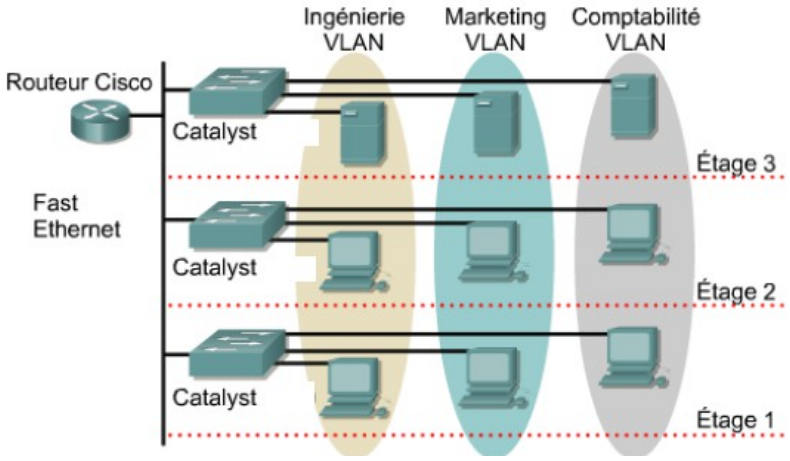
Les LAN virtuels - VLAN

1 – Présentation

Les VLANs sont des groupes d'utilisateurs répartis selon une méthode logique plutôt que par leur emplacement physique. Ainsi, il est possible sur un même commutateur de couche 2 de placer des utilisateurs appartenant à des réseaux IP différents. On retrouve les VLANs statiques qui sont définis selon le port du commutateur auquel l'utilisateur est connecté, et les VLANs dynamique. Ces derniers permettent de placer le port du commutateur automatiquement dans un VLAN défini, par exemple selon l'adresse MAC du poste qui s'y connecte.
Pour que les VLAN puissent communiquer entre eux, il est nécessaire de mettre en place un processus de routage, appelé routage inter-VLAN.

Principe de base routage inter-vlan



Dans cette architecture possédant des catalyts 2960 dit switch layer 2, seul le routeur permettra de faire le routage inter-vlan, a noté que Cisco permet de router des vlan sur des switch layer 2 grâce a des templates SDM.
Ces templates permettent d'optimiser les caractéristique du switch suivant sont utilisation sur le réseau.
Le template lan-base routing - SDM PREFER LANBASE-ROUTING – et permet au switch de gérer le routage statique IPV4 et créer 255 interfaces VLAN, ce template permet d'utiliser des commandes réservées au router et switch de niveau 3 – HSRP, IP ROUTING ...

Voici les 4 types de templates :

default : utilisation normal d'un layer 2 et équilibre de toutes les fonctions

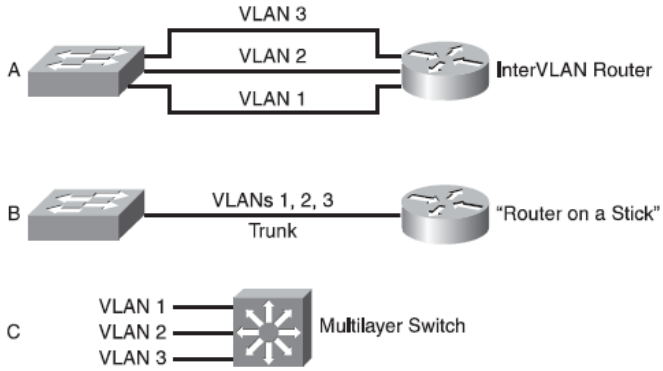
dual-ipv4-and-ipv6 : le Layer 2 pourra être utilisé dans des environnements dual-stack dit pile double ipv4 et ipv6 prenant en charge du coup l'ipv6, exemple pour configurer la double stack et le routage ipv4 et ipv6 on fera la commande suivante :

Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing

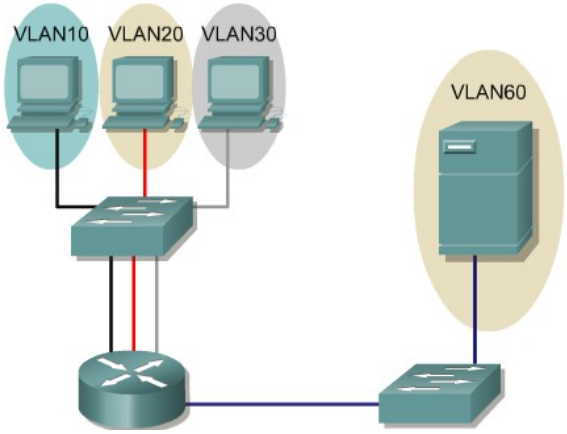
lanbase-routing : supporte la configuration de routes unicast autrement dit le routage statique

QOS : quality of service , gestion des flux suivant leur type VOIP , DATA, MGMT, … suivant votre configuration logique adoptée.

