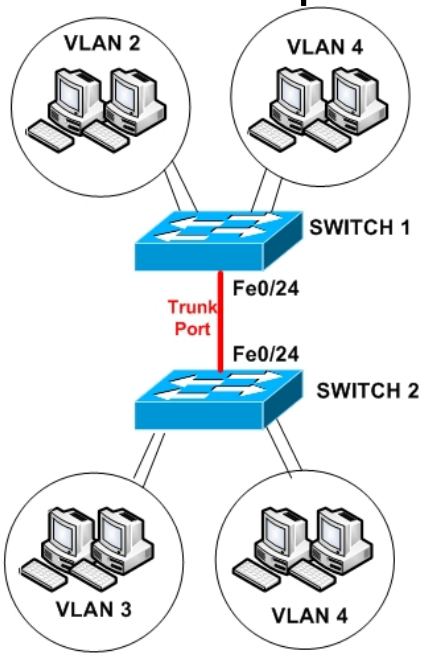
12- La commutation dans les LANs

- Equipement:
  - commutateur (**Switch**)

    (concentrateur ou **HUB**: Host Unit Broadcast, pas de commutation mais de la diffusion du signal d'entrée vers tous les autres ports)



12- La commutation dans les LANs

- Commutation:
  - Issue de la **téléphonie** et des réseaux **WAN**
  - Mise en œuvre dans Ethernet (**Switched Ethernet**)
  - **Pour résoudre les problèmes d'effondrement des réseaux**
  - Pour **garantir une certaine bande passante**
  - Traditionnellement, **mettre en relation directe un port d'entrée avec un port de sortie** (relation établie préalablement à toute communication par un protocole de signalisation)

12- La commutation dans les LANs

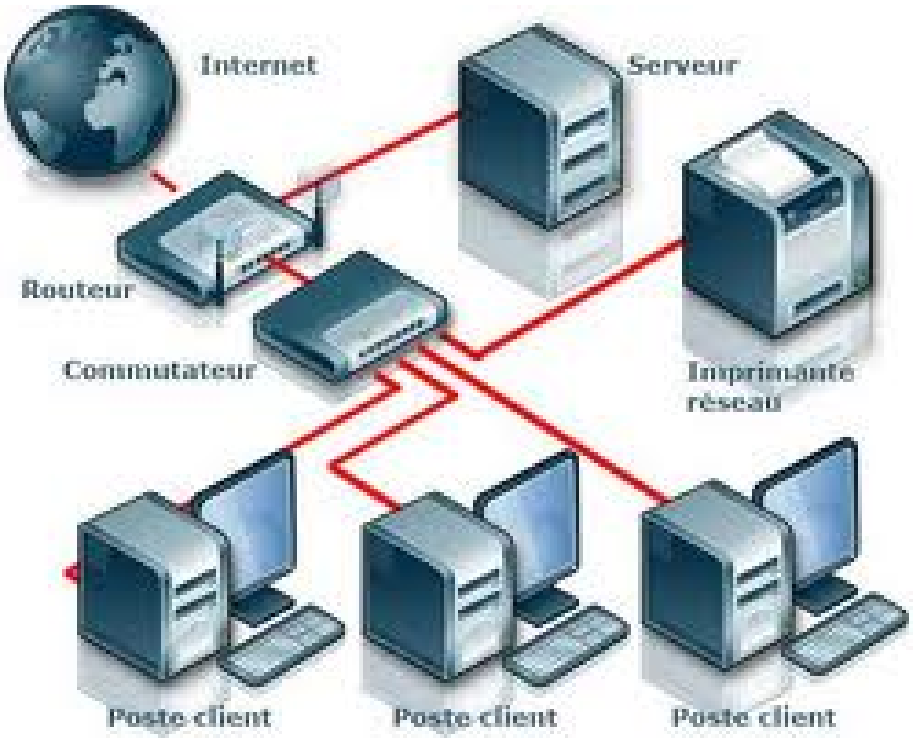
- **Table de commutation**:
  - **FDB**: Forwarding Data Base
  - **Statique:** remplie par l'administrateur, rare
  - **dynamiquement**: par examen des adresses MAC, localisation géographique des stations
- **Buffers** :
  - des ports d'entrées
  - des ports de sorties
- **Architecture**:
  - **Bus de fond de panier**:
    - collapsed Bacbone
    - très haut débit
    - au moins égal à la demi-somme des débits incidents
  - Ou **Mémoire partagée** à accès multiples simultanées
    - **La plus courante**

Host MAC Address	Port
00 00 80 45 FE 21	5
00 00 80 45 DA 47	3
00 40 00 80 45 FE	2
00 40 80 10 AA 21	1
00 00 80 00 FF AB	5

12- La commutation dans les LANs

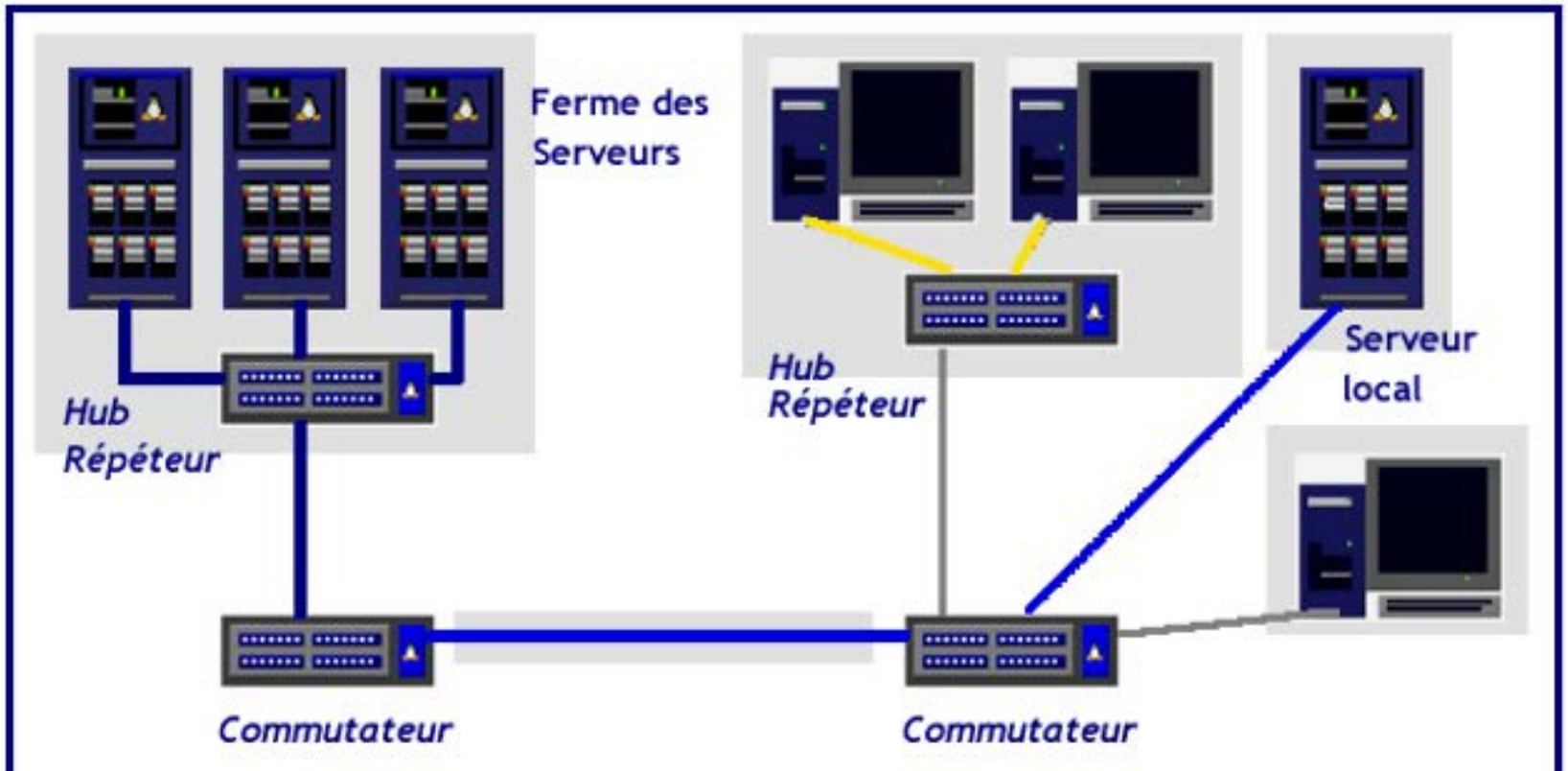
- **Différents modes** de commutation:

- Commutation **par port**:
- une station derrière un port



12- La commutation dans les LANs

- Commutation **par segment**:
  - **plusieurs stations derrière un port du switch**: c'est un segment



