

2022-
2024

Les VLAN

FIRAS RASSAA

ETUDIANT | ENSITECH

Sommaire

1.Définition des VLAN

2.Rôle des VLAN

3.Avantages des VLAN

4.Types de VLAN

5. Création des VLAN et affectation des ports aux mode Access et mode Trunk

6.Le routage inter-VLAN

1.Définition

Un VLAN, pour Virtual Local Area Network, décrit un type de réseau local. On le traduit en français par réseau local virtuel.

Le VLAN regroupe, de façon logique et indépendante, un ensemble de machines informatiques. On peut en retrouver plusieurs coexistant simultanément sur un même commutateur réseau.

2.Rôle des VLAN

Les VLAN permettent à un administrateur de segmenter les réseaux, les VLAN sont couramment utilisés pour segmenter le réseau par département ou par équipe. L'objectif est de faciliter la gestion et la sécurité des données.

Segmentation logique : Les VLAN permettent de diviser un réseau physique en plusieurs segments logiques. Cela peut être utile pour séparer différents types de trafic réseau, tels que le trafic des utilisateurs finaux, le trafic des serveurs, le trafic de gestion, etc.

Sécurité : Les VLAN peuvent aider à renforcer la sécurité du réseau en limitant l'accès aux ressources réseau sensibles. Par exemple, en plaçant les ordinateurs sensibles sur un VLAN distinct, on peut restreindre l'accès à ces ordinateurs uniquement aux utilisateurs autorisés.

Optimisation des performances : En segmentant le trafic réseau en fonction de son type, les VLAN peuvent aider à optimiser les performances du réseau. Par exemple, en isolant le trafic de diffusion (broadcast) sur des VLAN distincts, on peut réduire la quantité de trafic broadcast dans chaque segment, ce qui améliore les performances globales du réseau.

Gestion réseau : Les VLAN facilitent la gestion du réseau en permettant aux administrateurs réseau de regrouper des périphériques réseau logiquement, indépendamment de leur emplacement physique. Cela facilite la gestion des politiques de réseau, la configuration des périphériques réseau et la détection des problèmes.

3.Avantages des VLAN

Les principaux avantages des VLAN sont les suivants :

Sécurité : Les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité

Réduction des coûts : des économies sont réalisées grâce à une diminution des mises à niveau onéreuses du réseau et à l'utilisation plus efficace de la bande passante.

Meilleures performances : le fait de diviser des réseaux en plusieurs domaines de diffusion, réduit la quantité de trafic inutiles sur le réseau et augmente les performances

Réductions de la taille des domaines de diffusion : le fait de diviser un réseau en VLAN réduit le nombre de périphérique dans le domaine de diffusion

Gestion simplifiée : En regroupant logiquement les périphériques réseau en fonction de leur fonction ou de leur département, les VLAN facilitent la gestion des politiques réseau, des autorisations d'accès et des configurations de sécurité.

4.Types de VLAN

Il existe plusieurs types de VLAN

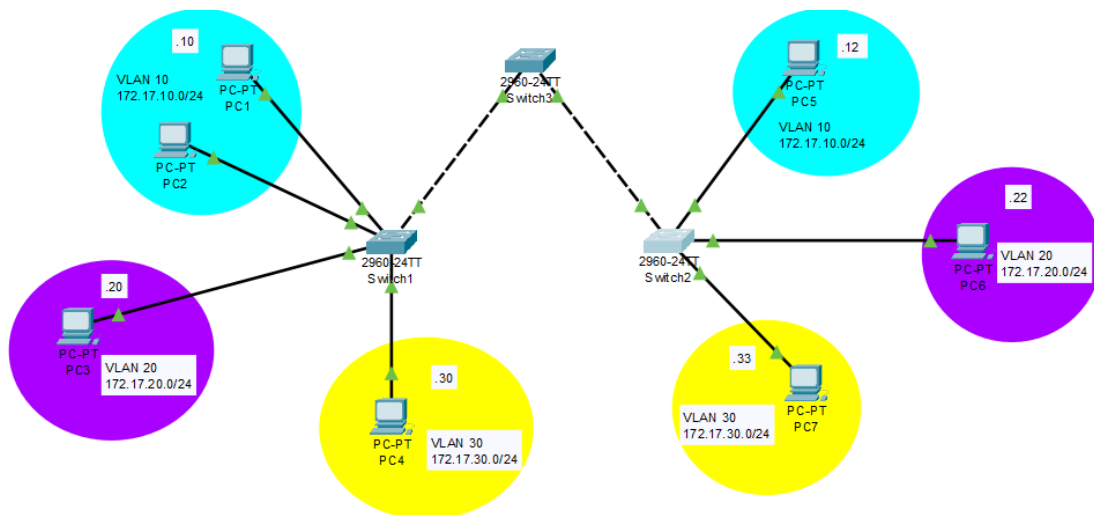
VLAN de données : Un VLAN de données est un réseau local virtuel configuré pour transmettre le trafic généré par l'utilisateur. Les VLAN de données sont utilisés pour diviser un réseau en groupes d'utilisateurs ou de périphériques.