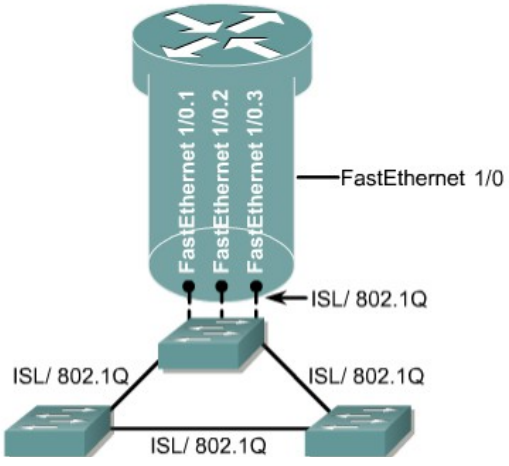
2 - Les 3 solutions de routage inter-vlan



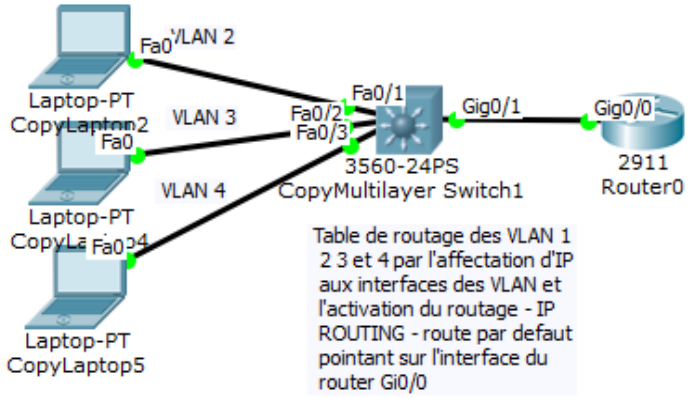
a. on connecte 3 interface du switch d'accès appartenant chacune a un vlan différent a 3 cartes fastethernet sur le routeur adressée avec l'adresse ip du vlan concerné.



b. on utilise un port du switch qu'on trunk/tag pour porter les vlan sur une fastEthernet du routeur qui possédé 3 sous interfaces IP appartenant chacune au sous-réseau des vlan concernés et qui est en mode trunk.



c. on utilise un switch de niveau 3/layer3 IP qui fera office de switch/routeur, switch et routeurs des schéma a et b seront concentré en switch de niveau 3, appelé aussi switch de distribution, contrairement au 2960 qui sont des switch d'accès ou dit switch de niveau 2 utilisé dans les schéma a et b ne gérant pas le routage et devant par conséquent utiliser un routeur externe.



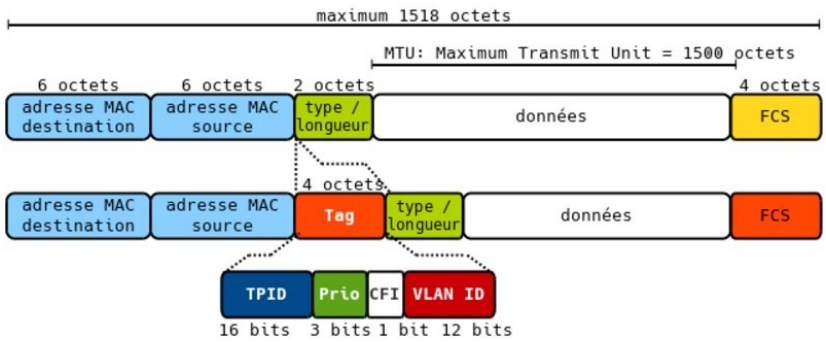
La notion de trunk ou Tag de vlan - 3 protocoles :

- propriétaire Cisco : ISL (Inter-Switch Link)
- 802.1q norme standart de IEEE
- Q in Q

ISL (inter switch Link)

Encapsulation des trames, propriétaire cisco très peu utilisé pour des raisons de compatibilité avec les autres marques, il encapsule la trame ethernet en lui rajoutant un header de 26 octets et un FCS (CRC) de 4 octets, le VLAN ID est codé dans un champ de 10 bits ne supportant que 1024 VLANs max.

