouté et interconnecté avec le commutateur « SW4 » (qui représente le cœur du réseau) comme le montre le nouveau schéma d'infrastructure :



Travail à faire

- Faire évoluer l'infrastructure sous Packet Tracer en intégrant et configurant le serveur et le routeur.
- Tester la communication entre les STA du service Production et le serveur « ressources ».
- Tester la communication entre les STA du service Ventes et le serveur « ressources ».

Note : après la mise en place du routage inter-VLAN, tous les VLAN pourront communiquer entre eux. Afin de gérer les différentes contraintes de communication entre les services, il sera nécessaire de mettre en place des listes de contrôle d'accès, ou ACL, (voir la rubrique « Exolab » sur le site du réseau Certa).

2ème Partie - Déploiement des VLAN avec le protocole VTP

Nous allons tester le déploiement automatique des VLAN dans une architecture de commutateur avec le protocole VTP. Ce protocole CISCO est basé sur la norme 802.1q et exploite une architecture client-serveur avec la possibilité d'instancier plusieurs serveurs.
L'annexe 2 propose plus d'informations sur ce protocole ainsi que les principales commandes associées.

Suite à des regroupements de services sur le même site, de nouveaux VLAN apparaissent. On décide de mettre en place le protocole VTP pour simplifier la mise en place des VLAN dans tous les commutateurs et prévoir une gestion plus rapide en cas d'évolution du nombre de ces VLAN.

Travail à faire

1. Sur le schéma issu de l'étape précédente :
   - Régler les commutateurs SW1, SW2 et SW3 en client VTP.
   - Régler le commutateur SW4 en serveur VTP pour le domaine « domVTP » avec le mot de passe « mdpvtp ».
   - Vérifier la configuration VTP de chaque commutateur puis comparer leur table de VLAN.

Le service « Ventes » devient le service « Commercial ».

2. Tester la modification du nom du VLAN « ventes » sur le serveur VTP et la propagation de cette modification sur les commutateurs clients.

Un nouveau VLAN doit être créé pour le service comptabilité, ses caractéristiques sont les suivantes :

Réseau	N° de VLAN	Nom de VLAN	Adresse réseau	Adresse de passerelle
Comptabilite	4	compta	192.168.4.0/24	192.168.4.254

Il sera composé de deux postes de travail :
- PC1 (192.168.4.1/24) connecté sur l'interface fa0/4 du commutateur SW2 ;
- PC2 (192.168.4.2/24) connecté sur l'interface fa0/4 du commutateur SW3.

3. Effectuer les tests suivants :
   - Tester l'ajout de ce nouveau VLAN sur un client.
   - Tester l'ajout de ce nouveau VLAN sur le serveur :
     - Vérifier la propagation du VLAN dans l'architecture de commutateurs ;
     - Tester le routage inter-VLAN avec ce nouveau VLAN

4. On souhaite ajouter une nouvelle branche réseau qui doit permettre d'une part, de relier de nouveaux postes clients dans les VLAN existants et d'autre part, d'interconnecter certains postes dans un VLAN isolé.
   - Ajouter un commutateur SWT relié au port fa0/22 de SW4 via son interface fa0/24.
   - Ajouter un commutateur SW5 relié au port fa0/23 de SWT via son interface fa0/24.
   - Paramétrer SW5 en client VTP.
   - Paramétrer SWT en mode VTP transparent et y ajouter les VLAN 2 et 3 manuellement.
   - Ajouter deux postes clients sur SW5 respectivement dans le VLAN 2 et 3 :
     - PC3 (192.168.2.5/24) connecté sur l'interface fa0/2 ;
     - PC4 (192.168.3.5/24) connecté sur l'interface fa0/3.
   - Ajouter le VLAN isolé 99 (associé au réseau 192.168.99.0/24) sur SWT, puis :
     - Vérifier que le VLAN n'est pas propagé sur les autres commutateurs ;
     - Ajouter deux postes (192.168.99.1/24 sur fa0/9 et 192.168.99.2/24 sur fa0/19) sur SWT dans le VLAN 99.

5. Tester l'ajout d'un nouveau serveur VTP dans votre domaine VTP :
   - Passer SW2 en mode VTP server, puis vérifier la configuration VTP de SW2 et de SW4 ;
   - Ajouter un VLAN 6 (nommé info) sur SW2 et tester sa propagation dans les clients et le comportement du premier serveur SW4.

Annexe 1 : Routage inter-VLAN avec la méthode « router-on-a-stick » (sous interfaces et mode trunk[1])

Extraits d'une source Cisco – http://netacad.com

Pourquoi utiliser des sous-interfaces ?

Le routage inter-VLAN existant au moyen d'interfaces physiques se heurte à une limite de taille. Les routeurs disposent d'un nombre limité d'interfaces physiques pour se connecter aux différents réseaux. À mesure que le nombre de VLAN augmente sur un réseau, la nécessité de posséder une interface de routeur physique par VLAN épuise rapidement la capacité du routeur.

