1 But

Le but de se TP est de segmenter le réseau d'une petite entreprise dont le câblage est figé à l'aide de VLAN.

2 Les VLAN

2.1 Définition

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

2.2 Les types de VLAN

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

- **VLAN de niveau 1** (aussi appelés VLAN par port, en anglais Port-Based VLAN) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur ;
- **VLAN de niveau 2** (également appelé VLAN MAC, VLAN par adresse IEEE ou en anglais MAC Address-Based VLAN) consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station ;
- **VLAN de niveau 3** : on distingue plusieurs types de VLAN de niveau 3 :
  - Le VLAN par sous-réseau (en anglais Network Address-Based VLAN) associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifient automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
  - Le VLAN par protocole (en anglais Protocol-Based VLAN) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

2.3 Les avantages du VLAN

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramètrage des commutateurs
- Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées
- Réduction de la diffusion du traffic sur le réseau

2.4 Plus d'informations

Les VLAN sont définis par les standards **IEEE 802.1D, 802.1p, 802.1Q et 802.10**.

Pour plus d'information vous pouvez lire l'excellent article de François Goffinet, Instructeur Cisco :

http://cisco.goffinet.org/s3/c8c9

3 Prérequis

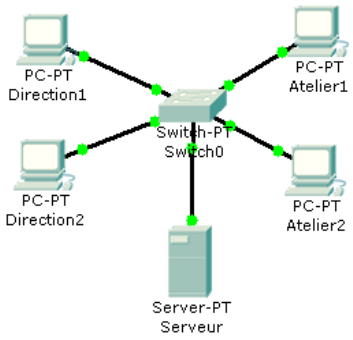
Pour réaliser ce TP, vous devez avoir fait les TP « Le matériel dans un réseau local TCP/IP », « Configuration des routeurs Cisco avec l'IOS » et « Les ACL – Création d'une DMZ ».

Vous aurez besoin du logiciel Packet Tracer V4.1 de Cisco.

4 Travail a réaliser

4.1 Le réseau

Réalisez la structure de réseau suivante :



Une petite entreprise dispose d'un local comprenant des bureaux (direction) et d'un atelier. L'ensemble est équipé d'un câblage ethernet dont tous les liens (cat 6) aboutissent dans une armoire de brassage et sont connectés à un switch Cisco manageable.

Pour des raisons de sécurité, les réseaux des deux services doivent être séparés. Toutefois, le serveur doit accessible des deux services.

Il n'est pas possible de les séparer physiquement, donc la séparation devra-t-être logique.

4.2 Deux réseaux logiques sur un même réseau physique

L'idée est de paramétrer les machines d'un même service avec une adresse IP et un masque incompatible avec les machines des autres services :

Direction	*Atelier*
192.168.1.0 / 24	192.168.2.0 / 24

Paramétrez les postes de travail avec des adresses appartenant à leur réseau. Le serveur appartient au service Direction.

Procédez aux tests de connectivité.

Source	*Destination*	*Résultat*
Direction1	Direction2	
Direction*x*	Atelier*x*	
Direction*x*	Serveur	
Atelier1	Atelier2	
Atelier*x*	Serveur	

Un employé de l'atelier a eu connaissance du type d'adressage IP en vigueur à la direction. Est-ce un problème pour la sécurité ? Expliquez pourquoi. (Simulez la situation)

4.3 Séparation par VLAN

Pour palier aux problèmes de sécurité, vous allez mettre en place une séparation des deux réseaux par VLAN.

Le switch est manageable et permet de créer des VLAN. Cliquez sur le switch, puis sur l'onglet Config et sur le bouton VLAN Database.

Créez un VLAN nommé « direction » et affectez lui le numéro 10.

Cliquez sur le bouton FastEthernet 0/0 (vérifiez que cette interface est connectée à direction1).

Créez l'association de ce port avec le VLAN « direction » en mode access.