802.1 Q ou Dot1q :Étiquetage de trame normalisée par l'IEEE.



Insertion d'un champ de 4 octet dans la trame Ethernet pour identifier les vlan (le tagging) :
-16 bits pour le champs ethertype (0x8100)

-3 bits pour la prioritée de la trame (802,1p), il fourni un mécanisme de qualité de service au niveau 2

-1 bit pour identifier un réseau token-ring

-12 bits pour le VLAN ID (soit 4096 possibilités). C'est appelé single tagging ou internal tagging.

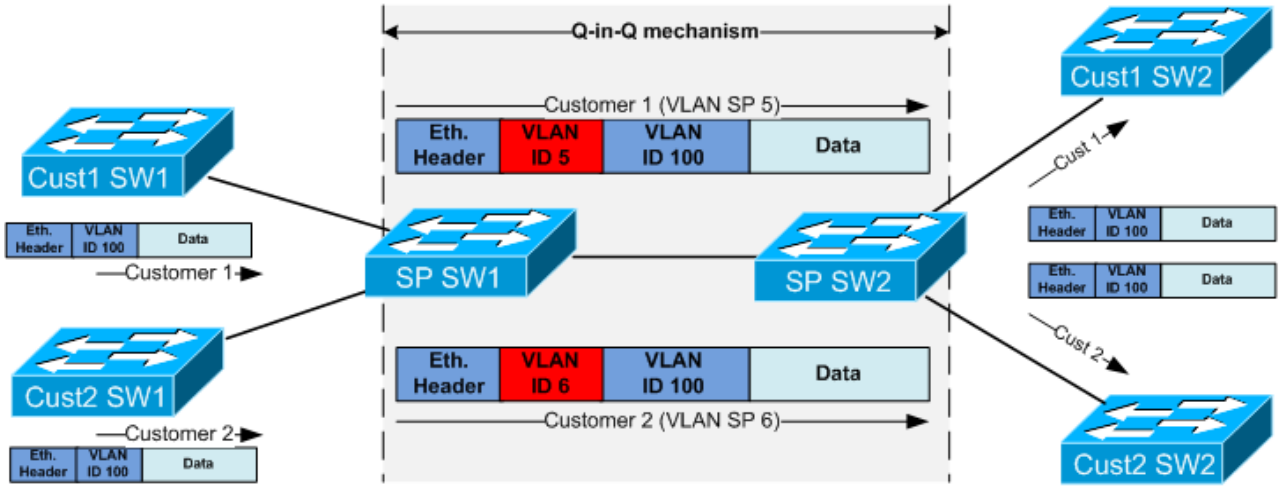
802.1QinQ Tunneling - 802,1AD

le **802 .1QinQ** permet de faire transiter des Vlan sur travers des liens WAN sur les protocoles WAN suivant :
EoMPLS : Ethernet over MPLS

Le 802.1ad est un avenant du 802.1q, appelé aussi VLANs stacking, la ou le 802.1q n'autorise qu'un seul TAG de VLAN par trame Ethernet, le QinQ permet d'insérer plusieurs TAG de VLAN dans la même trame Ethernet, permettant a un client de passer ses propres VLANs a l'intérieur d'un VLAN fournis par l'opérateur, de cette manière l'opérateur aura juste à configurer un VLAN pour chaque client sur son réseau

Le QinQ => Layer 2 protocol tunneling
Permet au fournisseur de préserver un TAG VLAN au travers du réseau WAN, en ajoutant un TAG 802,1Q qui correspond au client.

Il permet plus de flexibilité pour le design de l'architecture du client , **le trafic VTP , CDP** passent au travers de Q-in-Q de manière transparente.



3 - Format des trames Ethernet

Trame Ethernet standard

adresse MAC dst.	adresse MAC src.	EtherType/Size	Data	FCS

Trame Ethernet 802,1Q- Trunk IEEE

adresse MAC dst.	adresse MAC src.	**TPI (0x8100)**	**TCI (vlan)**	EtherType/Size	Data	FCS

TPI : Tag protocol identifier ou **Ethertype** sur 2 Octets, égal a 0x8100
Ethertype/size : le type de trame – **0x8100** en IPV4 et **0x86DD** en IPV6
TCI : Tag control information – 2 octets, égal au numéro de VLAN ID

Trame Ethernet 802.1AD – QinQ

adresse MAC dst.	adresse MAC src.	**S-TPI (0x88a8)**	**S-TCI (vlan)**	**C-TPI (0x8100)**	**C-TCI (vlan)**	EtherType/Size	Data	FCS

Le S (outer) représente le Fournisseur de service, C (inner) représente le client

S-TPI - **ISP:** Outer Tag Protocol Identifier ou Ethertype sur 2 octets (recommandé 0x88a8)

