VLAN

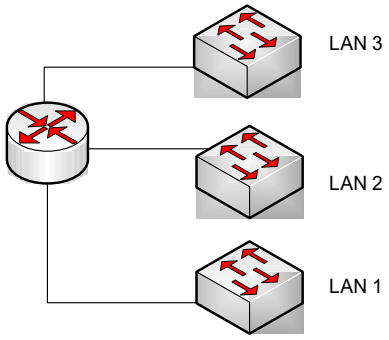
Présentation

VLAN - Virtual Area Network

Les vlan permettent de segmenter les utilisateurs par un **regroupement logique**, indépendemment des contraintes géographiques.

Segmentation sans VLAN

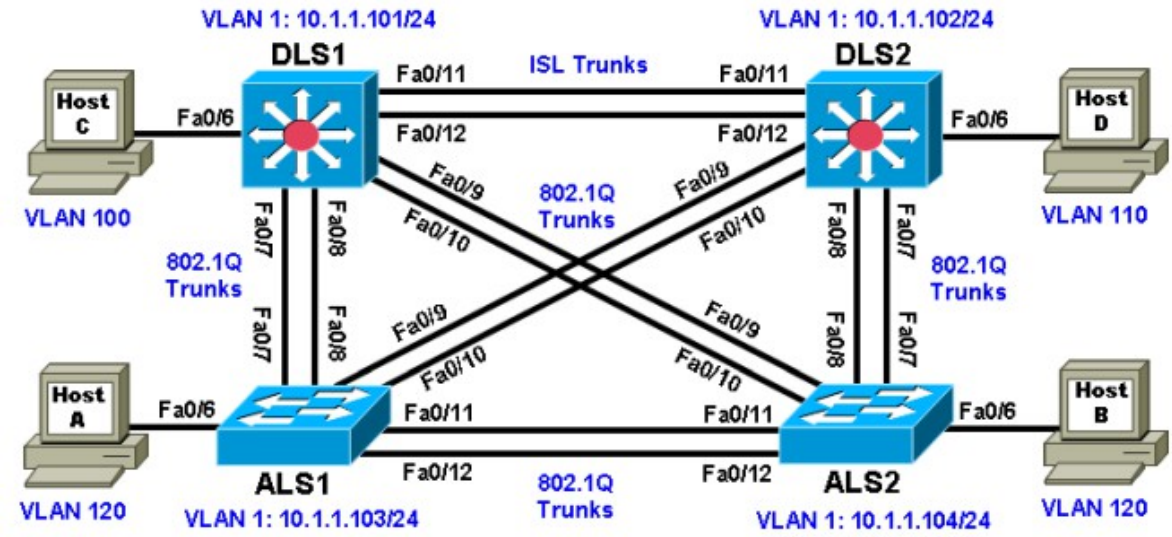
Une interface de routeur par sous-réseau/switch
le routeur permet la segmentation des domaines de broadcast IP



Segmentation par VLAN dans une architecture access/distrib

Architecture Full liens redondants, Full trunk avec 5 liens 802,1q et 1 lien ISL, chaque switch sera administrable par le Vlan 1 – vlan par défaut dit MGMT- management via l'adresse ip posé sur la SVI (switch virtual interface- permettra le traitement de couche 3 pour tous les paquets des port attachés a ce vlan) VLAN 1 de chacun, le routage inter vlan se fera via les Layers 3 DLS1 et DLS2, le spanning-tree permettant de définir DLS1 connecté a internet 1, comme lien actif de tous les ports reliés de ALS1 et ALS2, DLS2 connecté a internet 2 étant le passif

internet 1 **internet 2**



Avantage d'utiliser des VLAN

Gestion des broadcast IP/ARP par VLAN :

Tous les paquets ip du vlan et notamment les broadcast ip et mac seront maintenus dans ce vlan aux frontières du router/switch layer 3 qui bloquera tous les broadcast a l'interface sur lequel est connecté fastethernet/SVI Vlan

Migrations des utilisateurs :

un utilisateur pourra migrer d'un switch a un autre en se connectant sur un port attaché a son Vlan