Relevez les commandes IOS générée :

```
Switch>
```

Cliquez sur l'onglet CLI et créez en commandes IOS le VLAN « atelier » avec le numéro 20 et associez les ports connectés aux différentes machines avec les VLAN adéquats.

Procédez aux tests de connectivité.

Source	***Destination***	***Résultat***
Direction1	Direction2	
Direction*x*	Atelier*x*	
Direction*x*	Serveur	
Atelier1	Atelier2	
Atelier*x*	Serveur	

Modifiez le paramétrage réseau de Atelier1 pour qu'il ait une adresse IP compatible avec le réseau Direction. Procédez aux test de connectivité :

Source	***Destination***	***Résultat***
Atelier1	Atelier2	
Atelier1	Direction1	
Atelier1	Serveur	

Conclusion :

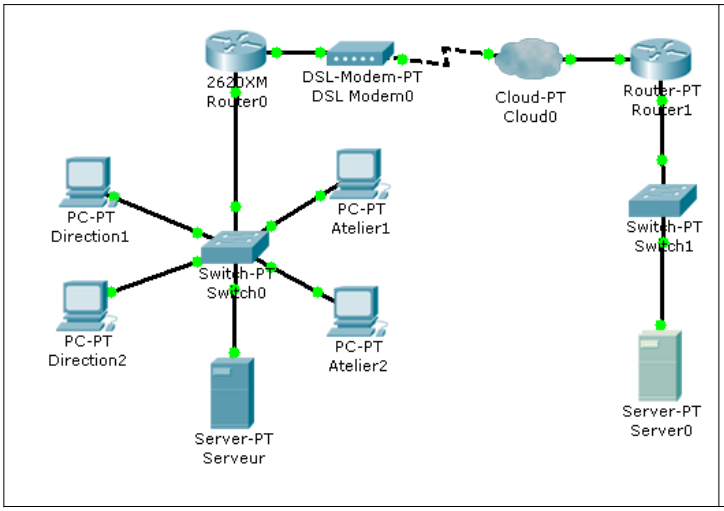
Sur un commutateur, on distinguera les ports dits "**access**" des ports dits "**trunk**". Un port "**access**" est un port qui ne transportera des informations que d'un seul VLAN. A priori, ce type de port connectera une station. Un port "**trunk**" est un port qui transportera des informations de plusieurs VLANs. On y connectera un autre commutateur, un routeur ou même la carte réseau 802.1q d'un serveur. Autrement dit, un port "access" n'est pas un port "trunk" et inversément. Toutefois, sur les switches Cisco on aura la possibilité de configurer le port en mode dynamique grâce au Dynamic Trunk Protocol (DTP, protocole point à point propriétaire Cisco).

http://cisco.goffinet.org/s3/vlan_concept

Que faudrait-il faire pour que le serveur soit accessible depuis les deux VLAN.

Packet Tracer ne permet pas de simuler une carte réseau 802.1q. Pour rendre accessible le serveur par les deux VLAN, on utilisera donc un routeur, ce qui présente aussi l'intérêt d'établir une connexion commune à tous les postes à internet et la définitions de règles de filtrages et de sécurisation.

4.4 Interconnexion des VLAN à l'aide d'un routeur



Router0-Modem : .....10.0.0.1 / 8
Router1-Cloud0 : .....10.0.0.2 / 8
Router1-Switch1 : .....89.0.0.1 / 8
Server0 : .....89.0.0.2 / 8

Mettez en place le routage automatique RIP sur les routeurs

Activez le service HTTP sur Server0

Router0 doit appartenir aux deux VLAN. Ses interfaces FastEthernet supportent la norme IEEE 802.1Q.

Sur Switch0, créez une association de type Trunk entre le port connecté au routeur et les VLAN.