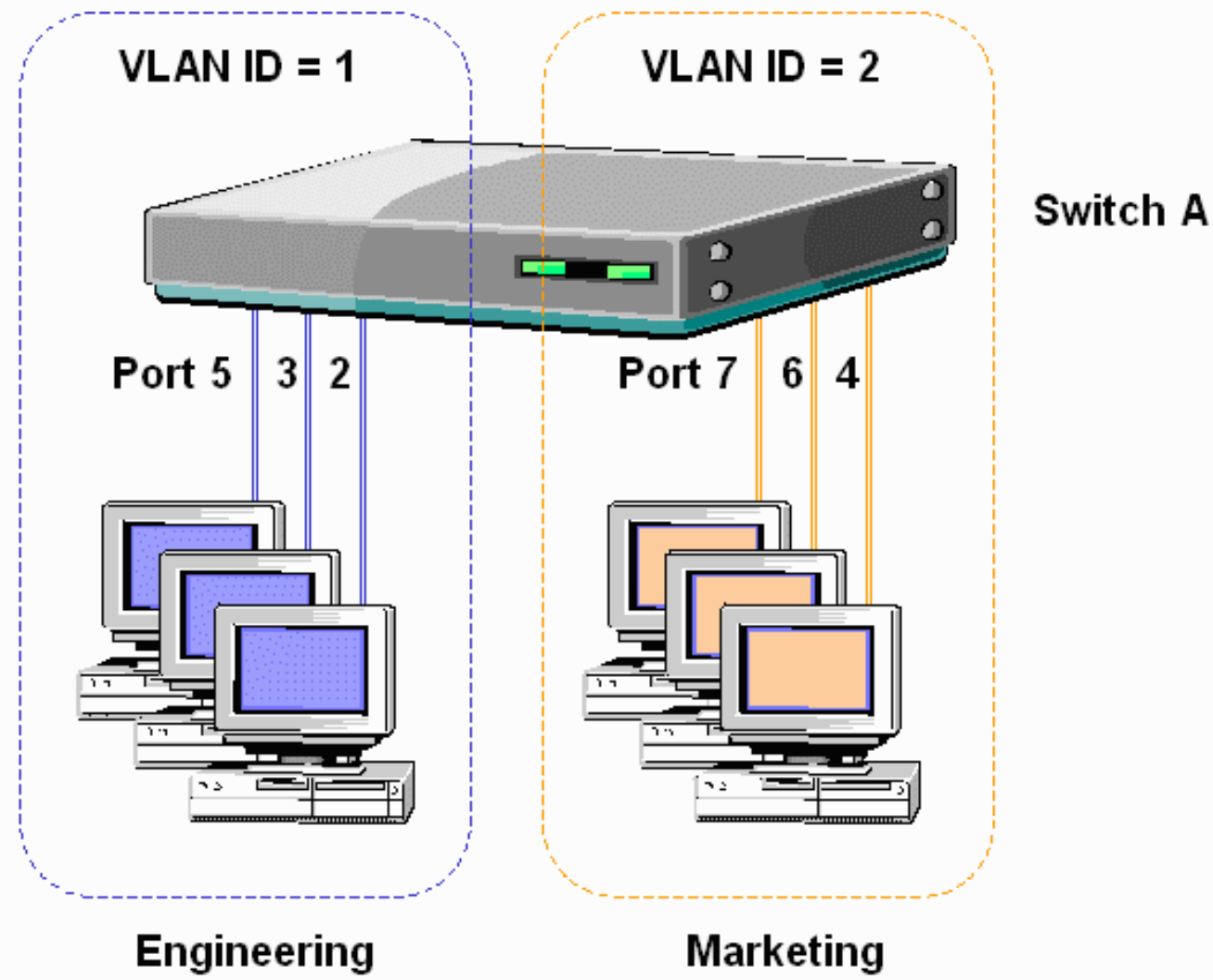
12- La commutation dans les LANs

- **Trois techniques:**
  - **1- Lecture de l'adresse destination au vol**:
    - Commutation à la volée (**cut and trougth**)
    - Commutation **rapide** (fast forward)
    - Technique **performante** en terme de nombre de trames commutées par seconde (**faible temps de latence**)
    - **Propage les trames erronées** (collisions)
  - **2- Stockage avant retransmission**:
    - **Store and forward**
    - **Contrôle** des trames
    - **Commutation** uniquement des **trames valides**
    - **Délai** de commutation
    - **Processeur rapide** pour **réduire le délai**
  - **3- Combinaison des deux techniques**:
    - **Retransmission** d'une trame **après avoir reçu** les **64 premiers octets** (augmentation de la durée d'une fenêtre de collision)

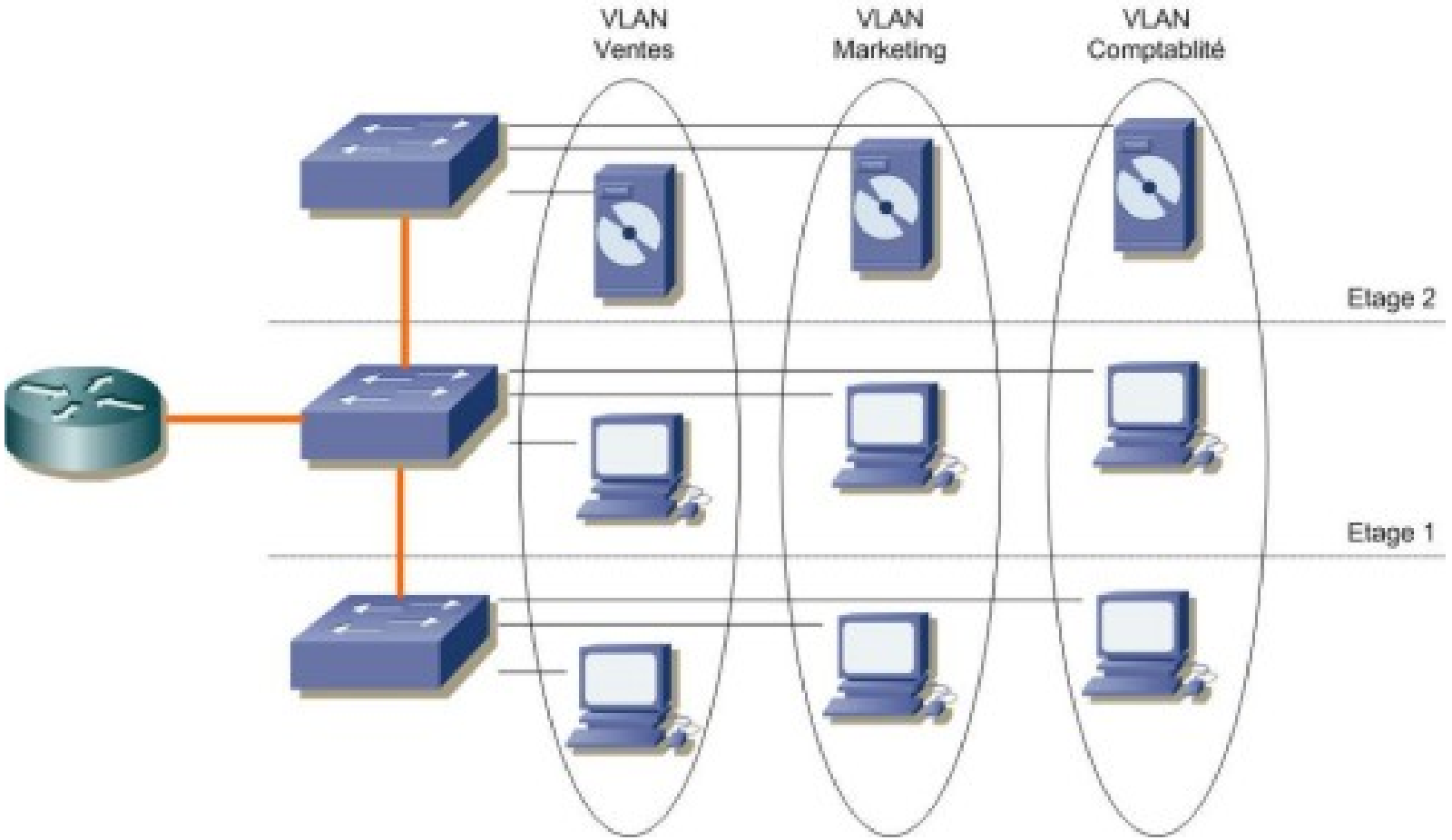
13- Les réseaux virtuels

- **VLAN**: Virtual Local Area Network
- **Plusieurs réseaux logiques** indépendants sur **un même réseau physique** selon des critères prédéfinis (ports, adresse MAC, adresse IP, protocole,…)
- **Segmentation virtuelle**
- **Communication** autorisée **entre machines d'un même Vlan**
- Communication **inter-Vlan**: passer par un **routeur ou un commutateur de niveau 3 (commutateur routeur).**
- Réaliser des réseaux **axés sur l'organisation de l'entreprise**
- **Domaine de diffusion indépendamment de la situation géographique** des systèmes
- Assurer la **mobilité des postes de travail** (déplacement)
- **Répartition** et **partage optimale des ressources**
- **Un logiciel d'administration** permet d'affecter chaque système raccordé au commutateur à un réseau logique d'appartenance
- **Affectation manuelle** ou **automatique**