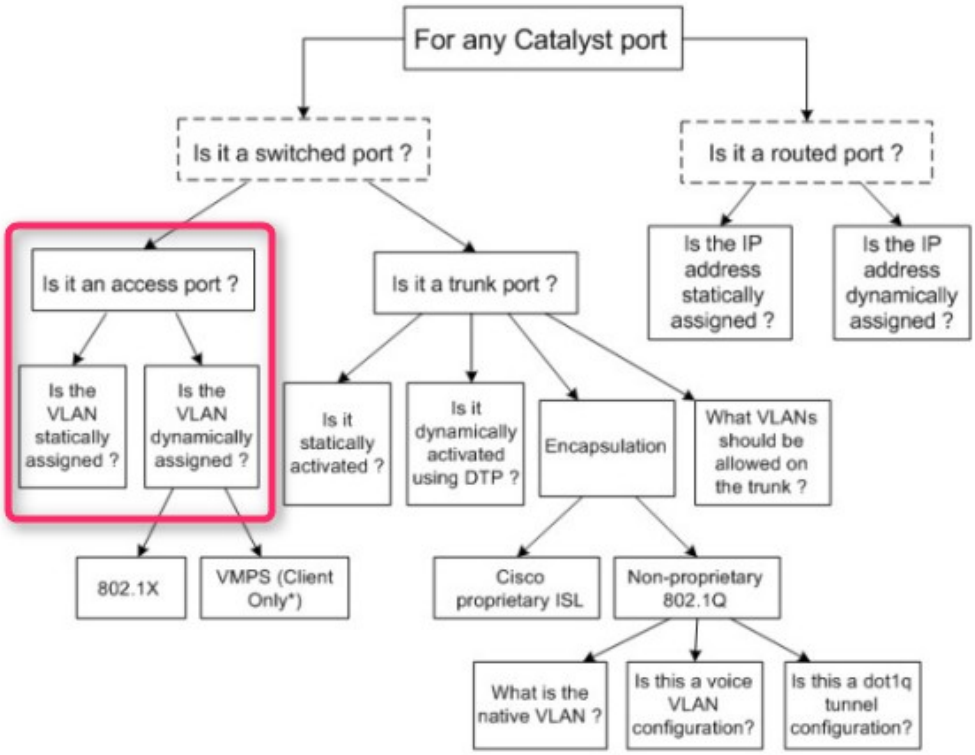
Création de VLAN Voice :

utilisation du vlan voix sur tous les ports

Sécurité

l'accès d'un vlan a un autre pourra se filtrer via DLS1 et DLS2 en utilisant des ACL sur les SVI

Implémentation des VLANs



Les 2 affectations d'un port a un vlan se font soit en **statique** soit en **dynamique** (très peu utilisé)

- **Statique, affectation du vlan directement au port**
- **Dynamique**

1 802.1x, par **authentification utilisateur** via un server ACS -acces control system- radius ou tacacs , et affectation du vlan au port

2 Utilisation d'un serveur VMPS VLAN Membership Policy Server (cisco) Blade server

- la Base de donnée sur le server contiendra l'**assignation d'un port à un vlan en fonction de l'adresse MAC** (switchport access dynamic)**,**suivant l'authentification MAC le client sera positionné dans un vlan

Les différents types de VLAN

VLAN par default :

le vlan 1, celui dans lequel sont mis tous les ports par défaut

VLAN natif :

Les trames du vlan natif ne sont pas taguées en 802,1q afin d'assurer l'inter-opérabilités avec les matériels ne supportant pas le tagging. C'est par ce VLAN que transitent les protocoles de contrôles le CDP, VTP, Pagp et Lacp (etherchannel) et DTP, Spanning-tree (rstp-pvst), tous les protocoles de Layer 2 utilisés par les swicth, **par défaut c'est le VLAN 1**.

VLAN utilisateur : VLANs classiques, mode access

VLAN de gestion ou d'administration des équipements :