Dans les grands réseaux, l'une des alternatives consiste à avoir recours au trunking VLAN et aux sous-interfaces. Le trunking VLAN permet à une seule interface physique de routeur d'acheminer le trafic de plusieurs VLAN. Cette technique est appelée « router-on-a-stick » et utilise des sous-interfaces virtuelles sur le routeur pour dépasser les limites matérielles reposant sur les interfaces physiques du routeur.

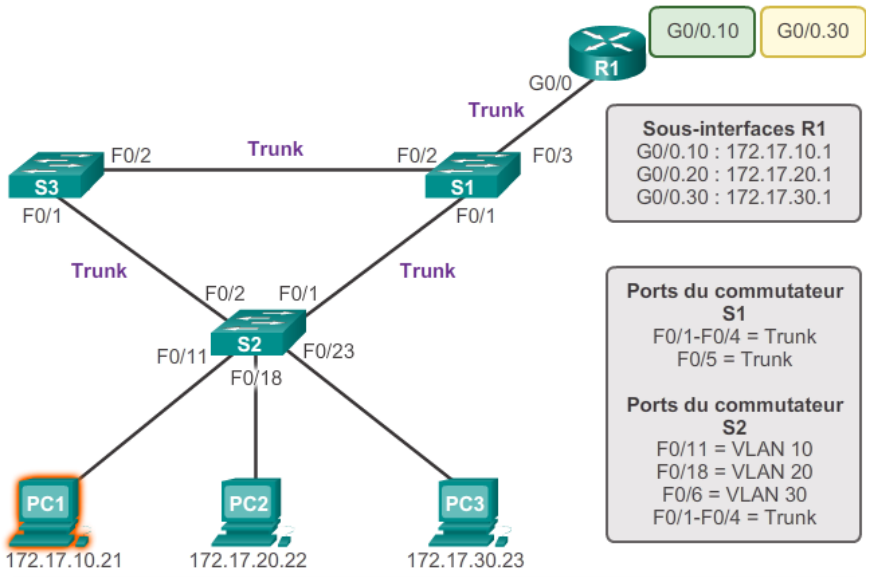
Les sous-interfaces sont des interfaces virtuelles basées sur un logiciel qui sont affectées à des interfaces physiques. Chaque sous-interface est configurée indépendamment avec sa propre adresse IP et son propre masque de sous-réseau. Cela permet à une seule interface physique de faire simultanément partie de plusieurs réseaux logiques.

Nommage et configuration des sous-interfaces du routeur

En mode *router-on-a-stick*, la configuration du routeur diffère par rapport à celle qu'utilise le routage inter-VLAN classique. La figure ci-dessous montre que plusieurs sous-interfaces sont configurées.

Chaque sous-interface est créée à l'aide de la commande de mode de configuration globale **interface** *interface_id subinterface_id*. La syntaxe pour la sous-interface est l'interface physique, dans ce cas **g0/0**, suivie d'un point et d'un numéro de sous-interface. Le numéro de sous-interface est libre (max : 2^{32}), mais il reflète généralement le numéro du VLAN. Dans cet exemple, les sous-interfaces portent les numéros **10** et **30** pour faciliter la mémorisation des numéros des VLAN auxquels elles sont associées. La sous-interface GigabitEthernet 0/0.10 est créée à l'aide de la commande en mode de configuration globale **interface g0/0.10.**

Sur l'exemple ci-dessous, l'interface physique G0/0 du routeur a donc été « divisée » en trois sous-interfaces nommées G0/0.10, G0/0.20 et G0/0.30 lesquelles ont leur propre adresse IP et leur appartenance à un VLAN : 10, 20 ou 30.



[1]Le terme de TRUNK dans le sens 'agrégation de VLAN' est propre à CISCO. Les autres constructeurs l'utilisent plutôt dans le sens 'agrégation de liens'. L'agrégation de liens est alors indiquée par la notion de 'ports tagués' [tagged/untagged ports].

1) Le PC1 sur le VLAN 10 communique avec le PC3 sur le VLAN 30 via le routeur R1 en utilisant une seule interface de routeur physique.
2) Le PC1 envoie son trafic de monodiffusion au commutateur S2.
3) Le commutateur S2 marque alors le trafic de monodiffusion comme provenant du VLAN 10 et le transmet par sa liaison trunk au commutateur S1.
4) Le commutateur S1 transfère le trafic étiqueté depuis l'autre interface trunk sur le port F0/5 vers l'interface du routeur R1.
5) Le routeur R1 accepte le trafic de monodiffusion étiqueté sur le VLAN 10 et l'achemine vers le VLAN 30 en utilisant ses sous-interfaces configurées.
6) Le trafic de monodiffusion est étiqueté avec le VLAN 30 lors de son transfert depuis l'interface de routeur vers le commutateur S1.
7) Le commutateur S1 transmet le trafic de monodiffusion étiqueté via l'autre liaison trunk au commutateur S2.
8) Le commutateur S2 supprime l'étiquette VLAN de la trame de monodiffusion et transfère la trame au PC3 sur le port F0/6.