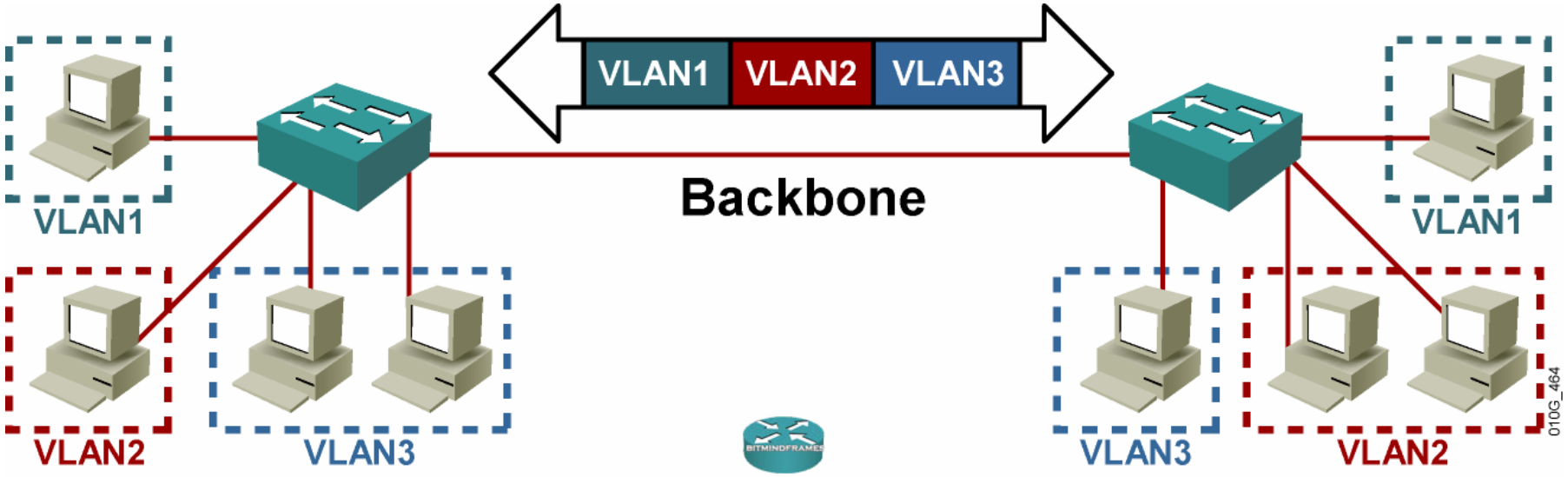
13- Les réseaux virtuels



13- Les réseaux virtuels



13- Les réseaux virtuels



13- Les réseaux virtuels

- **différents niveaux** de VLAN:

- **VLAN de niveau 1**:

  - VLAN par **port**
  - **Port Based** VLAN
  - Regroupe **les stations connectées à un même port** du commutateur
  - **Configuration statique**:
  - Le **déplacement d'une station** implique son **changement de VLAN**
  - **Un port peut appartenir à plusieurs VLAN** (donc les stations qui lui sont raccordées)
  - Mode **sécurisé**, un utilisateur ne peut déplacer sa machine

13- Les réseaux virtuels

- **VLAN de niveau 2**:
  - **VLAN MAC**
  - Associe les stations par leur adresses MAC
  - **MAC Address-Based VLAN**
  - de ce fait **deux stations raccordées à un même port** (sur le même segment) **peuvent appartenir à deux VLAN différents**
  - **Table de commutation remplie par l'administrateur** : déplacement et regroupement de stations dans le logiciel d'administration (Drag and Drop)
  - **Une station peut appartenir à plusieurs VLAN**
  - **Indépendants des protocoles de niveau supérieur**
  - Commutation **rapide**

13- Les réseaux virtuels

- **VLAN de niveau 3**:
  - **VLAN d'adresse réseau**
  - **Network Address-Based** VLAN
  - Constitué de stations définies par leur adresse réseau
  - **Plage d'adresses** ou par **masque de sous-réseau** (Subnet IP)
  - **Utilisateurs affectés dynamiquement** à un VLAN
  - **Une station** peut appartenir à **plusieurs VLAN** par **affectation statique**
  - Mode de fonctionnement le **moins performant**, le commutateur devant accéder à l'adresse de niveau 3 pour identifier le VLAN d'appartenance. **Adresse réseau** utilisée comme **étiquette**, il s'agit de **commutation et non de routage**, l'entête n'est pas modifiée

13- Les réseaux virtuels

- Possible de **réaliser des VLAN** par:

- **Protocole**:
  - communication uniquement entre stations utilisant le même protocole
- **Application**:
  - Numéro de port TCP

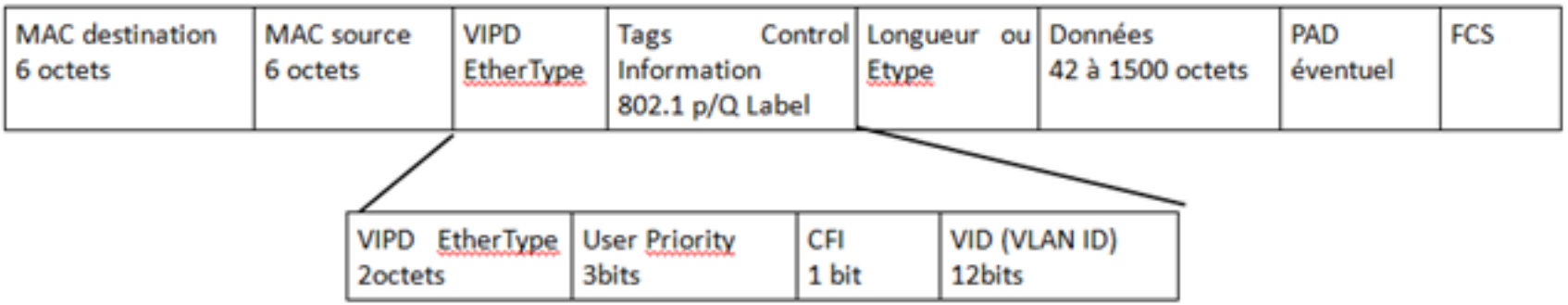
- **Mot de passe**
  - Au login de l'utilisateur

- **Lorsque un réseau comporte plusieurs commutateurs, chaque commutateur doit localiser toutes les machines (table d'acheminement) et connaître le VLAN d'appartenance de la source et du destinataire (filtrage de trafic). Si le réseau est important, les tables peuvent devenir très grandes et pénaliser les performances.**

- Il est **plus facile d'étiqueter les trames**

13- Les réseaux virtuels

- **Etiquetage des trames**:



- **Norme IEEE 802.1Q**:
  - définit l'étiquetage des trames
  - **Étiquette**: **identifie le VLAN de la station source**
  - **Commutateur**: n'a plus qu'à **connaître les VLAN d'appartenance des stations qui lui sont raccordées**
  - **VLAN tagging**
  - **4 octets supplémentaires** dans la trame (1522 octets)
  - Pour gérer **8 niveaux de priorité** (QOS)

13- Les réseaux virtuels

- **VPID**: Vlan Protocol Identifier
  - Identifie le **format de la trame 802.1p/Q**
  - 2 octets
  - Valeur: **0x8100**
  - Pour garantir la **compatibilité avec l'existant**
  - Vu comme une **encapsulation supplémentaire**
- **User Priority**:
  - Niveau de **priorité du vlan**
  - 3 bits, **8 niveaux possibles**
- **CFI**: Canonical Format Identifier
  - O: ethernet
  - 1: token-ring
- **VID**: Vlan Identifier
  - **Identification du Vlan destination**
  - 12 bits (4096 -2 = **4094 vlan possibles**)

CONFIGURATION DE VLAN

- **Objectif** d'une configuration de vlan:
  - configuration de **réseaux différents** sur un **même switch**.

- **Avantages principaux** de la segmentation par vlan :
  - **réduction** des **domaines de broadcast**
  - **accroissement de la sécurité** (mettre des filtres en place pour la communication entre les réseaux)

- **Principe de fonctionnement** du vlan par port:
  - **Un tag de 4 octets** est ajouté à la **trame Ethernet.**
  - Ce **tag** comprend entre autre **l'identifiant du vlan**.
  - Ainsi la **trame sera transmises uniquement aux ports appartenant au vlan identifié dans la trame.**

Types de configuration des ports des switchs

- Le **port** est configuré en **mode acces** ou en **mode trunk**

- **Le mode acces :**
  - est utilisé pour **la connexion terminale d'un périphérique (pc, serveur) appartenant à un seul vlan.**

- **Le mode trunk**:
  - est utilisé dans le cas ou **plusieurs vlans doivent circuler sur un même lien.**
  - cas d'une **liaison entre 2 switchs** ou d'un **serveur ayant une interface appartenant à plusieurs vlans.**

Vlan non affecté à un port et présent sur le switch

- Des **vlan peuvent être crées sur le switch et n'être affectés à aucun port:**
- cas du **vlan de management** (une adresse ip sera configurée sur ce vlan)
- Un **switch qui sert de liaison** aura également les vlan qui doivent le traverser déclarés dans sa configuration
- **VLAN natif**: c'est **le vlan par défaut du switch** (en général le vlan 1)
    - **Sans configuration, tous les ports du switch sont placés dans ce vlan.**
    - Ce **vlan n'est pas marqué** même s'il passe sur une liaison trunk