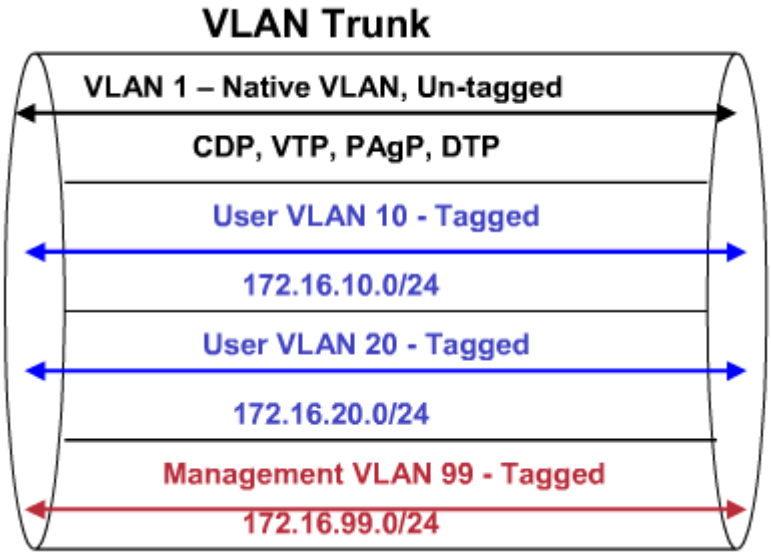
Un réseau local virtuel de gestion est un vlan que vous configurez pour accéder aux fonctions de gestion d'un commutateur. Le VLAN 1 configuré par défaut fait office de vlan de gestion, Il faut affecter une adresse ip et un masque de sous-réseau. Un commutateur peut être géré via HTTP/HTTPS, telnet, ssh, ou snmp. N'utiliser pas le vlan1 comme vlan de gestion.

Configurer une interface de gestion sur chaque commutateur dans le même vlan.
Par sécurité on crée un autre réseau local VLAN 99 ou de votre choix que l'on affecte a un port par lequel on connectera le PC pour l'administration

Il n'ai pas possible de supprimer le vlan 1, mais vous pouvez créer un vlan dit « tampon » dans lequel vous poser toutes vos interfaces non utilisées et désactivez l'interface VLAN 1 en faisant un « shutdown ».

Les VLANs portés via un port TRUNK/dot1q/802,1q

Principe de fonctionnement des liens Trunks entre tous les switchs pour porter les Vlans



Mise en place de l'adresse IP sur l'interface vlan 99

```
Configure terminal
interface vlan99
ip address 172.17.99.11 255.255.255.0
no shutdown
end
```

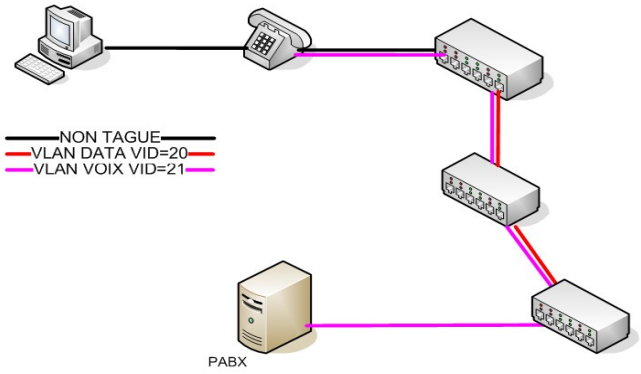
Le port fast 0/18 appartient au vlan 99

```
configure terminal
interface fastethernet 0/18
switchport mode access vlan 99
end
```

Cette configuration IP est a faire sur chaque commutateur avec une adresse ip différente mais dans le même réseau ou sous-réseau, dans ce cas on configurera un des ports de DLS1 le 18 par exemple pour appartenance et branché le Pc d'administration a partir duquel on pourra ouvrir des connexion telnet/ssh sur tous les switch via leur adresse ip.
Une autre solution sera possible via une connexion câble console a partir d'un PC sur un switch en utilisant un terminal/putty, et faire un telnet/ssh sur tous les autres swicth a partir du terminal.

VLAN de auxiliaire :

Avec l'arrivée de la VOIP il existe un mode « auxiliaire » entre le mode ACCESS et le mode TRUNK, il permet de préciser sur un port en mode access, un VLAN supplémentaire spécifique pour la voix, c'est utilisé dans le cas ou la machine est reliée au téléphone IP qui relais les données du pc plus ses trames VOIP vers le switch, dans ce cas le VLAN voix est appelé VLAN auxiliaire, il sera tagué par le téléphone et sera totalement transparent pour la machine connectée derrière.



Les VLANs et leur numérotation

VLAN 1 : le VLAN natif par défaut

VLAN 1 à 1001 sont les vlan standards enregistré dans le fichier VLAN.DAT sur la mémoire FLASH (VLAN database)

VLANs 1002 à 1005 : VLAN réservés pour FDDI et TOKEN RING ils sont créés automatiquement et on ne peux les supprimés.