VLAN par défaut: Au démarrage initial d'un commutateur, tous ses ports font partie du VLAN par défaut qui est le VLAN 1.

VLAN natif : Toutes les trames passant par un "Trunk" sont ainsi étiquetées sauf les trames appartenant au VLAN natif. Donc, les trames du VLAN natif, par défaut le VLAN 1, ne sont pas étiquetées

VLAN de gestion : Un VLAN de gestion est un réseau local virtuel configuré pour accéder aux fonctionnalités de gestion d'un commutateur via une adresse IP (ICMP, Telnet, SNMP, HTTP)

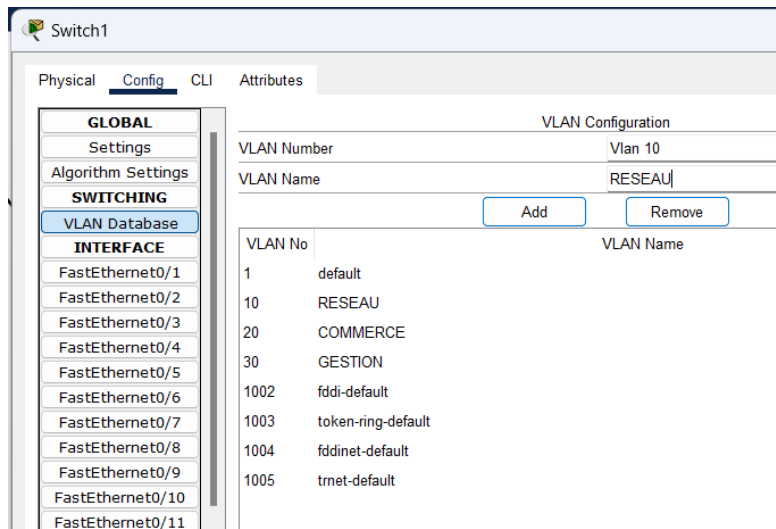
5. Création des VLAN et affectation des ports aux mode Access et mode Trunk



Pour ce TP on a imaginé une architecture réseau, on l'a réalisée sur Cisco packet tracer, l'objectif de ce tp est la création de 3 VLAN, puis d'affecter les ports au VLAN en mode Access

Pour commencer on va créer les VLAN pour cela deux manières sont possible par le terminal CLI ou directement dans l'onglet configuration, on privilégiera le terminal

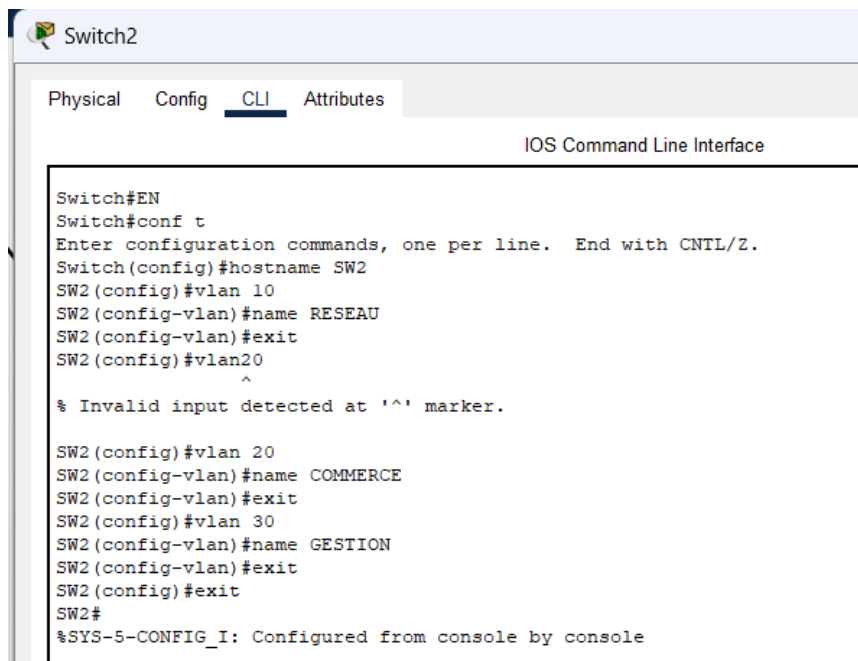
La première façon de création des VLAN est dans l'onglet config en entrant les informations du VLAN, procéder donc comme ci-dessous :