Configuration des switch

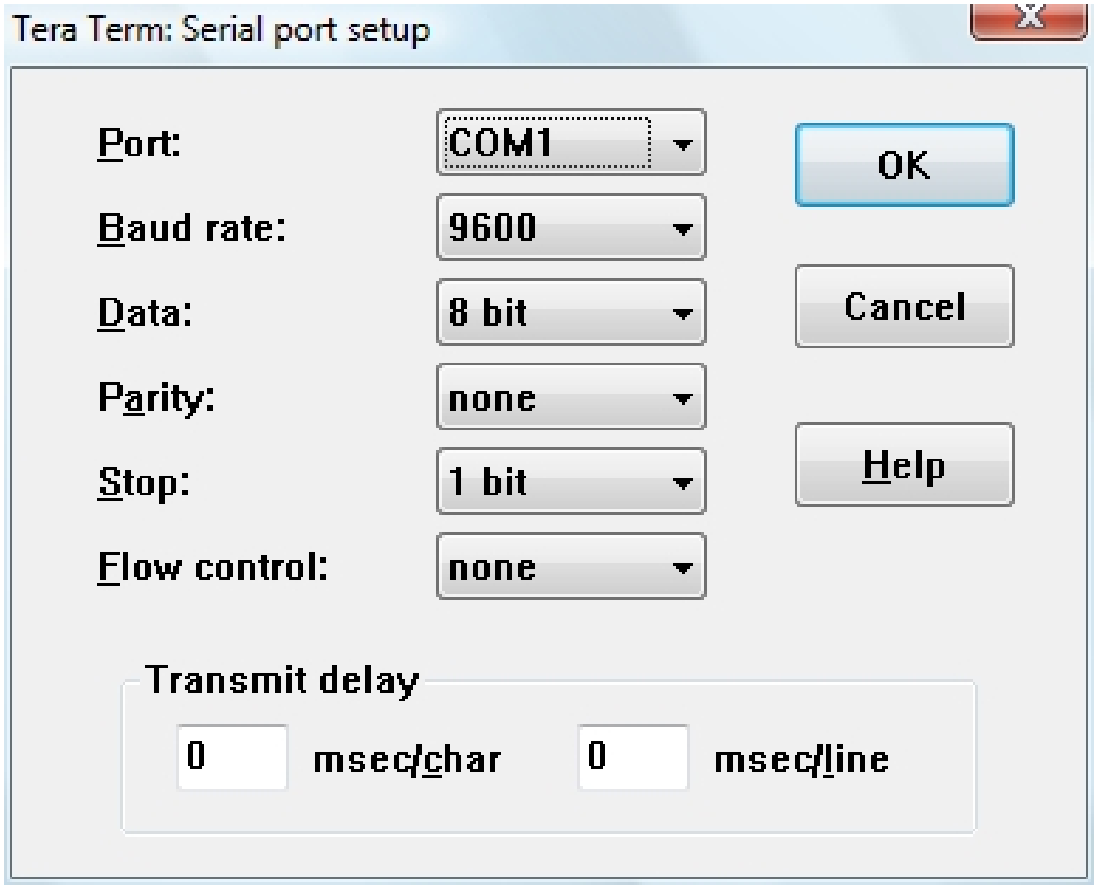
- La **première connexion : via le port console** du **switch.**

- On utilisera **un câble série** fourni avec le switch.

- La **prise RJ45** du câble est **connectée sur le switch**
- La **fiche DB9** est branchée **sur le PC**

- On utilisera **un terminal de connexion**
    - Exemples de **logiciels pour port série**:
    - Pour Windows: **hyper terminal**, **tera term pro**
    - Pour linux: **minicom**

Configuration du terminal



Mode console d'un switch

- Mode **avec** ou **sans privilège**
- **Une fois connecté** nous sommes placés dans un **mode sans privilège**
  - on ne peut effectuer que des commandes de diagnostique ou d'information
- **L'invite de commande** du **mode sans privilège** est: **Switch>**
- Pour **modifier la configuration**:
  - il faut passer en **mode privilégié**
    en entrant la commande: Switch>**enable**
- Voici le **nouvel invite de commande**: **Switch #**

Les invites de commande en fonction du contexte

- En **fonction des commandes entrées**, le switch présente des **invites de commande différentes**.

- **Mode configuration**:

  - Switch# **configure terminal**
    Switch(**config**)#

- **Configuration d'une interface**:

  - Switch(config)# **interface fastEthernet 0/1**
    Switch(**config-if**)#

Navigation entre les modes

- Commande **exit** : permet **d'accéder au contexte précédent**:

```
Switch  (config)#interface fastEthernet 0/1
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

- Commande **end**: permet **d'accéder à la racine**:

```
Switch#configure terminal
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#end
Switch#
```

- Commande **logout:** permet la **déconnexion**

```
Switch#logout
```

Aide pour la console

- ? : le point d'interrogation

- **Affiche les commande** disponibles **en fonction du contexte** dans lequel on se trouve

- exemple:

```
Switch#?
Exec commands:
access-enable Create a temporary Access-List entry
access-template Create a temporary Access-List entry
archive manage archive files
beep Blocks Extensible Exchange Protocol commands
cd Change current directory
clear Reset functions
clock Manage the system clock
cns CNS agents
--More--
```

Aide pour la console

- Affiche les **choix possibles** lors de la **saisie d'une commande**
  - exemple:

```
Switch#show ?
aaa Show AAA values
access-lists List access lists
accounting Accounting data for active sessions
```

- Nous propose les **choix possibles** lors de la **saisie des caractères** d'une commande:
  - exemple:

```
Switch#sh?
shell        show

Switch#sh
```

Commandes abrégées

- Possible **d'utiliser les commandes abrégées**.
- exemple les commandes suivantes **envoient le même résultat:**
-

Switch#wr
Building configuration...
[OK]

Switch#write
Building configuration...
[OK]

-

Switch#sh ru
Building configuration...

Current configuration : 783 bytes
!

Switch#show running-config
Building configuration...

Current configuration : 783 bytes

Startup-config et running-config

- **startup-config** : configuration utilisée au démarrage du switch.
- **running-config:** configuration courante utilisée par le switch.
- **Au démarrage du switch**: les configurations **startup-config et running-config sont les mêmes.**
- Si une **modification de configuration** est réalisée:
  - la **running-config sera modifiée**.
  - la startup-config ne sera pas modifiée.
- Pour **modifier la configuration de démarrage**:
  - il faudra **enregistrer la configuration courante (running-config) dans la startup-config**
  - toute **modification effectuée et non enregistrée** sera **annulée au prochain démarrage** du switch.

  Cette caractéristique est **intéressante en cas de problème grave suite à une modification** de configuration (par exemple une perte de lien). Il suffira **de redémarrer le switch pour revenir à l'état précédent la modification.**

Affichage de la configuration

- **Affichage de la configuration startup-config**
  - Switch# **show startup-config**

```
Using 783 out of 65536 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
--More--
```

- **Affichage de la configuration running-config**
  - Switch# **show running-config**

```
Building configuration...

Current configuration : 783 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
--More--
```

Enregistrement de la configuration

- **Deux commandes** peuvent être utilisée **pour enregistrer la configuration courante:**
  - switch# **copy running-config startup-config**
  - switch# **write**

    - switch# **copy running-config startup-config**
      Destination filename [startup-config]?
      Building configuration...
      [OK]
      0 bytes copied in 0.931 secs (0 bytes/sec)

  - Ou bien;
    - switch# **write**
      Building configuration...
      [OK]
      switch#

  - En abrégé:
    - switch# **co ru st**
      Destination filename [startup-config]?
      Building configuration...
      [OK]
      0 bytes copied in 0.923 secs (0 bytes/sec)
    -
      switch# **wr**
      Building configuration...
      [OK]
      switch#

Suppression de la configuration

- La commande suivante **supprime la configuration de démarrage**:

```
switch# write erase

Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
switch#
```

- La commande suivante **supprime les vlans configurés**:

```
switch# delete flash:vlan.dat

Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
switch#
```

- Il faut ensuite redémarrer le switch.

Redémarrage du switch

- Redémarrer un switch Cisco **avec la ligne de commande:**
    - switch# **reload**
      Proceed with reload? [confirm]
- Redémarrer un switch Cisco **avec temporisation**
    - **Deux méthodes** sont possibles:

– switch#**reload in ?**
  Delay before reload (mmm or hhh:mm)

  switch#reload in 5
  Reload scheduled for 15:24:35 CEST Mon Apr 4 2011 (in 5 minutes) by console
  Proceed with reload? [confirm]
  switch#

  ***
  *** --- SHUTDOWN in 0:05:00 ---
  ***

– switch#**reload at 16:00**
  Reload scheduled for 16:00:00 CEST Mon Apr 4 2011 (in 40 minutes) by console
  Proceed with reload? [confirm]
  switch#

- **Pour annuler le redémarrage:**

  switch#reload cancel

  switch#
  switch#

  ***
  *** --- SHUTDOWN ABORTED ---
  ***

  switch#

- **Affichage de l'état du redémarrage**

  switch#show reload

  Reload scheduled for 16:00:00 CEST Mon Apr 4 2011 (in 40 minutes) by console
  switch#

Configuration de base

- **Comment configurer:**
    - le nom du switch,
    - la configuration IP,
    - la passerelle par défaut
    - et création des mots de passe pour l'authentification.
- **Préparation: Il nous faut,**
    - le nom du switch,
    - le nom du domaine DNS,
    - l'adresse IP,
    - le masque de sous réseau,
    - la passerelle par défaut,
    - un nom de login pour l'administrateur
    - et le mot de passe administrateur.

- **Configuration du nom du switch, du domaine DNS, puis enregistrement de la configuration.**

- Dans l'exemple, le **nom du switch** est : ***2960-RG*** et **le domaine** est ***mondomaine.local*.**

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#hostname 2960-RG
2960-RG(config)#ip domain-name mondomaine.local
2960-RG(config)#end
2960-RG#wr
Building configuration...
[OK]
2960-RG#
```

- **Pour supprimer le nom du commutateur et le nom de domaine**, il faut saisir les commandes suivantes.

```
2960-RG(config)#no hostname
Switch(config)#no ip domain-name
Switch(config)#
```

Adressage IP du switch:

- Pour **superviser celui ci à distance**.
- Un **vlan dédié au management du switch est configuré** (ex : vlan2).
- L'adresse IP sera donc associée au vlan 2.
    - La configuration IP choisie est: Adresse IP : 192.168.100.25
    - Masque de sous-réseau : 255.255.255.0
    - Passerelle par défaut : 192.168.100.1

- 2960-RG(config)#**vlan 2**
  2960-RG(config-vlan)#**exit**
  2960-RG(config)#**interface vlan2**
  2960-RG(config-if)#**ip address 192.168.100.25 255.255.255.0**
  2960-RG(config-if)#**ex**
  2960-RG(config)#**ip default-gateway 192.168.100.1**

Adrssage IP du switch

- **Vérification de la configuration du vlan d'administration**

```
2960-RG#sh run int vlan2
Building configuration...

Current configuration : 64 bytes
!
interface Vlan2
ip address 192.168.100.25 255.255.255.0
end

2960-RG#
```

- **Suppression de l'adresse IP et de la passerelle par défaut:**

```
2960-RG(config)#interface vlan2
2960-RG(config-if)#no ip address
2960-RG(config-if)#ex
2960-RG(config)#no ip default-gateway
```

Ajout de mot de passe pour l'authentification

- La connexion au switch s'effectue :
  - par le port console en utilisant la ligne associée à ce port
  - ou bien à distance en utilisant les lignes virtuelles (appelées VTY).
    Par défaut, il n'y a pas de compte créé pour l'authentification.