Avant de recevoir une adresse IP, une sous-interface doit être configurée pour fonctionner sur un VLAN spécifique à l'aide de la commande **encapsulation dot1q** *vlan_id*. Dans cet exemple, la sous-interface G0/0.10 est affectée au VLAN 10 et la sous-interface G0/0.30 au VLAN 30.

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
```

Une fois les sous-interfaces configurées, elles doivent être activées. Lorsque l'interface physique est activée avec la commande **no shutdown**, toutes les sous-interfaces configurées sont activées. De la même manière, si l'interface physique est désactivée, toutes les sous-interfaces le sont également. Dans cet exemple, la commande **no shutdown** est exécutée en mode de configuration d'interface pour l'interface G0/0 qui, à son tour, active toutes les sous-interfaces configurées.

```
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
```

Remarque : la méthode router-on-a-stick de routage inter-VLAN ne va pas au-delà de 50 VLAN.

Vérification des sous-interfaces

La commande **show vlans** affiche des informations sur les sous-interfaces VLAN du logiciel Cisco IOS. Le résultat présente les deux sous-interfaces VLAN, GigabitEthernet 0/0.10 et GigabitEthernet 0/0.30.

```
R1# show vlans
<résultat omis>
Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.10

  Protocols Configured:  Address:     Received:   Transmitted:
          IP             172.17.10.1         11             18
<résultat omis>
Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.30