The screenshot shows the Cisco Packet Tracer interface for Switch1. The 'Config' tab is active, and the 'VLAN Database' is selected. The 'VLAN Configuration' section shows a new VLAN being created with the number 10 and the name RESEAU. The 'Add' button is highlighted.

VLAN No	VLAN Name
1	default
10	RESEAU
20	COMMERCE
30	GESTION
1002	fdi-default
1003	token-ring-default
1004	fdinet-default
1005	trnet-default

La méthode qu'on va adopter est donc la suivante celle où l'on configure les VLAN directement par le terminal, voici un exemple ci-dessous :



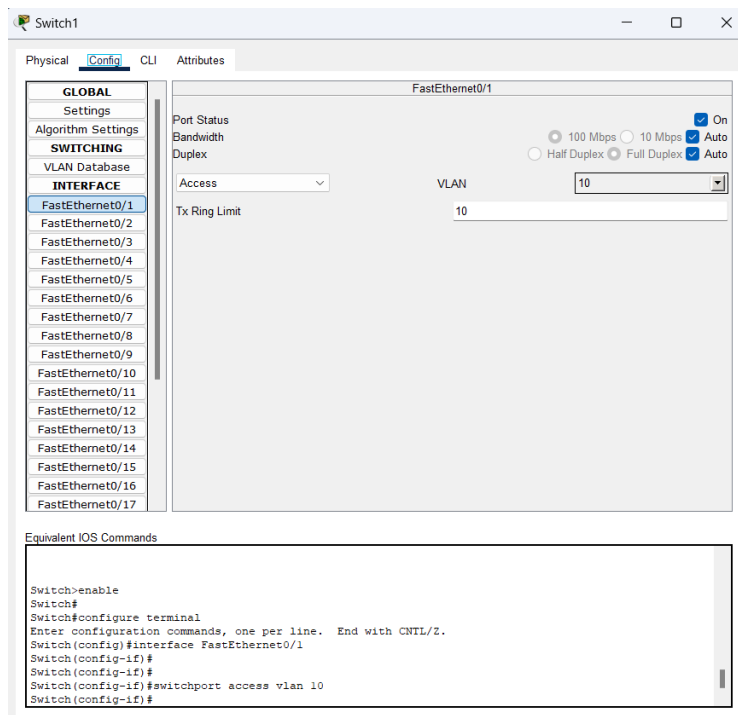
```
Switch2
Physical Config CLI Attributes
IOS Command Line Interface

Switch#EN
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW2
SW2(config)#vlan 10
SW2(config-vlan)#name RESEAU
SW2(config-vlan)#exit
SW2(config)#vlan20
^
% Invalid input detected at '^' marker.

SW2(config)#vlan 20
SW2(config-vlan)#name COMMERCE
SW2(config-vlan)#exit
SW2(config)#vlan 30
SW2(config-vlan)#name GESTION
SW2(config-vlan)#exit
SW2(config)#exit
SW2#
%SYS-5-CONFIG_I: Configured from console by console
```

Nous avons correctement créer les VLAN, l'étape suivante est donc l'affectation des ports au VLAN

Pour affecter les VLAN aux ports on peut aussi procéder des deux manières qu'on a pu voir précédemment, par la config directement ou bien par le terminal



On peut remarquer les commandes de configuration du CLI lorsqu'on affecte le port de l'interface du Switch 1 aux VLAN 10.



Pour configurer directement par le CLI, dirigez-vous directement sur le terminal du Switch 2 puis exécuter les commande suivante : En → conf t → int fa0/2 (en fonction de votre câblage) → switchport mode access → switchport access vlan 10.