- Il faut créer au minimum :
  - **un mot de passe pour l'accès aux différents terminaux** (console et virtuel)
  - et **un mot de passe pour l'accès au mode privilégié (enable).**

- Le mode d'administration par défaut est telnet.

- **Par défaut, mots de passe en clair lors de l'affichage du fichier de configuration.**

- **Activer le service *encryption-password***: les **mots de passe** apparaitront alors **chiffrés** lorsque les commandes d'affichage de la configuration sont entrées.

  - ***La commande est:*** Switch(config)#**service password-encryption**

Affichage des lignes disponibles.

- On notera la **ligne accessible par la console (CTY)**
- et **les lignes virtuelles (VTY) pour l'accès distant au switch.**

  - **2960-RG#sh line**

```
Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int
* 0 CTY - - - - - 0 0 0/0 -
1 VTY - - - - - 0 0 0/0 -
2 VTY - - - - - 0 0 0/0 -
3 VTY - - - - - 0 0 0/0 -
4 VTY - - - - - 0 0 0/0 -
5 VTY - - - - - 0 0 0/0 -
6 VTY - - - - - 0 0 0/0 -
7 VTY - - - - - 0 0 0/0 -
8 VTY - - - - - 0 0 0/0 -
9 VTY - - - - - 0 0 0/0 -
10 VTY - - - - - 0 0 0/0 -
```

Création des mots de passe et configuration de la console et des lignes virtuelles

- **Un mot de passe est créé pour se loguer au différentes lignes.**

```
2960-RG(config)#enable secret M02p@55
2960-RG(config)#line con 0
2960-RG(config-line)#password P@55w0rd
2960-RG(config-line)#login
2960-RG(config-line)#exit
2960-RG(config)#line vty 0 15
2960-RG(config-line)#password P@55w0rd
2960-RG(config-line)#login
2960-RG(config-line)#end
2960-RG#
```

- Il y a maintenant un **mot de passe à saisir pour l'accès au switch**
- et un **mot de passe à saisir pour l'accès au mode avec privilège.**

```
User Access Verification

Password:
2960-RG>en
Password:
2960-RG#
```

Configuration et affichage de l'heure

- switch#clock set 15:19:00 4 april 2011
  switch#
  switch#show clock
  15:19:05.609 CEST Mon Apr 4 2011
  switch#

Configuration des ports

- **Configuration les interfaces des switchs (vitesse, duplex, ...)**

- Les commandes suivantes ont été testées sur des
  switchs série 2950, 2960, 3750 et 6500

- Quelques mots sur **les noms des interfaces**:
  - Les interfaces **100Mbits/s** sont nommées **fastethernet,**
  - Les interfaces **1Gbit/s** sont nommées **gigabitEthernet**,
  - Et les interfaces **10Gigabit/s** sont nommées **TenGigabitEthernet.**

- Les **numéros des ports** ont **la syntaxe suivante**:
  - **0/1** C'est-à-dire, ***numéro du module/numéro du port***
  - ou **1/0/1** ***numéro du switch dans le stack/numéro du module/numéro du port*.**

- La commande suivante affiche la configuration courante d'une interface.
    - En cas de modification, il faut enregistrer cette configuration...

2960-switch#sh running-config interface fastEthernet 0/1

```
Building configuration...

Current configuration : 85 bytes
!
interface FastEthernet0/1
switchport access vlan 7
switchport mode access
end
```

- Commande pour afficher les valeurs des compteurs d'une interface:

2960-switch#show interfaces gigabitEthernet 0/1

GigabitEthernet0/1 is up, line protocol is up (connected)
Hardware is Gigabit Ethernet, address is 0026.3750.2950 (bia 0026.3750.2950)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is 10/100/1000BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 187000 bits/sec, 231 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
225348823 packets input, 188621734150 bytes, 0 no buffer
Received 130125788 broadcasts (87756518 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 87756518 multicast, 0 pause input
0 input packets with dribble condition detected
1222204 packets output, 103305303 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
2960-switch#

- **Plusieurs infos intéressantes**:

    - le port est up ou down,
    - l'interface est de type giga, fonctionne en full duplex avec un débit de 100Mbit/s.
    - Pour les stats, il y a les compteurs concernant le débit et les erreurs.
      Ainsi, en cas de modification sur une interface, les deux commandes précédentes permettent de vérifier la prise en compte de la modification.

- **Résumé des informations pour l'ensemble des ports:**

- 2960-switch#**show interfaces status**

  Port Name Status Vlan Duplex Speed Type
  Fa0/1 notconnect 3 auto auto 10/100BaseTX
  Fa0/2 notconnect 3 auto auto 10/100BaseTX
  Fa0/3 notconnect 6 auto auto 10/100BaseTX
  Fa0/4 notconnect 3 auto auto 10/100BaseTX
  Fa0/5 notconnect 3 auto auto 10/100BaseTX
  Fa0/6 notconnect 3 auto auto 10/100BaseTX
  Fa0/7 notconnect 3 auto auto 10/100BaseTX
  Gi0/1 connected trunk a-full a-100 10/100/1000BaseTX

- **Modification de la description, la vitesse et le duplex d'une interface**
- **Ajout d'une description**

```
2960-RG(config)#int fastEthernet 0/1
2960-RG(config-if)#description serveur de fichier
2960-RG(config-if)#end
```

- **Paramétrage de la vitesse et du mode duplex d'un port.**

  - Par défaut, la vitesse et le mode duplex des ports sont configurés automatiquement.
  - Le switch et le périphérique connecté négocient la valeur de ces paramètres.
  - Il est néanmoins possible de fixer ces valeurs. Dans ce cas, les valeurs seront fixées sur le switch et sur le matériel connecté.

- **Paramètre disponible pour une interface 100Mbit/s:**

```
2960-RG(config-if)#speed ?
10 Force 10 Mbps operation
100 Force 100 Mbps operation
auto Enable AUTO speed configuration

2960-RG(config-if)#duplex ?
auto Enable AUTO duplex configuration
full Force full duplex operation
half Force half-duplex operation
```

- **Pour fixer la vitesse à 10Mbit/s puis le mode duplex half:**

```
2960-RG(config)#interface fastEthernet 0/1
2960-RG(config-if)#speed 10
2960-RG(config-if)#duplex half
2960-RG(config-if)#end
```

- **on vérifie dans la conf et sur l'interface**:

  2960-RG#**sh run int fa0/1**
  Building configuration...
  Current configuration : 331 bytes
  !
  interface FastEthernet0/1
  description serveur de fichier
  speed 10
  duplex half

  2960-RG#sh int fa0/s1
  FastEthernet0/1 is down, line protocol is down (notconnect)
  Description: serveur de fichier
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 10Mb/s, media type is 10/100BaseTX

- **Pour remettre les paramètres par défaut:**

```
2960-RG(config)#int fastEthernet 0/1
2960-RG(config-if)#speed auto
2960-RG(config-if)#duplex auto
```

- **Désactiver et activer une interface**
- Dans l'exemple, on **désactive puis on réactive l'interface fa0/1**.

```
Switch(config)#int fa0/1
Switch(config-if)#shut
Switch(config-if)#end
Switch#
*Mar 2 02:38:13.253: %SYS-5-CONFIG_I: Configured from console by console
*Mar 2 02:38:13.849: %LINK-5-CHANGED: Interface FastEthernet0/1, changed
state to administratively down
```