Sur le routeur, configurez les interfaces virtuelles FastEthernet 0/0.10 et FastEthernet 0/0.20 :

```
Router0(config)# in fa 0/0.10
Router0(config-subif)# encapsulation dot1Q 10
Router0(config-subif)# ip address 192.168.1.254 255.255.255.0
Router0(config-subif)#exit
Router0(config)# in fa 0/0.20
...
```

Paramétrez les passerelles par défaut sur les postes des VLAN Direction et Atelier :

VLAN	*Passerelle par défaut*
Direction	
Atelier	

Procédez aux tests de connectivité :

Source	*Destination*	*Résultat*
Direction1	Direction2	
Direction*x*	Atelier*x*	
Direction*x*	Serveur	
Atelier1	Atelier2	
Atelier*x*	Serveur	

Vérifiez la connexion à internet (navigateur web) pour chaque postes de l'entreprise :

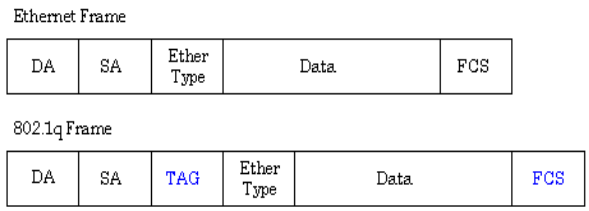
Placez-vous en mode simulation , filtrez le protocole ICMP et depuis Direction1, pinguez Serveur.

Dans la liste des évènements, consultez le format des trames entre chaque appareil : Double-cliquez sur l'évènement pour rendre visible le message sur le schéma, puis cliquez sur l'enveloppe et sur l'onglet « Inbound PDU Detail ».

Vous constatez la différence entre les trames émises depuis un port « access » et « trunk » du switch.

Le fonctionnement des VLANs inter-opérables IEEE 802.1q répondent au principe de l'étiquetage des trames (tagging) par l'ajout dans les trames d'un "tag" de 4 octets ou 32 bits dont 12 bits sont consacrés au numéro de VLAN. Sur un ou plusieurs swiches, seuls les trames possédant ce même numéro peuvent communiquer ensemble d'un commutateur à l'autre ou à une carte réseau IEEE802.1Q.

Une trame entrant sur un port de commutateur est "étiquetée" si elle doit passer à un autre commutateur via un port « trunk ». Cette étiquette ne sera retirée que lorsque la trame sera commutée vers la destination finale dans le bon VLAN.



Que contient le champs TAG ?

L'état actuel du réseau satisfait-il :

• aux exigences de connexion ?	
• aux exigences de sécurité ?	

Rappel : on souhaite que tous les postes de l'entreprise puissent accéder à internet, au serveur interne mais l'atelier ne doit pas accéder à la direction.

4.5 Sécurisation des accès

Pour réaliser ce type de filtrage des accès, il faut utiliser une liste de contrôle d'accès associée aux interfaces virtuelles du routeur de l'entreprise :

Créez une liste de contrôle d'accès étendue appliquée en entrée sur chaque interface virtuelle du routeur pour effectuer les opérations suivantes :

- Tous les hôtes pour tous les protocoles ip peuvent accéder au serveur.
- Le serveur pour tous les protocoles ip peut accéder à tous les hôtes.
- Les hôtes du réseau Ateliers pour tous les protocoles ip ne doivent pas accéder au réseau Direction.

```
Router0(config)#
```

Expliquez chacune des lignes access-list ci-dessus.

Effectuez les tests de connectivité :

Source	***Destination***	***Résultat***
Direction*x*	Atelier*x*	
Atelier*x*	Direction*x*	
Direction*x*	Serveur	
Atelier*x*	Serveur	
Direction*x*	Internet	
Atelier*x*	Internet	
Serveur	Internet	

4.6 Conclusion

Représentez le schéma équivalent du réseau physique ainsi créez et précisez quels les avantages fournis par l'utilisation des VLAN.

Equivalent réseau physique	Avantages des VLAN :