Voici un exemple de la configuration par CLI :

```
SW2(config)#interface FastEthernet0/1
SW2(config-if)#
SW2(config-if)#
SW2(config-if)#switchport access vlan 1
SW2(config-if)#exit
SW2(config)#interface fa0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 10
SW2(config-if)#exit
SW2(config)#int fa0/3
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 20
SW2(config-if)#exit
SW2(config)#int fa0/4
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 30
SW2(config-if)#exit
SW2(config)#
```

Remarque : Le mode access sur Cisco Packet Tracer est une façon de configurer un commutateur (switch) pour que chaque port soit assigné à un seul groupe d'appareils appelé VLAN. Cela permet de garder les appareils connectés sur un port séparés des autres, sauf s'ils sont dans le même groupe.

Essayez maintenant de tester la connectivité entre le PC1 et le PC5, on envoie un paquet du PC1 au PC5 on constate qu'il ne peuvent pas communiquer ensemble.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC1	PC5	ICMP		0.000	N	0	(edit)	

Cela est tout à fait normal nous devons donc configurer le SW3

Suivez la procédure que vous préférez pour créer les VLAN sur le switch 3

Une fois les VLAN créés, nous allons configurer les ports en mode trunk utiliser la méthode que vous préférez, pour le SW3 on utilisera le CLI :

- Hostname SW3 → interface range (pour regrouper les deux interfaces du switch) fa0/1-2 → switchport mode trunk → switchport trunk allowed (pour lui affecter les VLAN) vlan 10,20,30 → exit

```
Switch(config)#hostname SW3
SW3(config)#int
% Incomplete command.
SW3(config)#int range fa
% Incomplete command.
SW3(config)#int range fa0
^
% Invalid input detected at '^' marker.

SW3(config)#int range fa0/1-2
SW3(config-if-range)#switchport mode trunk

SW3(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

SW3(config-if-range)#switchport trunk allowed vlan 10,20,30
SW3(config-if-range)#exit
```

Surtout n'oubliez pas de configurer les deux autres switch, pour ma part je les configure avec la configuration directe.

Le PC1 et le PC5 peuvent maintenant communiquer ensemble.

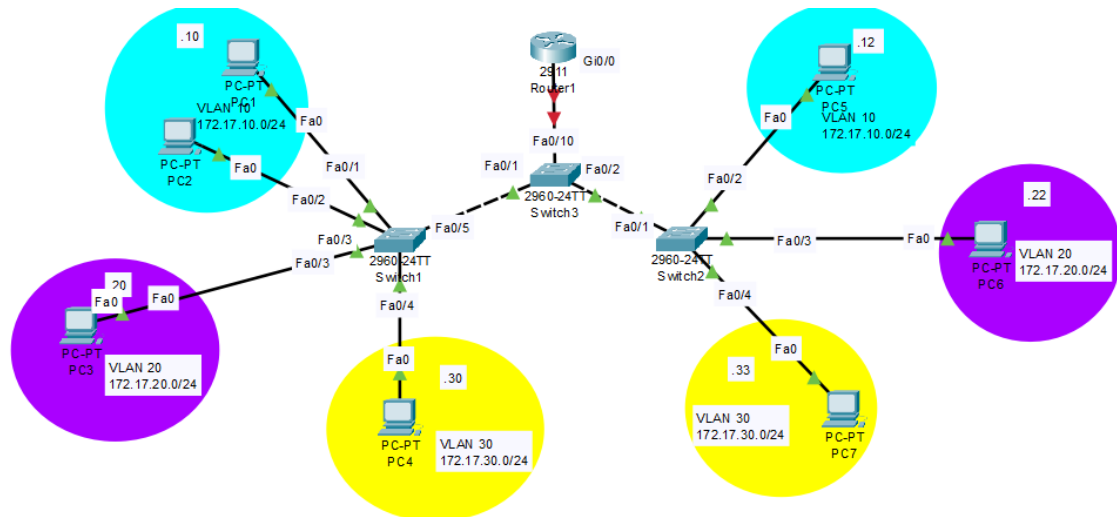
Par contre quand on essaye de faire communiquer le PC1 du VLAN 10 avec le PC3 du VLAN 20, cela ne fonctionne pas, en effet pour qu'il puisse communiquer nous devons ajouter un routeur et le configurer, c'est ce que nous allons voir dans la partie routage inter-VLAN.

Remarque : Le mode trunk sur Cisco Packet Tracer est une configuration spéciale sur un commutateur (switch) qui permet à un seul port de transmettre plusieurs VLAN à la fois.

6. Le routage inter-VLAN

Pour cette partie on rajoute un routeur qui va nous permettre de faire communiquer les VLAN entre eux.