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#no shut
Switch(config-if)#end
*Mar 2 02:38:29.989: %SYS-5-CONFIG_I: Configured from console by console
*Mar 2 02:38:30.920: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed
state to down
```

- **Suppression de la configuration d'un port**

- La commande suivante réinitialise le port avec la configuration par défaut. On vérifie en affichant la configuration du port (gi1/0/1 dans l'exemple).

  switch(config)#default interface gigabitEthernet 1/0/1
  Interface GigabitEthernet1/0/48 set to default configuration
  switch(config)#**end**
  switch#sh run int gi1/0/1
  Building configuration...

  Current configuration : 39 bytes
  !
  interface GigabitEthernet1/0/1
  end

  switch#

- **Affichage du statut PoE (power over ethernet) des ports**

- La technologie poe (802.3af) permet l'alimentation électrique de périphérique (téléphone, borne wifi, ...) par les ports des switchs.
- Si le switch supporte cette technologie, la commande suivante permet de visualiser le budget électrique général ainsi que le statut de chaque port.
- **2960-RG#show power inline**

  Module Available Used Remaining
  (Watts) (Watts) (Watts)
  ------ --------- -------- ---------
  1 370.0 37.8 332.2
  Interface Admin Oper Power Device Class Max
  (Watts)
  --------- ------ ---------- ------- ------------------ ----- ----
  Fa1/0/1 auto off 0.0 n/a n/a 15.4
  Fa1/0/2 auto on 6.3 IP Phone 7960 n/a 15.4
  Fa1/0/3 auto on 6.3 IP Phone 7960 n/a 15.4
  Fa1/0/4 auto on 6.3 IP Phone 7960 n/a 15.4
  Fa1/0/5 auto on 6.3 IP Phone 7960 n/a 15.4
  Fa1/0/6 auto off 0.0 n/a n/a 15.4
  Fa1/0/7 auto on 6.3 IP Phone 7960 n/a 15.4
  Fa1/0/8 auto off 0.0 n/a n/a 15.4

Configuration des VLAN sur un switch Cisco

- **Configuration des vlans par port sur un switch Cisco**.
  Les commandes suivantes ont été testées sur des switchs série 2950, 2960, 3750 et 6500

- **Rappel sur la notion de VLAN (Virtual Local Area Network)**
  - objectif d'une configuration de vlan: permettre la configuration de réseaux différents sur un même switch.
  - plusieurs façon de configurer les vlans. On traitera uniquement du vlan par port.
  - La norme utilisée ici porte l'identifiant 802.1q.
  - Les avantages principaux de la segmentation par vlan sont:
    - la réduction des domaines de broadcast
    - et l'accroissement de la sécurité (si des filtres sont mis en place pour la communication entre les réseaux).

- **Principe de fonctionnement du vlan par port:**

  Un tag de 4 octet est ajouté à la trame ethernet. Ce tag comprend entre autre l'identifiant de VLAN. Ainsi, la trame sera transmise uniquement aux ports appartenant au vlan identifié dans la trame.

- **Type de configuration des ports des switchs Cisco**
-

  Le port est configuré en mode *access* ou en mode *trunk*.
  Le mode *access* est utilisé pour la connexion terminale d'un périphérique (pc, imprimante, serveur, ...) appartenant à un seul vlan. Le mode *trunk* est utilisé dans le cas ou plusieurs vlans doivent circuler sur un même lien. C'est par exemple le cas de la liaison entre deux switchs ou bien le cas d'un serveur ayant une interface appartenant à plusieurs vlans.

Cas particulier de la connexion d'un téléphone IP suivi d'un PC sur un port

Dans le cas de l'utilisation d'un ordinateur connecté à un téléphone IP (ce dernier étant connecté à un port du switch), le port aura deux vlans (un vlan dédié au réseau donnée et un vlan dédié au réseau voix). Le port sera configuré en général en mode *access*, une commande sera ajoutée pour la configuration du vlan voix (*voice vlan*).

- **VLAN non affecté à un port et présent sur le switch:**

  Des vlans peuvent être créés sur un switch et n'être affectés à aucun port. C'est le cas du vlan de management (une adresse IP sera configurée sur ce vlan).
  Un switch qui sert de liaison aura également les vlans qui doivent le traverser déclaré dans sa configuration.

- **Communication entre les vlans:**

  La communication entre les vlans est possible en passant par un routeur ou un switch de niveau 3 (switch-routeur).
  Selon l'utilisation, il peut être conseillé de filtrer les réseaux au minimum au moyen d'ACLs (access control list).

- **VLAN natif**:

  Le vlan appelé "natif" est le vlan par défaut du switch (en général le vlan 1). Sans configuration, tous les ports du switch sont placés dans ce VLAN. Ce vlan n'est pas marqué même si il passe sur une liaison trunk.

- Configuration type d'un switch:
- La liaison entre les switchs est en mode *trunk*.
- Les autres ports des switchs sont en mode *access*.
- Le vlan dédié aux téléphones sera également configuré sur tous les ports en plus de leur vlan data respectif.

- Un vlan dédié à l'administration et à la supervision du switch sera créé.
- L'adresse IP de supervision du switch sera associée à ce vlan.

- **Ajout de vlan**

    - **Création du vlan 2 puis des vlans 3 à 5**

      2960-RG(config)#**vlan 2**
      2960-RG(config-vlan)#**name administration**
      2960-RG(config-vlan)#**ex**
      2960-RG(config)#**vlan 3,4,5**
      2960-RG(config-vlan)#**ex**
      2960-RG(config)#

- **suppression d'un vlan**

      2960-RG(config)#**no vlan 2**

- **Affichage des vlans ainsi que des affectations de port**

2960-RG#show vlan

VLAN Name Status Ports

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Gi0/1
2 administration active
3 VLAN0003 active
4 VLAN0004 active Fa0/5, Fa0/6, Fa0/7, Fa0/8
5 VLAN0005 active
10 VLAN0010 active Fa0/1
1002 fddi-default act/unsup
1003 token-ring-default act/unsup

- **Affectation d'un port à un vlan**
- Dans l'exemple ci-dessous le port est configuré en mode access puis il est placé dans le vlan 3.
  Pour un switch série 2950, 2960, 3750 2960-

    - RG(config)#**interface fastEthernet 0/1**
      2960-RG(config-if)#**switchport mode access**
      2960-RG(config-if)#**switchport access vlan 3**
      2960-RG(config-if)#**ex**
      2960-RG(config)#

- **L'exemple suivant présente la configuration des ports 5 à 8 en mode access, puis configurés avec le vlan 4**

```
2960-RG(config)#interface range fastEthernet 0/5-8
2960-RG(config-if-range)#switchport mode access
2960-RG(config-if-range)#switchport access vlan 4
2960-RG(config-if-range)#end
2960-RG#
```

- **Pour un switch série 6500**

```
6500(config)#interface gi 0/2
6500(config-if-range)#switchport
6500(config-if-range)#switchport mode access
6500(config-if-range)#switchport access vlan 4
6500(config-if-range)#end
6500#
```

- **Configuration d'un port en mode trunk**
  (par exemple une connexion entre deux switch)

- **Pour un switch série 2950 et 3750**
  3750(config)#**interface gigabitEthernet 1/0/1**
  3750(config)#**switchport trunk encapsulation dot1q**
  3750(config-if)#**switchport mode trunk**
  3750(config-if)#

- **Pour un switch série 2960**
  2960-RG(config)#**interface gigabitEthernet 1/0/1**
  2960-RG(config-if)#**switchport mode trunk**
  2960-RG(config-if)#

- **Pour un switch série 6500**
  6500(config)#**interface gigabitEthernet 1/0/1**
  6500(config-if)#**switchport**
  6500(config-if)#**switchport trunk encapsulation dot1q**
  6500(config-if)#**switchport mode trunk**
  6500(config-if)#

- **Filtrage des vlans sur un port uplink**
  - Pour les swiths série 2950, 2960, 3750, 6500
  - **dans l'exemple, on autorise les vlans 2,3 et 10 a être transportés sur le lien**

```
2960-RG(config)#interface gigabitEthernet 1/0/1
2960-RG(config-if)#switchport trunk allowed vlan add 2,3,10
2960-RG(config-if)#
```

- **Pour interdire un vlan de passer par le lien trunk (dans l'exemple, le vlan3):**

```
2960-RG(config-if)#switchport trunk allowed vlan remove 3
2960-RG(config-if)#
```

- **Pour supprimer la commande de filtrage:**

```
2960-RG(config-if)#no switchport trunk allowed vlan
2960-RG(config-if)#
```

- **Configuration d'un vlan dédié à la téléphonie**
- Le protocole cdp doit préalablement être activé.

```
2960-RG(config)#vlan 10
2960-RG(config-vlan)#name voip
2960-RG(config-vlan)#ex
2960-RG(config)#int fastEthernet 0/1
2960-RG(config)#switchport voice vlan 10
```

- **Suppression de la configuration d'un port**
- Comme d'habitude, il suffit de mettre la commande no devant les commandes entrées précédemment.
  Par exemple:

```
2960-RG(config)#int fastEthernet 0/1
2960-RG(config-if)#no switchport access vlan
2960-RG(config-if)#no switchport mode acc
2960-RG(config-if)#end
```

- **Configuration du protocole VTP (Vlan Transport Protocol) en mode transparent**
- Le protocole VTP permet la configuration automatique de vlan entre des serveurs VTP et des clients sur un même domaine VTP.
  Pour utiliser uniquement la base locale de vlan sur nos commutateurs, on configure VTP en mode transparent.

```
Switch(config)#vtp domain mondomaine
Changing VTP domain name from NULL to mondomaine
Switch(config)#
Switch(config)#vtp mode transparent
Device mode already VTP Transparent for VLANS.
Switch(config)#vtp password passdomaine
Setting device VTP password to passdomaine
Switch(config)#vtp version 2
Switch(config)#^Z
Switch#
Switch#
Switch#show vtp status
VTP Version capable : 1 to 3
VTP version running : 2
VTP Domain Name : mondomaine
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0012.dbab.4321
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
--------------
VTP Operating Mode : Transparent
Maximum VLANs supported locally : 1005
Number of existing VLANs : 19
Configuration Revision : 0
MD5 digest : 0x1D 0x52 0x66 0xAA 0xD8 0xAA 0x30 0xFF
0x6C 0xCA 0xB0 0x6F 0x5C 0xF3 0x9D 0xCC
Switch#
```

- **Commande nonegociate**

- Le **protocole DTP** (**D**ynamic **T**runking **P**rotocol) :
    - permet à deux commutateurs qui sont connectés ensemble de monter un lien trunk automatiquement sous certaines conditions (par exemple la connexion d'un port configuré par défaut en dynamic auto vers un port trunk). En général, il vaut mieux désactiver cette possibilité.
      On désactive donc cette option sur tous les ports access et trunk.
    - **Switch(config)#interface range fastEthernet 1/0/1 - 10**
      Switch(config-if-range)#switchport nonegotiate

- Vérification sur une interface:

Switch#show interfaces fa1/0/2 switchport
Name: Fa1/0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 2 (VLAN0002)

Configuration de la qos pour la voip

- Configuration automatique de la qos dédiée à la voip:

  Les commandes suivantes ont été testées sur des switchs série 2950, 2960 et 3750.

- Des commandes permettent de configurer la qualité de service automatiquement
  - pour les ports d'accès (sur lesquels sont reliés les téléphones)
  - et pour les ports d'uplink (liaison entre les switches).

- **Activation de la qos pour les switchs séries 3750 et 2960**
  - Port d'accès:

```
3750(config)#int fastEthernet 0/1
3750(config-if)#auto qos voip cisco-phone
3750(config-if)#end
```

- **Affichage de la configuration du port** (les commandes de qualité de service ont été ajoutées):
-

```
3750#sh run int fastEthernet 1/0/1
Building configuration...