Sur un switch configuré en mode transparent utilisant une version d'IOS « Enhanced » il,est possible de créer des VLANs étendus, 1006 à 4096.

Les Vlan's les plus courant

```
vlan 10
name OFFICE
!
vlan 20
name VOICE              //vlan voix
!
vlan 30
name GUEST              //vlan invités
!
vlan 50
name SERVERS            //vlan server
!
vlan 100                //vlan de management
name MGMT
!
vlan 200                //vlan de transfert firewall / routeur
name TRANS
!
vlan 900
name NATIVE             //porter les protocoles
!
vlan 999                //vlan tampon
name UNUSED
```

Les 3 mode des interfaces Fastethernet des Switchs

1.Mode Trunk

-Le trunk, il permet de porter les vlan entre les switch (ISL propriétaire cisco / 802.1Q)

```
Comm1(config)#interface range fa0/1-4
Comm1(config-if-range)#switchport mode trunk
Comm1(config-if-range)#switchport trunk native vlan 99
Comm1(config-if-range)#no shutdown
Comm1(config-if-range)#end
```

2.Mode d'accès

-assignation des ports en mode d'accès et affectation au vlan côté PC clients

```
interface FastEthernet0/5
switchport access vlan 30
switchport mode access
```

3.Mode dynamique

Négociation dynamique du mode des ports, mode d'accès ou trunk utilise le protocole **DTP Dynamique trunking** protocole

```
conf t
interface fastethernet 0/1
switchport mode dynamic
```

Création de vlan

```
sur un switch
conf t / vlan 2 / name fab

sur un router intégrant une carte switch

vlan database / vlan 2 name fab
interfast fastethernet0/2 / switchport mode access / swittchport access vlan fab
```

Voir les vlans

```
show vlan
show vlan id numéro-vlan  //pour identifier les ports affectés
```

Effacement des configurations d'un switch

a/Effacer le fichier de configuration en mémoire flash

```
erase startup-config
```

b/Effacer les Vlan

```
Détacher les ports affectés aux différents vlans, les repositionner dans le vlan 1

Faire un no vlan all
ou
delete flash:vlan.dat
puis reloader et vérifier en faisant un show vlan
```

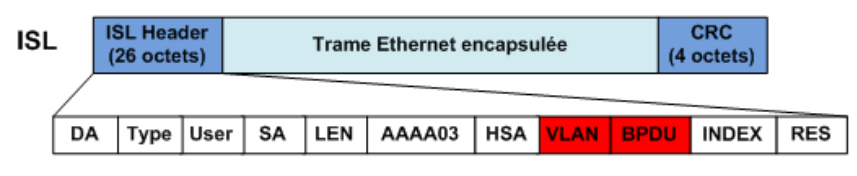
Routage inter-vlan

Il existe 2 types de tunking

ISL Inter Switch Link	802.1Q
Propriétaire	Normalisé
Encapsulation	Tag
Indépendant du niveau 2	Dépend du protocole Ethernet
Encapsule l'ancienne trame dans une nouvelle	Ajoute un champ dans l'entête de la trame initiale

1. 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**, il est utilisé que sur des liens point à point.



2. Le protocole 802.1 Q ou Dot1q

Ce protocole n'est utilisé que sur les **liens point à point (point to point).**

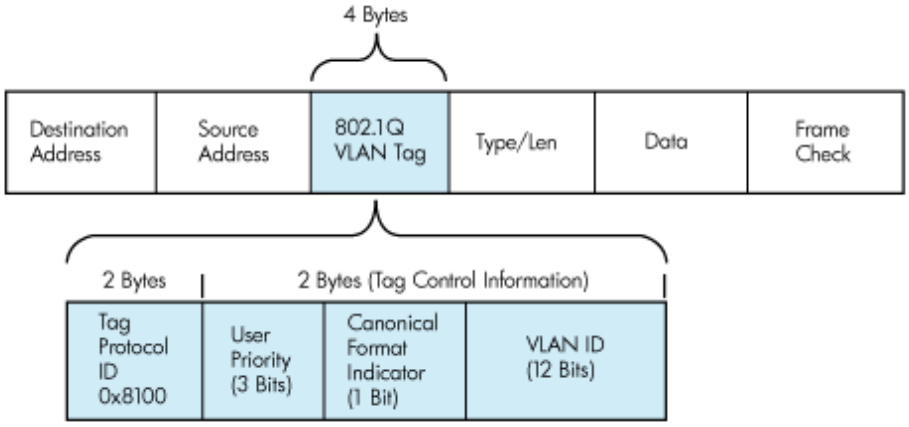
Étiquetage de trame normalisée par l'IEEE. Insertion d'un champ de 4 octet dans la trame Ethernet pour identifier les vlan (le tagging)