Routeur : Un routeur est un appareil qui dirige le trafic entre différents réseaux en analysant les adresses IP des paquets de données et en choisissant le meilleur chemin pour les acheminer à leur destination.



Nous allons donc configurer l'interface fa0/10 du switch 3 pour lui allouer les vlan 10,20 et 30, pour cela diriger vous dans le terminal CLI et suivre la procédure suivante :

Enable → conf t → int fa0/10 → switchport mode trunk → switchport trunk allowed vlan 10,20,30 → exit

```
SW3>enable
SW3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#int fa0/10
SW3(config-if)#switchport mode trunk
SW3(config-if)#switchport trunk allowed vlan 10,20,30
SW3(config-if)#exit
SW3(config)#
SW3(config)#interface FastEthernet0/10
SW3(config-if)#
```

Maintenant on vas configurer l'interface du routeur, avec les 3 sous-interface, chaque sous-interface pour chaque vlan

Ouvrez le CLI du router puis suivez les étapes suivante :

- EN → conf t → hostname R1 → int g0/0.10 (pour créer une sous interface) → encapsulation dot1Q 10 (pour spécifier l'encapsulation VLAN) → ip add 172.17.10.1 255.255.255.0 → exit

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/0.10
^
% Invalid input detected at '^' marker.

R1(config)#int g0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip add 172.17.10.1 255.255.255.0
R1(config-subif)#exit
R1(config)#
```


Ensuite nous continuons pour les autres sous-interface :

Int g0/0.20 → encapsulation dot1Q 20 → Ip add 172.17.20.1 255.255.255.0

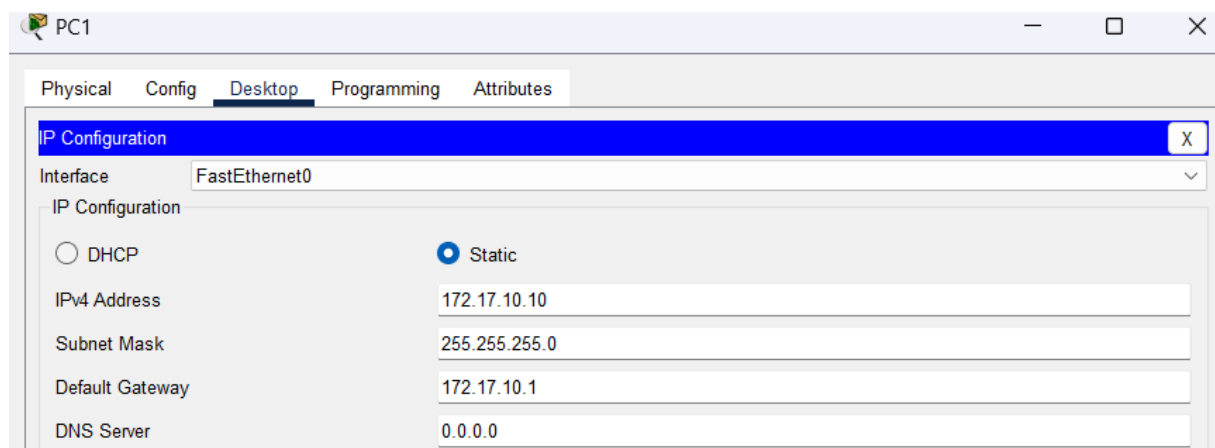
La même chose pour le VLAN 30 :

```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0.20
R1(config-subif)#encapsulation dot
% Incomplete command.
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip add 172.17.20.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#172.17.30.1 255.255.255.0
^
% Invalid input detected at '^' marker.

R1(config-subif)#ip add 172.17.30.1 255.255.255.0
R1(config-subif)#exit
R1(config)#
```

Il faut ensuite activer l'interface physique, donc toujours dans le terminal CLI du routeur 1, on va suivre la procédure suivante : int g0/0 → no shutdown

Le routeur est maintenant correctement configuré, il faut maintenant ajouter la passerelle à tout les pc dans IP configuration dans l'onglet dektop qui est 172.17.10.1 pour le VLAN 1 pour le VLAN 2 c'est 172.17.20.1 et pour le VLAN 3 c'est 172.17.30.1



Maintenant on peut essayer de faire communiquer le PC1 avec le PC6, cela fonctionne correctement

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	PC6	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC3	PC7	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC4	PC5	ICMP		0.000	N	2	(edit)	(delete)

Remarque : L'encapsulation permet avec un seul lien physique, le routage de plusieurs vlan.