Current configuration : 295 bytes
!
interface FastEthernet1/0/1
switchport access vlan 4
switchport mode access
switchport voice vlan 10
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
mls qos trust device cisco-phone
mls qos trust cos
auto qos voip cisco-phone
spanning-tree portfast
end
```

- Port de liaison, trunk ou uplink, switch série 2960 et 3750
  3750(config)#int gi 0/1
  3750(config-if)#auto qos voip trust
  3750(config-if)#end

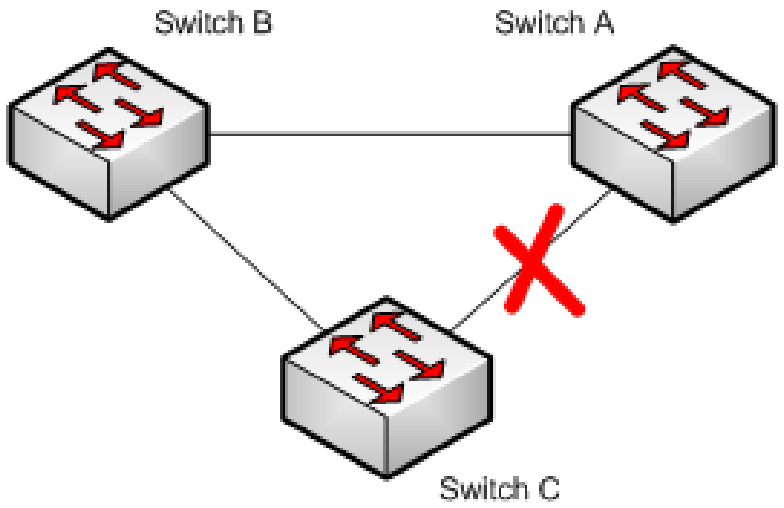
- **Activation de la qualité de service pour un port uplink série 6500**
- Activation générale
  6500(config)#mls qos

- Activation pour un port uplink (concerne la qos appliquée sur le niveau 2)
  6500(config)#int gi 0/1
  6500(config-if)#mls qos trust cos

Configuration du spanning-tree sur un switch Cisco

- Pour rappel, l'objectif du protocole (défini par la norme 802.1d) est de gérer les boucles sur un réseau local dans le cas de l'utilisation de lien redondant.
  Si une possibilité de boucle est détectée, un des ports du switch est bloqué.

  C'est un protocole de niveau 2.



- Par défaut le spanning-tree est actif sur le commutateur (mode pvst+). Il existe deux autres modes disponibles sur les commutateurs: rapid pvst+ basé sur le protocole 802.1w et MSTP basé sur le protocole 802.1s.

  Dans certain cas, il est souhaitable de fixer les priorités par défaut.
  Le switch qui aura la priorité la plus basse sera élu root. On choisit un switch qui est placé en tête du réseau (backbone) puisque tout le traffic passe par lui et qu'en général, il n'y a pas beaucoup de machine cliente connectée.
  De plus, on peut préférer un lien par rapport à un autre, pour des raisons de débit différent par exemple.

  La priorité par défaut d'un switch est de 32768. La priorité d'un port par défaut est 128. Si on abaisse le chiffre, le switch ou le port devient prioritaire par rapport aux autres.
  Activation du rapid spanning-tree sur le switch
- 2960-RG(config)#spanning-tree mode rapid-pvs

- **Vérification des informations**
- 2960-RG#sh spanning-tree

  VLAN0001
  Spanning tree enabled protocol rstp
  Root ID Priority 28673
  Address 0008.e4ff.ec11
  Cost 23
  Port 9 (GigabitEthernet0/1)
  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
  Address 0026.4585.2100
  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
  Aging Time 300 sec

  Interface Role Sts Cost Prio.Nbr Type
  ---------- ---- --- --------- -------- --------------------------------
  Gi0/1 Root FWD 19 128.9 P2p

- Il est possible, entre autre, de préciser une interface à la suite de la commmande *sh spanning-tree*.
  Fixer le switch root
- Dans la copie d'écran suivante le switch est root pour les vlans 1 à 100. Puis on affiche les données spanning-tree pour le vlan 4.
  switch(config)#spanning-tree vlan 1-100 root primary
  switch(config)#end
  switch#show spanning-tree vlan 4

  VLAN04
  Spanning tree enabled protocol rstp
  Root ID Priority 24726
  Address 0026.525b.3500
  This bridge is the root
  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID Priority 24726 (priority 24576 sys-id-ext 4)
  Address 0026.525b.3500
  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
  Aging Time 300 sec

  Interface Role Sts Cost Prio.Nbr Type
  ---------- ---- --- --------- -------- --------------------------------
  Fa0/3 Desg FWD 19 128.3 P2p
  Gi0/1 Desg FWD 19 128.9 P2p

  switch#

Configuration des services syslog, NTP et SNMP

- **Commande pour afficher les logs**
- 2960-RG#show log
  Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)

  *Mar 1 00:01:00.481: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up
  *Mar 1 00:01:29.808: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
  *Mar 1 00:07:22.490: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down
  *Mar 1 00:07:22.499: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state

- **Configuration du service syslog**
- Le pré-requis est d'avoir installé un serveur type syslog (adresse 192.168.0.123 dans l'exemple).

  Configuration du niveau d'information demandée: dans l'exemple, on demande le maximum d'information.

```
2960-RG(config)#logging trap ?
<0-7> Logging severity level
alerts Immediate action needed (severity=1)
critical Critical conditions (severity=2)
debugging Debugging messages (severity=7)
emergencies System is unusable (severity=0)
errors Error conditions (severity=3)
informational Informational messages (severity=6)
notifications Normal but significant conditions (severity=5)
warnings Warning conditions (severity=4)


2960-RG(config)#logging trap debugging
2960-RG(config)#
```

- Puis on configure l'étiquette associée à chaque message (ici local4) ainsi que l'adresse IP du serveur syslog.
  2960-RG(config)#logging facility local4
  2960-RG(config)#logging 192.168.0.123

- **Configuration du service NTP**
- Synchronisons maintenant les informations horaires du switch à un serveur NTP (network time protocol).
  Nous indiquons dans un premier temps l'adresse IP du serveur NTP, puis on configure le fuseau horaire ainsi que le moment de passer à l'heure d'été (dans l'exemple: pour la France).
  2960-RG(config)#ntp server 192.168.0.124
  2960-RG(config)#clock timezone cet 1
  2960-RG(config)#clock summer-time cest recurring last Sun Mar 3:00 last Sun Oct 3:00

- Quelques commandes de vérification: les associations avec le serveur ntp et l'affichage de la date et de l'heure courante:
  2960-RG#sh ntp associations

  address ref clock st when poll reach delay offset disp
  *~192.168.0.124 208.52.173.46 2 0 64 1 1.7 4.27 15875.
  * master (synced), # master (unsynced), + selected, - candidate, ~ configured
  2960-RG#sh clock
  16:51:03.048 cet Thu Jan 27 2011
  2960-RG#

- **Configuration du service SNMP**
- Voyons maintenant comment configurer l'accès de notre switch à un serveur de supervision basé sur le protocole SNMP.

  Nous configurons tout d'abord une liste d'accès pour autoriser uniquement la connexion du serveur de management SNMP, puis nous indiquons le nom de la communauté SNMP ainsi que les droits associés (lecture (ro) ou lecture/écriture (rw)).
  2960-RG(config)#access-list 1 permit 192.168.1.2
  2960-RG(config)#snmp-server community macomm ro 1
  2960-RG(config)#exit
  2960-RG#show snmp community

- **Configurer une priorité sur un port**
- Dans l'exemple, l'interface prioritaire sera gi0/1 pour les vlans 1 à 100. On affiche ensuite les informations pour le vlan 4.

```
switch(config)#interface gigabitEthernet 0/1
switch(config-if)#spanning-tree vlan 1-100 port-priority 64
switch(config-if)#end
switch#show spanning-tree vlan 4

VLAN04
Spanning tree enabled protocol rstp
Root ID Priority 32918
Address 0008.e3de.fe32
Cost 23
Port 9 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32918 (priority 32768 sys-id-ext 4)
Address 0026.525b.3500
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/3 Desg FWD 19 128.3 P2p
Gi0/1 Root FWD 19 64.9 P2p


switch#
```

- **Configuration des ports d'accès reliés à un switch**
- Lors du démarrage d'un switch, la recherche de la meilleure topologie prend un peu de temps. La commande suivante fait passer directement le port de l'état *blocking* à l'état *forwarding*, le démarrage de l'interface est donc plus rapide. On appliquera cette commande sur les ports reliés à des machines terminales (PC, imprimante, ...).

  2960-RG(config)#int range fa0/1 - 8
  2960-RG(config-if-range)#spanning-tree portfast

- Vérification
  2960-RG#sh run int fa0/1
  Building configuration...

  Current configuration : 107 bytes
  !
  interface FastEthernet0/1
  switchport access vlan 2
  switchport mode access
  spanning-tree portfast
  end

- Désactivation du *spanning-tree portfast* pour une interface puis vérification.

```
2960-RG(config)#int fa0/1
2960-RG(config-if)#no spanning-tree portfast
2960-RG(config-if)#end
2960-RG#sh run int fa0/1
Building configuration...