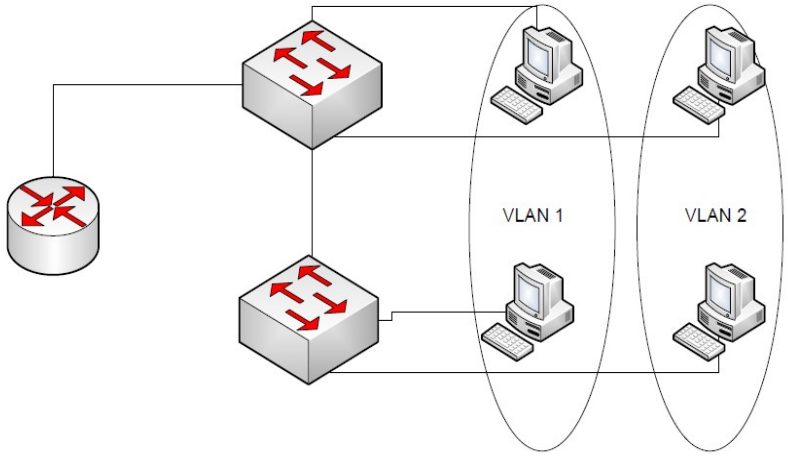
S-TCI : **ISP** Outer Tag Control Information sur 2 octets (le numéro du vlan externe)

C-TPI – **Customer :** Inner Tag Protocol Identifier ou Ethertype sur 2 octets (recommandé 0x8100)

C-TCI – **Customer :** Inner Tag Control Information sur 2 octets (le numéro du vlan interne)

Utiliser la norme IEEE 802.1ad implique **d'augmenter la taille maximal des trames Ethernet de 4 octets** (ou de passer en **JumboFrame**).

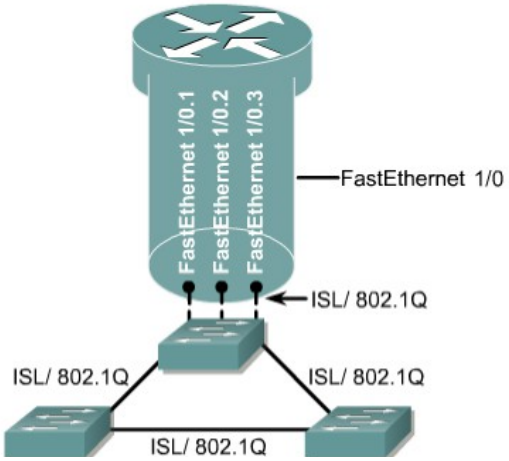
4 - Configuration des commutateurs



On commence par créer notre VLAN l le VLAN2 . A savoir : la VLAN 1 existe déjà, il s'agit du VLAN d'administration. Ensuite on va en mode de configuration de l'interface et on l'affecte à notre VLAN 2 sur lequel sera connecté le PC qui aurat comme passerelle la sous-interface VLAN 2 du routeur .

Dans ce cas le port numéro 2 du switch est assigné au VLAN 2.Dans notre exemple les ports qui relient les switch entre eux et le lien qui va du switch vers le routeur est appelé Trunk. Pour le configurer il faut aller en mode de configuration de ce port.

5 - Configuration d'un router on a stick



R1(config)#**interface fastethernet 0/1**
R1(config-if)#**no shutdown**
R1(config-if)#**interface fastethernet 0/1.1**
R1(config-subif)#**encapsulation dot1q 1**
R1(config-subif)#**ip address 172.17.1.1 255.255.255.0**
R1(config-if)#**interface fastethernet 0/1.11**
R1(config-subif)#**encapsulation dot1q 11**
R1(config-subif)#**ip address 172.17.11.1 255.255.255.0**
R1(config-if)#**interface fastethernet 0/1.30**
R1(config-subif)#**encapsulation dot1q 30**
R1(config-subif)#**ip address 172.17.30.1 255.255.255.0**
R1(config-if)#**interface fastethernet 0/1.99**
R1(config-subif)#**encapsulation dot1q 99 native** **-Solution 1-a et b**
R1(config-subif)#**ip address 172.17.99.1 255.255.255.0**