  Protocols Configured:  Address:     Received:   Transmitted:
          IP             172.17.30.1         11              8
```

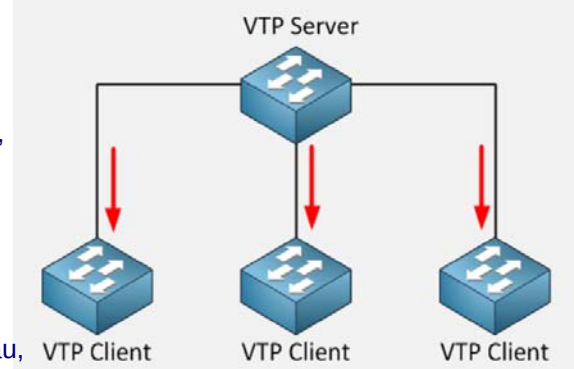
Examinons ensuite la table de routage à l'aide de la commande **show ip route**.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP,M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
       L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default,
       U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP,
       l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

   172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
C      172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L      172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C      172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L      172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

Dans l'exemple, les routes définies dans la table de routage indiquent qu'elles sont associées à des sous-interfaces spécifiques, et non à des interfaces physiques distinctes. Il existe deux routes dans la table de routage. Une route mène au sous-réseau 172.17.10.0, connecté à la sous-interface locale G0/0.10. L'autre route mène au sous-réseau 172.17.30.0, connecté à la sous-interface locale G0/0.30.

Annexe 2 : comprendre le VTP (source Cisco2)

Un commutateur doit être déclaré en serveur et on lui attribue un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifié ou supprimé. Ainsi chaque commutateur client présent dans le domaine héritera automatiquement des VLAN créés sur le commutateur serveur.
Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants :



- **Le mode serveur**
  - L'information est stockée dans la NVRAM,
  - il définit le nom de domaine VTP,
  - il peut ajouter, modifier ou supprimer un VLAN,
  - il stocke la liste des VLAN du domaine VTP.
- **Le mode client VTP :**
  - il possède un nom de domaine,
  - il stocke une liste de VLAN non modifiable.
- **Le mode transparent :**
  - il ne participe pas aux domaines VTP du réseau,
  - il transmet les paquets VTP via ses liens Trunk,
  - il possède sa propre liste de VLAN qu'il est possible de modifier.

Remarques :

- Les messages VTP se propagent sur les liens configurés en **Trunk** (norme **802.1Q**).
- VTP ne gère que la plage de VLAN comprise entre **1 et 1005**. La plage étendue 1006 à 4096 n'est pas supportée. Pour cela, il faut basculer en mode *Transparent* sur tous les switchs et créer ses VLAN étendus à la main.
- Il existe **3 versions** de VTP, bien vérifier qu'une et une seule version est active sur son réseau pour éviter les surprises (v1 et v2 sont incompatibles entre elles).
- La configuration VTP n'est pas visualisable dans la running-config mais est stockée dans le fichier ***vlan.dat*** (comme la configuration des VLAN) situé dans la mémoire flash (un *show flash:* permet de voir ce fichier).

Configurer VTP

- **Sur le commutateur serveur :**

server(config)# vtp domain testVTP	*Configurer le domaine VTP qui permet à tous les commutateurs d'être dans le même "groupe"*
server(config)# vtp mode server	*Configurer le mode serveur*
server(config)#VTP password SESAME	*Configurer le mot de passe pour sécuriser les échanges VTP (Optionnel)*

- **Sur le commutateur client :**

client(config)# vtp domain testVTP	*Indiquer le domaine VTP.*
client (config)#vtp mode client client (config)#vtp mode transparent	*Configurer le mode: client ou transparent*
server(config)#vtp password SESAME	*Donner le mot de passe identique à celui du serveur*

Note :

Sur une configuration initiale, l'ajout est facultatif, car si le domaine VTP n'est pas renseigné, c'est la première annonce qui est acceptée comme nom de domaine et enregistrée. Si un nom de domaine existe déjà, il n'y a pas de modification. Cela permet d'avoir plusieurs domaines VTP sur la même infra (même si c'est quand même déconseillé).

[2] Présentation du protocole VTP : http://www.cisco.com/cisco/web/support/CA/fr/109/1092/1092443_21.pdf)

La commande SHOW VTP STATUS permet de vérifier la configuration VTP sur les commutateurs :

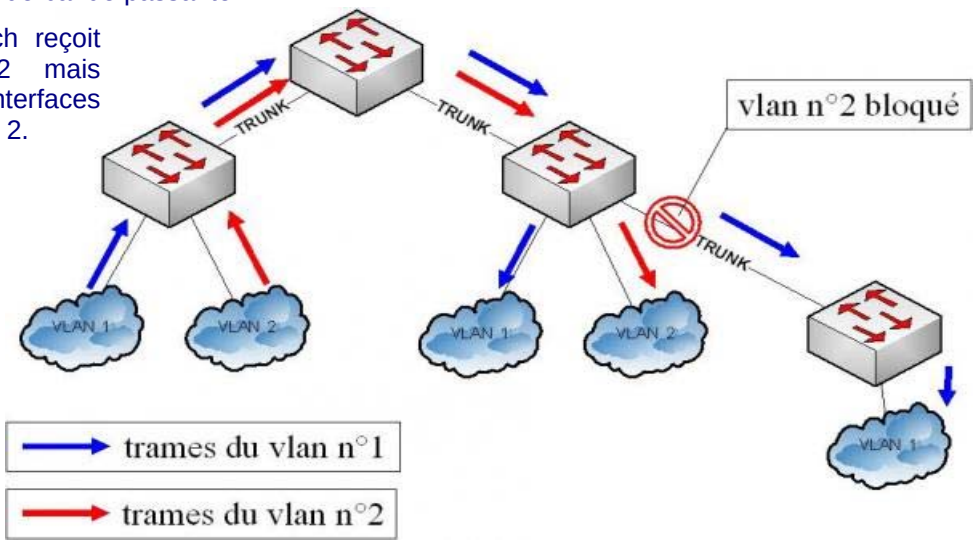
server# show vtp status	**client# show vtp status**
VTP Version : 2 Configuration Revision : 4 Maximum VLANs supported locally : 255 Number of existing VLANs : 7 VTP Operating Mode : Server VTP Domain Name : testVTP VTP Pruning Mode : Disabled VTP V2 Mode : Disabled VTP Traps Generation : Disabled MD5 digest : 0x5D 0x23 0x68 0xA9 0x6D 0xBD 0x06 0x63 Configuration last modified by 0.0.0.0 at 3-1-93 00:07:38	VTP Version : 2 Configuration Revision : 4 Maximum VLANs supported locally : 255 Number of existing VLANs : 7 VTP Operating Mode : Client VTP Domain Name : testVTP VTP Pruning Mode : Disabled VTP V2 Mode : Disabled VTP Traps Generation : Disabled MD5 digest : 0x5D 0x23 0x68 0xA9 0x6D 0xBD 0x06 0x63 Configuration last modified by 0.0.0.0 at 3-1-93 00:07:38

Note sur le VTP Pruning : cette commande optionnelle et non disponible dans Packet Tracer permet de faire des économies de bande passante.

Imaginons qu'un switch reçoit les VLAN 1 et 2 mais qu'aucune de ses interfaces appartiennent au VLAN 2.

Lorsque le switch voisin lui enverra des trames du VLAN 2, ce switch les supprimera car aucune de ses interfaces n'appartient à ce VLAN.

Il est donc inutile que le switch voisin lui envoie du trafic pour le VLAN 2.



On active alors la fonction *VTP pruning* pour avertir le switch voisin de ne pas lui envoyer de trafic pour ce VLAN. La fonction s'active à partir du switch Server.