-16 bits pour le **champs ethertype/type de trame** – Code Trunk **0x8100 = Dot1q/802,1q**

- 3 bits pour la **priorité du Vlan**

- 1 bit pour identifier un réseau token-ring,

- **12 bits pour le VLAN ID** (soit **4096 possibilités**).



Configuration du routage inter vlan via un router appelé - router on a stick

Création de sous interfaces sur le routeur et mise en place du trunk (dot1q)

```
R1(config)#interface fastethernet 0/1
R1(config-if)#no shutdown                          //activer
R1(config-if)#interface fastethernet 0/1.1         //les sous-interfaces sont activées par défaut
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 172.17.1.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.10        //sous-interface 0.10 on affetce le numéro de
                                                   //vlan a la sous-interfaces par defaut pour une
                                                   //meilleur compréhension et lecture
R1(config-subif)#encapsulation dot1q 10            //activation du trunk et affectation de la
                                                   //sous-interface au vlan10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-if)#interface fastethernet 0/1.99
R1(config-subif)#encapsulation dot1q 99 native     //appartenance de la sous-interface
                                                   //au vlan 99, vlan de gestion (native)
R1(config-subif)#ip address 172.17.99.1 255.255.255.0
```

Protocole VTP - Virtual trunking protocol

Permet de centraliser la création de vlan sur un switch de distribution par exemple et de les exporter automatiquement sur les autres switch, mais n'affecte pas les ports au vlan.

3 modes :

- Serveur
- Client
- Transparent

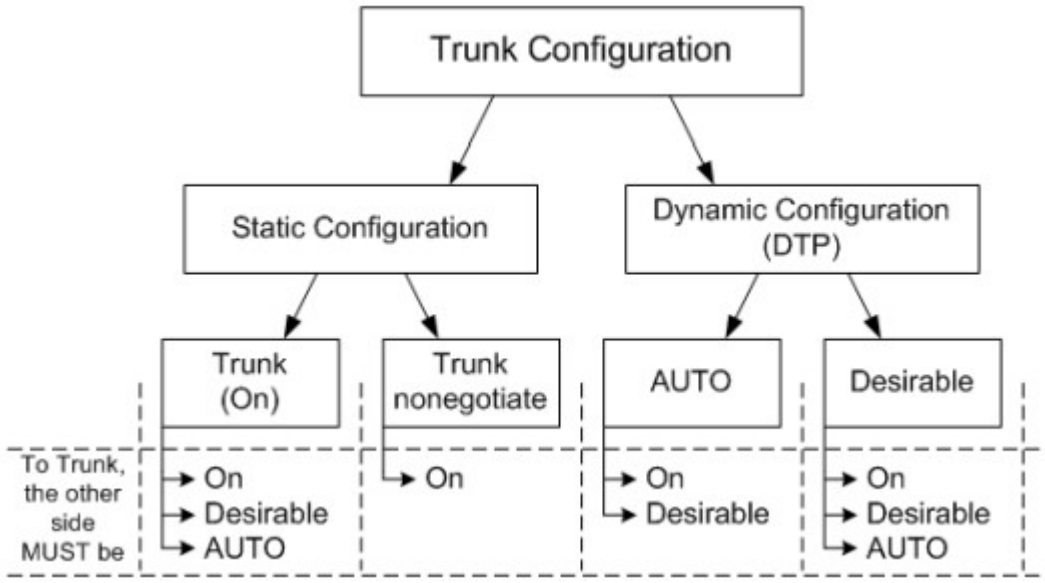
Configuration de VTP

vtp domain nom_domaine
vtp mode server
vtp password passwd
Par défaut les switch sont en mode serveur

vérification

show vtp status

DTP – protocole Dynamic trunking protocol



Désactiver le mode dynamique : int range fast 0/1-4 – no switchport mode dynamic – switchport nonegotiate – switchport mode trunk – switchport trunk native vlan 56

Dynamic Trunking Protocol permet à un port de dialoguer avec le port d'en face dans le but de passer en mode trunk ou non.