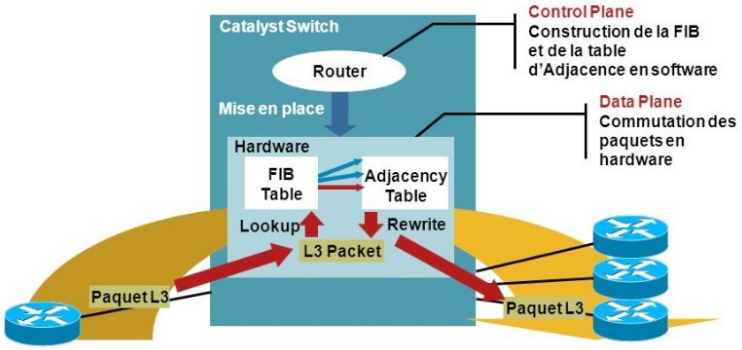
Le routeur permet la commutation entre les VLAN. L'interface Ethernet du routeur est connectée au trunk des commutateurs. Ainsi l'interface physique du routeur reçoit les paquets de plusieurs réseaux différents (chaque VLAN étant un réseau IP différent). Il est donc indispensable de créer des sous-interfaces à notre routeur, puis d'indiquer quelle sous-interface reçoit quel VLAN. On commence par indiquer au routeur que son interface Fa0/0 n'a plus d'existence physique avec le commande no ip address.

On passe en mode de configuration des sous-interfaces

L'interface physique est activée par la commande **no shutdown**, car les interfaces de routeur sont inactives par défaut. Les interfaces virtuelles deviennent actives par défaut.
· La sous-interface peut utiliser tout nombre en 32 bits mais il est conseillé d'affecter le numéro de VLAN au numéro d'interface pour une meilleure lecture et compréhension.

La commande encapsulation dot1q **1**, indique au routeur que la sous-interface va recevoir des parquets venant d'un lien trunk, et que ces parquets seront au format 802.1q et qu'ils appartiennent au **VLAN 1**.

6 – Les Switch de niveau 3



L'utilisation d'un switch de niveau 3 pour router les vlans permettra de profiter du fond de panier et donc un gain de temps pour le routage inter contrairement a la méthode router on a stick qui génère un goulot d'étranglement, une latence supérieur et point de rupture.

7 – CEF - Cisco Ewpress Forwarding

La technologie Cisco CEF est utilisée pour les switch de niveau 3.

Il peut être utilisé sur les routeurs et sur les switch de niveau 3

Il permet un routage beaucoup plus rapide tout en consommant moins de Temps CPU

Le routage se fait au niveau Hardware et non logiciel.

Il intègre 2 tables :

a. La table FIB – Forwarding Information Base
b. La table Adjacency

La FIB a le même utilité que la table de routage , elle contient l'adresse réseau ansi que le saut suivant.
Elle reprend la table de routage et les données sont rangées hiérarchiquement pour une optimisation maximal de routage.

La table Adjacency utilise des adresses de niveau 2 des interfaces voisines connectées.

La table FIB est remplie par l'intermédiaire de la table de routage RIB.

La table Adjacency se remplira en envoyant des requêtes ARP et contiendra donc les adresse MAC des voisins.

Pour router un paquet, le switch regarde dans sa FIB l'adresse réseau du voisin ou envoyer la trame, puis utilise la table d'adjacense pour connaître l'adresse MAC.

L'utilisation de CEF se voit inutilisée pour certains types de paquets qui utiliseront la table de routage classique,

Les paquets de type traceroute
les paquets de type tunneling : VPN
Les paquets dont l'encapsulation ne sera pas supportée
Les paquets dont la valeur TTL et égale a Zéro

CEF prend en charge tous les filtres de types ACL permettant ainsi une rapidité d'exécution de filtrage, puisqu'ils seront exécutés au niveau Hardware.

Activation de Cico Express Forward

SWITCH-SYNAPS(config)# ip cef

8 - Portage des VLAN via le trunk

2 type de portage

1 – a **Vous choisissez de porter tous les vlans sans filtre entre un routeur et le switch, et le vlan de gestion (vlan 99) qui sera porteur des protocoles (native)**

sur l'interface du switch connectée au routeur

```
com1#conf t
interface fast 0/1
switchport trunk vlan 99 native
switchport mode trunk
```

ou

1 – b **Vous utiliser un vlan de gestion et vous désirez ne porter que certains Vlan.**

```
interface FastEthernet0/3
switchport trunk native vlan 99
switchport trunk allowed vlan 11,30
switchport mode trunk
```

1-c **Vous désirez ne porter que certains vlan et pas le vlan de gestion**

```
switchport trunk allowed vlan 11,30
switchport mode trunk
```

Le DTP – Dynamic Trunking Protocol sa sert a quoi ?

Développer par Cisco, il permet de former un trunk dynamique sur une interface configurée en accès sur laquelle le mode DTP est activé.

L'idée étant de faire du **trunk plug en play**, un réseau de switch doit fonctionner dés que l'on connecte les équipements, cela expliquant pourquoi le DTP est activé par défaut.

Exemple

Une interface LAN d'un switch configurée dans un VLAN avec la commande

switchport access vlan 5

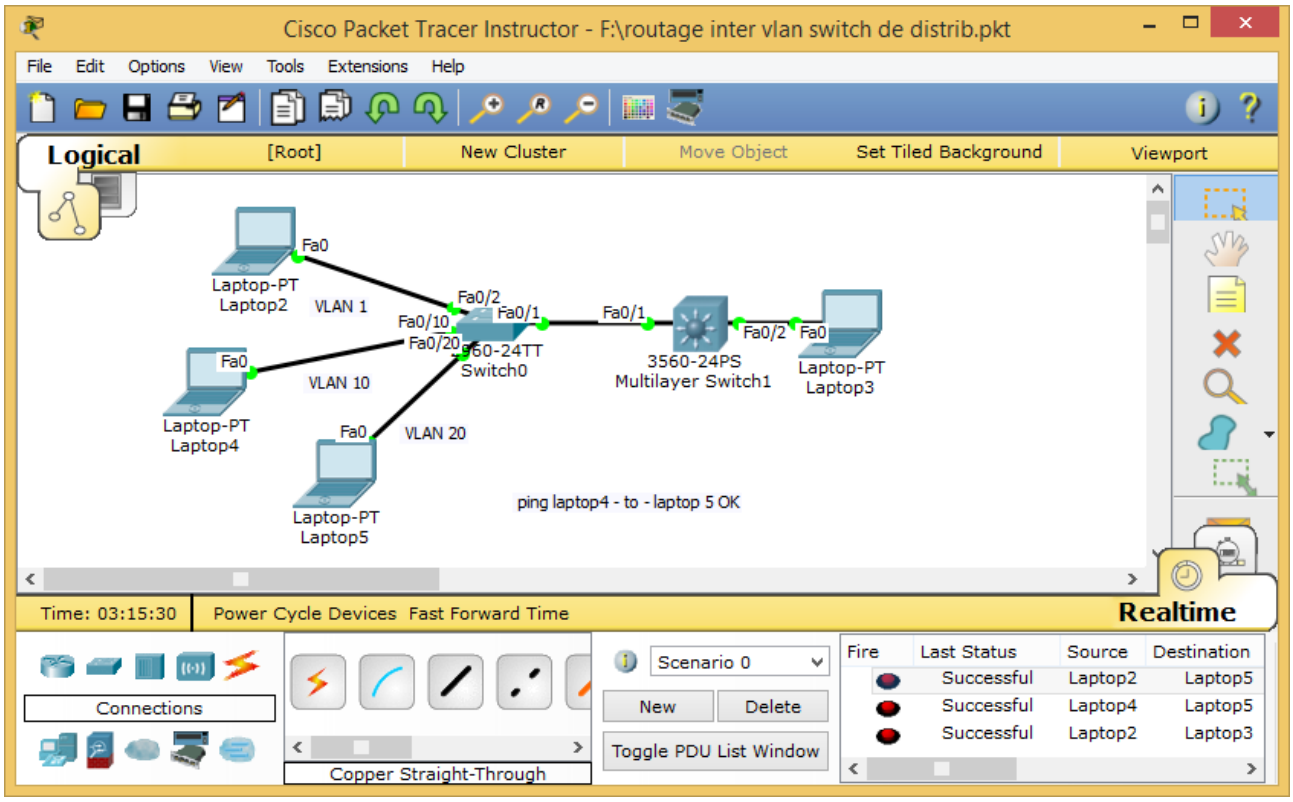
A l'aide d'un autre switch ou d'une application sur un pc vous passez l'interface réseau connectée au switch en mode TRUNK , via la commande switchport mode trunk

l'interface en **mode access** du premier switch qui appartient au VLAN5 passe automatiquement en mode TRUNK via le protocole **n-802.1q**

Le trunk par défaut laissant passer tous les vlans avec un Wireshark une capture permettra d'obtenir tous les paquets circulant sur le réseau.

La désactivation du DTP permet aussi un gain temps processeur puisqu'il n'y aura plus de phases de négociation.