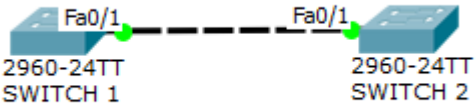
- `switchport nonegociate` ne négocie pas le trunk ; la commande n'est accessible que sur un port configuré en mode access ou trunk.
- `switchport mode dynamic {auto | desirable}`. Active l'auto configuration du port :
  - mode **desirable** : négocie activement pour passer le lien en trunk ; il passe donc en mode trunk face à un port configuré en trunk, desirable ou en auto. C'est le mode par défaut.
  - mode **auto** : négocie passivement le lien en trunk (= il répond juste aux sollicitations qu'il reçoit); il passe en trunk uniquement face à un port configuré en mode trunk ou desirable.

Si rien n'est spécifié c'est une faille potentielle (VLAN hopping) quand c'est sur un port relié à une machine utilisateur (ce dernier peut se faire passer pour un switch, forcer en mode trunk, et faire passer tous les VLANs dessus).

Synthèse des interactions

	Dynamic auto	Dynamic desirable	Trunk	Access
Dynamic auto	access	trunk	trunk	access
Dynamic desirable	trunk	trunk	trunk	access
Trunk	trunk	trunk	trunk	déconseillé
Access	access	access	déconseillé	access

Exemple mode DTP




```
SWITCH1#sh interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

```
SWITCH2#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

On voit que le port est configuré en mode dynamique automatique

	Dynamic auto	Dynamic desirable	Trunk	Access
Dynamic auto	access	trunk	trunk	access
Dynamic desirable	trunk	trunk	trunk	access
Trunk	trunk	trunk	trunk	déconseillé
Access	access	access	déconseillé	access

On passe le port du SWITCH 2 en mode TRUNK

```
SWITCH2(config)#interface fas
SWITCH2(config)#interface fastEthernet 0/1
SWITCH2(config-if)#swi
SWITCH2(config-if)#switchport mo
SWITCH2(config-if)#switchport mode tr
SWITCH2(config-if)#switchport mode trunk

SWITCH2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
```

le switch1 passe automatiquement en mode trunk

```
SWITCH1#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
```

```
SWITCH1#sh interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

```
SWITCH2#show int fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

Sur le switch 1 le port 1 reste en mode 'dynamique auto' , la négociation du trunk est 'ON' , le vlan natif est le vlan 1, tous les vlan sont portés par le trunk

Sur le switch 2 le port est en 'mode trunk' , vlan 1 est le vlan natif est tous les vlan sont portés

Visualisation des interfaces trunk, « mode on » pour le trunk sur switch 2 et mode auto DTP pour switch 1

```
SWITCH2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
```

```
SWITCH1#sh interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
```