ROUTAGE DE VLAN sur Switch Layer 3 - Switch de distribution



désactivation du mode DTP dynamique auto sur les switch de distribution pour mettre en place le mode trunk manuellement

1. désactiver le mode DTP sur tous les ports des switch avec un range

Sur un port access

switchport mode access

switchport nonegociate

Sur un port Trunk

switchport trunk encapsulation dot1q

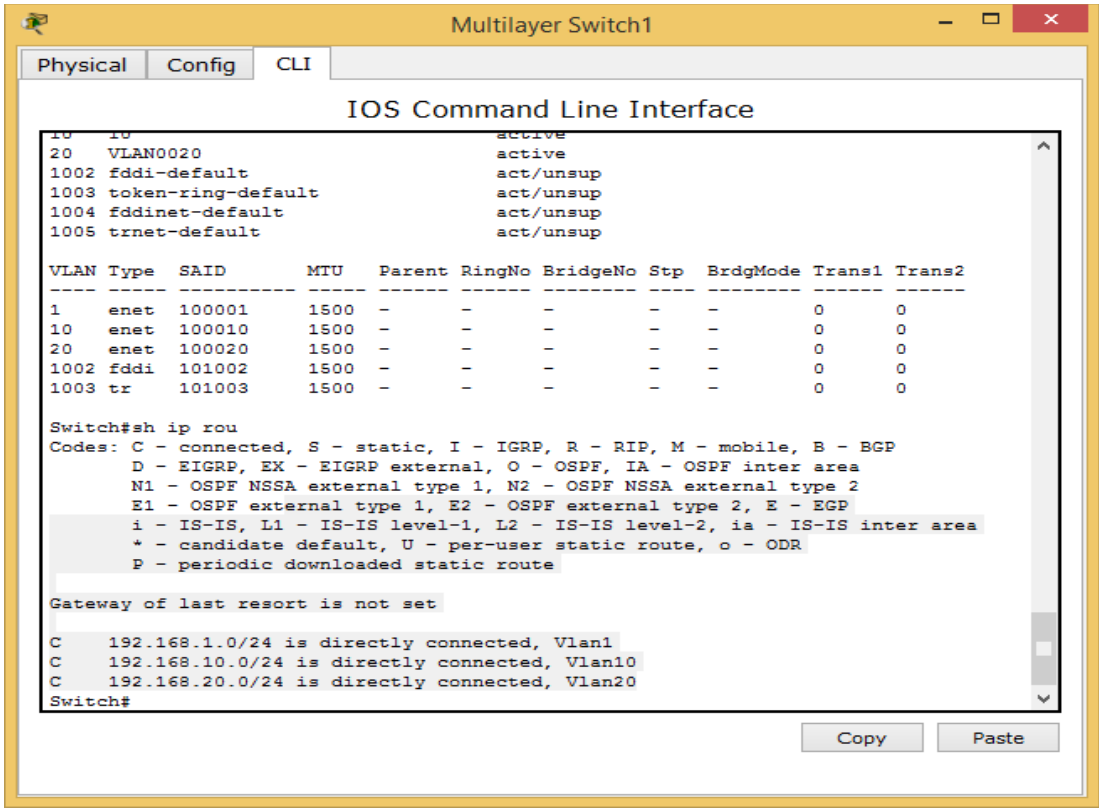
switchport mode trunk

switchport nonegotiate

2. configuration des port fast 0/1 en trunk sur les 2 switch - switch0 et switch1 via fast 0/1

interface fastethernet 0/1
switchport mode trunk
switchport trunk native vlan 10

Routage switch de distribution



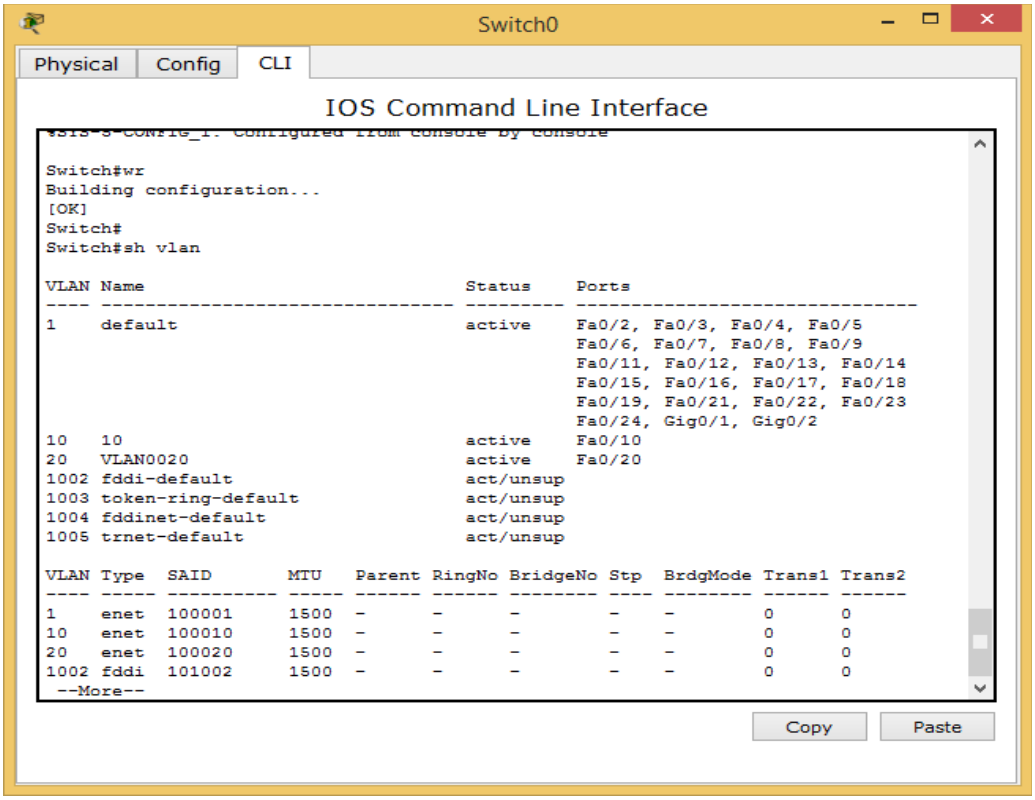
activer le routage sur le switch de distribution

ip routing

interface Vlan1
ip address 192.168.1.1 255.255.255.0
!
interface Vlan10
ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
ip address 192.168.20.1 255.255.255.0

interface FastEthernet0/1
switchport trunk native vlan 10
switchport mode trunk

configuration sur le switch d'accés



interface FastEthernet0/1

switchport trunk native vlan 10
switchport mode dynamic desirable

interface FastEthernet0/10

switchport access vlan 10
switchport mode access
!

interface FastEthernet0/20

switchport access vlan 20
switchport mode access

Service DHCP IPV4 sur Switch Layer 3 ou 2

Les switch 2960 Layer 2 ou 3650/3750 Layer peuvent devenir serveur DHCPV4 dans une architecture réseau LAN/MAN

Le switch server DHCP distribue et gère les adresses à partir de POOLS d'adresses qui seront liés aux VLAN par le bais des interfaces virtuelles - SVI (sub virtual interface) du switch .

Le 2960 comme le 3650 ou 3750 Layer 3 permettent de router les VLANs et d'insérer des routes statiques.

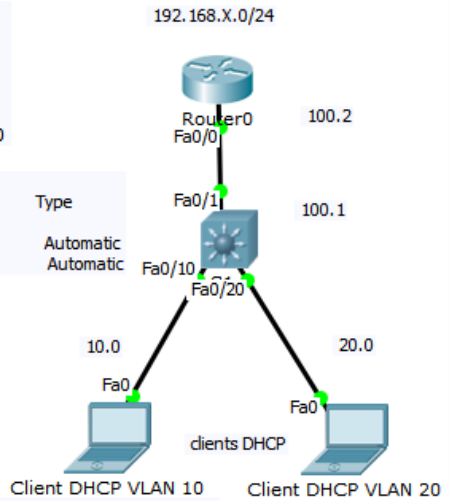
Le schéma ci-dessous met en place un serveur DHCPv4 sur un switch Layer 3 avec 2 pools d'adresses 10.0 et 20.0, correspondant respectivement au VLAN10 et VLAN20, les 2 pc connectés sur les ports 0/10 et 0/20 affecté au VLAN10 et VLAN20 se verront attribués les adresses ip du pool appartenant au VLAN concerné.

Une route statique par défaut permettra de guider les packets dont les réseaux ne sont pas connus vers le routeur coté internet.

Il nous est possible de remplacer le switch de distribution par un switch d'accès en utilisant le template « SDM prefer lanbase-routing »

```
interface FastEthernet0/0
 ip address 192.168.100.2 255.255.255.0
 duplex auto
 speed auto
!
ip classless
ip route 192.168.0.0 255.255.0.0 FastEthernet0/0
```

```
Switch>sh ip dhcp binding
IP address      Client-ID/          Lease expiration        Type
                Hardware address
192.168.10.11   0050.0F35.6959      --                      Automatic
192.168.20.11   0005.5E9B.6DD8      --                      Automatic
```




```
hostname Switch
!
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.20.1 192.168.20.10
!
ip dhcp pool DHCPV10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.10.3
ip dhcp pool DHCPV20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 192.168.20.3
!
ip routing
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 no switchport
 ip address 192.168.100.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1
```

```
PC>ipconfig /?
Packet Tracer PC IP Configuration

Usage:
ipconfig { /? | /renew | /release | <IP> <subnet mask> [<default gateway>] }

PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::250:FFF:FE35:6959
   IP Address.....: 192.168.10.11
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.10.1
```

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::205:5EFF:FE9B:6DD8
   IP Address.....: 192.168.20.11
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.20.1
```