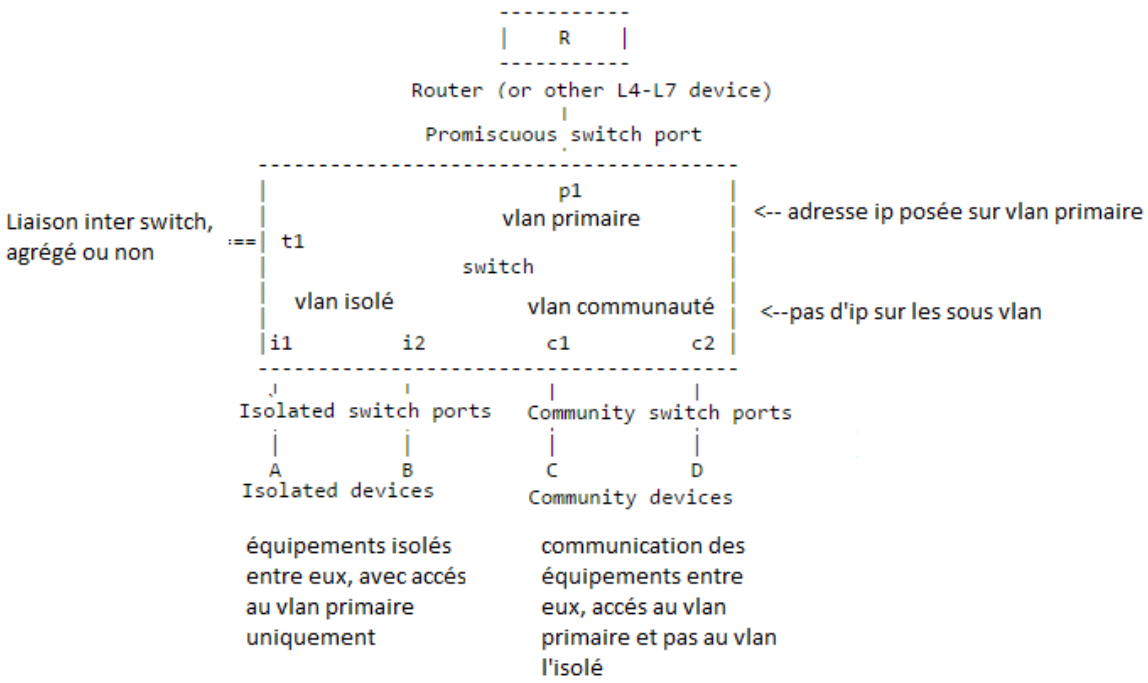
Les privates Vlan

fonctionnement d'uns infrastructure de private VLAN

Le Private Vlan est composé :

Vlan primaire – promiscuous : contenant les « promiscuous ports »
Vlan secondaires : isolated ou community – contenant le « host ports »

Les différents VLAN sont dans le même sous-réseau IP , seul de VLAN primaire possédera une interface de niveau 3 , ou passerelle par défaut de tous les équipements appartenant aux autres VLAN isolated / community



Utilisation des 3 types de VLAN

le Vlan primaire ou promiscuous :

un équipement ds ce vlan peut communiquer avec tous les autres Vlans au sein du private Vlan, on retrouvera les routers ou firewalls ou autre services mutualisés

le vlan isolated

séparé au niveau 2 table CAM, les machines ne peuvent communiquer entrent elles, idem pour les broadcast, les seules communication se font vers le vlan primaire

le vlan community

les machines au sein de la même communauté peuvent communiquer entre elles et vers le vlan primaire, les machines d'une communauté ne pourront pas communiquer avec les machines des autres communautés ou avec des vlan isolated

Le private vlan est actif sur le port du switch, ce qui entraîne que les utilisateurs doivent être sur des ports différents pour être isolés, dans le cas ou on a un point d'accès connecté a un port isolé ça n'isolera pas les utilisateurs connectés sur le point d'accès, ni dans le cas de raccord d'un switchA sur le port isolé du swicth, les utilisateurs connectés sur le swicthA ne seront pas isolés

Exemple

la zone des « invités »
Dans une société nous décidons d'isoler les invités d'une salle de réunion de notre réseau, pour la réalisation de cette isolation , nous mettrons les clients dans un **vlan isolated** afin qu'il puisse avoir accès a internet suivant les règles du firewall et qu'il ne puisse pas communiquer ensemble, et on mettra le pare feu dans le **vlan primary**

Résumé des commandes

Command	Description
vlan *vlan-id*	creates a VLAN
name *vlan-name*	names a VLAN
show vlan	shows vlan information
shutdown	disables an interface
no shutdown	enables an interface
vtp mode [client | server | transparent]	sets VTP mode
show vtp status	shows vtp configuration
switchport access vlan *vlan-id*	assigns the default VLAN for a port
switchport mode access	assigns an access port
switchport mode trunk	assigns a trunk port
switchport nonegotiate	disables DTP
switchport trunk allowed vlan remove *vlan-list*	removes VLANs from a trunk port
switchport trunk encapsulation dot1q	configures trunk for 802.1Q encapsulation
switchport trunk encapsulation isl	configures trunk for ISL encapsulation
switchport trunk allowed vlan	Allow VLANS to be carried by trunk, 1, 1002-1005 required
vlan database	Enters vlan database configuration mode
vtp domain *domain-name*	Assigns the domain name for VTP
vtp mode [client | server | transparent]	Configures the VTP mode
show interfaces *interface-id* **switchport**	shows the switchport configuration
ping *ip-address*	sends an ICMP echo request