Current configuration : 83 bytes
!
interface FastEthernet0/1
switchport access vlan 2
switchport mode access
end

2960-RG#
```

Mise à jour de l'IOS switch Cisco

- Commande pour afficher le modèle du switch, la version de l'IOS, pour mettre à jour le switch et pour sauvegarder la configuration.
  Les commandes suivantes ont été testées avec les switchs série 2950, 2960 et 3750.

- **Affichage de la version de l'IOS**
- La commande suivante affiche la version de l'IOS, le numéro de série du switch, l'uptime (la durée depuis le dernier démarrage), ...

```
2960-RG#show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(55)SE1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Thu 02-Dec-10 08:16 by prod_rel_team
Image text-base: 0x00003000, data-base: 0x01800000

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(44r)SE1, RELEASE SOFTWARE (fc2)

29060-RG uptime is 2 weeks, 21 hours, 26 minutes
System returned to ROM by power-on
System image file is "flash:/c2960-lanbasek9-mz.122-55.SE1/c2960-lanbasek9-mz.122-55.SE1.bin"

Switch Ports Model SW Version SW Image
------ ----- ----- ---------- ----------
* 1 9 WS-C2960PD-8TT-L 12.2(55)SE1 C2960-LANBASEK9-M
```

- Dans ce cas, le numéro de version de l'IOS est 12.2(55)SE1. L'IOS est stocké dans la flash, le switch a redémarré il y a deux semaines et c'est un 2960 8 ports.

  Affichage des fichiers présents dans la flash:
  2960-RG#dir flash:
  Directory of flash:/

  2 -rwx 4120 Mar 14 1993 23:49:35 +00:00 multiple-fs
  3 -rwx 1091 Mar 14 1993 23:49:34 +00:00 private-config.text
  4 -rwx 2176 Mar 14 1993 19:03:35 +00:00 vlan.dat
  5 -rwx 2401 Mar 14 1993 23:49:34 +00:00 config.text
  6 drwx 512 Mar 7 1993 04:10:49 +00:00 c2960-lanbasek9-mz.122-55.SE1

  27998208 bytes total (18131456 bytes free)
  2960-RG#

- L'IOS ainsi que les fichiers de configuration sont stockés à cet emplacement (flash:). On notera aussi la place occupée et disponible.

- **Mise à jour d'un IOS**
- Nous avons besoin d'un IOS (disponible chez Cisco) et d'un serveur tftp.
  La commande suivante simplifie la mise à jour puisqu'elle fait tout toute seule (configuration des variables, suppression de l'ancien IOS, et installation du nouvel IOS). Il ne reste plus qu'a redémarrer le switch (il peut aussi redémarrer tout seul en option).
  Bien sur, durant la mise à jour, il ne faut pas débrancher le switch sous réserve de devoir passer au plan B qui est nettement plus long...

  L'adresse du serveur tftp est dans notre cas 192.168.1.123.
  2960-switch#archive download-sw /overwrite tftp://192.168.1.123/c2960-ipbasek9-tar.122-55.SE1.tar
  Loading /c2960-ipbasek9-tar.122-55.SE1.tar from 192.168.1.123 (via Vlan2): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

- Il est maintenant temps de faire une pause et d'aller boire un café...

  Lorsque le switch a terminé sa mise à jour, vérifions que la nouvelle image est en place par un *dir flash:*, puis vérifions que le nouvel IOS est bien pris en compte dans les variables de démarrage:
  2960-RG#show boot
  BOOT path-list : flash:/c2960-lanbasek9-mz.122-55.SE1/c2960-lanbasek9-mz.122-55.SE1.bin
  Config file : flash:/config.text
  Private Config file : flash:/private-config.text
  Enable Break : no
  Manual Boot : no
  HELPER path-list :
  Auto upgrade : yes
  Auto upgrade path :
  NVRAM/Config file
  buffer size: 65536
  Timeout for Config
  Download: 0 seconds
  Config Download
  via DHCP: disabled (next boot: disabled)
  2960-RG#

Comment faire?

Il suffit de connecter le cable de stack à l'arrière des switches. Pour le 2960s, un module doit également être ajouté.

Pour optimiser la bande passante et pour améliorer la redondance, l'architecture stackée

- Si tout est OK, redémarrons le switch, la commande *show version* permet de vérifier la version de la nouvelle image installée.
  Sauvegarde de la configuration
- Sauvegarde du fichier de configuration en utilisant un serveur tftp.
  2960-RG#copy flash:config.text tftp://192.168.2.1/
  Address or name of remote host [192.168.2.1]?
  Destination

Comment mettre en place une pile de switch 3750 ou 2960s

- **Pourquoi stacker des switchs?**
- Simplifier l'administration (l'ensemble des switchs apparaissent pour l'administrateur comme un seul switch),
- Améliorer la bande passante entre les switches,
- Améliorer la redondance en cas de panne.
- **Comment faire?**
- Il suffit de connecter le cable de stack à l'arrière des switches. Pour le 2960s, un module doit également être ajouté.
  Pour optimiser la bande passante et pour améliorer la redondance, l'architecture stackée formera une boucle. Ci dessous, un exemple d'un stack composé de deux switchs.

- **Pré-requis pour stacker des switches sans problème**
- Puisque les switchs appartenant à une pile seront vus comme un seul switch, les versions d'IOS doivent être identiques pour tous les switchs. Avant de stacker des switchs, on vérifiera les versions d'IOS de chaque switch.
  Et si un switch est ajouté à une pile, il est préférable que l'IOS de ce switch corresponde à celui du stack en place.

  Autre solution: Si il y a uniquement une différence de version entre les IOS et que ceux ci sont récents (je vous laisse chercher la version minimum), le switch peut lancer une mise à jour automatique.
  Dans l'exemple suivant, le switch 2 a été ajouté, la version courante de l'IOS ne convient pas (*mismatch*). Le switch lance la procédure de mise à jour automatique.

```
cisco-3750#sh switch
Switch/Stack Mac Address : 0012.e350.0356
H/W Current
Switch# Role Mac Address Priority Version State
----------------------------------------------------------
*1 Master 1234.e350.0356 1 0 Ready
2 Member d235.eb65.3108 1 2 Version Mismatch

cisco-3750#
Jan 21 14:42:30.338: %IMAGEMGR-6-AUTO_COPY_SW_INITIATED: Auto-copy-software process
initiated for switch number(s) 2
```

- Si l'autoconfiguration ne se lance pas, on peut toujours tenter de recopier l'IOS sur le switch qui a été ajouté.
  La commande suivante recopie l'IOS du switch 1 vers le switch 2 (*destination-system*). Il faudra ensuite rédémarrer le switch.
  cisco-3750#archive copy-sw /destination-system 2 1
- **fonctionnement et configuration des switchs de la pile**
- Un switch maitre est élu et gère le controle de la pile de switch. Lorsqu'un switch est ajouté à une pile, les ports s'ajoutent à la configuration en cours. Ainsi, les ports du switch numéro 1 de la pile auront comme numéro 1/0/x, les ports du switch numéro 2 de la pile auront comme numéro 2/0/x, etc ... Les autres paramètres de configuration sont communs.
  Il y a donc un seul fichier de configuration pour l'ensemble des switchs. Les numéros de ports apparaissent dans ce fichier.

- La commande suivante affiche la configuration du port 5 du deuxième switch du stack:
  sw-3750#show running-config interface fastEthernet 2/0/5
  Building configuration...

  Current configuration : 309 bytes
  !
  interface FastEthernet2/0/5
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
  end

- Pour afficher le numéro d'un swith dans la pile, il faut presser le bouton mode pour selectionner l'item *stack*, le numéro du port qui clignote correspond au numéro du switch.

- **Quelques commandes de supervision**
- Affichage des switchs appartenant à la pile ainsi que la correspondance des ports reliés entre eux.

```
sw-3750#sh switch detail
Switch/Stack Mac Address : aa12.4321.0372 H/W Current
Switch# Role Mac Address Priority Version State
----------------------------------------------------------
*1 Master aa12.4321.0372 1 0 Ready
2 Member aa12.b7a4.4256 1 0 Ready
3 Member aa11.c4d2.325a 1 0 Ready



Stack Port Status Neighbors
Switch# Port 1 Port 2 Port 1 Port 2
----------------------------------------------------------
1 Ok Ok 3 2
2 Ok Ok 3 1
3 Ok Ok 2 1

sw-3750#
```

- Quelques commandes d'affichage de statistique sur les ports de stacks:
  sw-3750#sh switch stack-ring speed

  Stack Ring Speed : 32G
  Stack Ring Configuration: Full
  Stack Ring Protocol : StackWise

-
  sw-3750#sh switch stack-ring activity

  Sw Frames sent to stack ring (approximate)
  ---
  1 2507518748
  2 1995263804

  Total frames sent to stack ring : 4502782552

-
  sw-3750#sh switch stack-ports summary

  Switch#/ Stack Neighbor Cable Link Link Sync # In
  Port# Port Length OK Active OK Changes Loopback
  Status To LinkOK
  --- --- --- --- --- --- --- --- ---
  1/1 OK 2 50 cm Yes Yes Yes 2 No
  1/2 OK 2 50 cm Yes Yes Yes 5 No
  2/1 OK 1 50 cm Yes Yes Yes 4 No
  2/2 OK 1 50 cm Yes Yes Yes 1 No

- **Comment afficher la version les informations administratives d'un switch appartenant à un stack**
- La commande d'affichage suivante permet de visualiser la version de l'ios ou encore le numéro de série de chaque switch.

  sw-3750#sh version

  .....

  Switch Ports Model SW Version SW Image
  ------ ----- ----- ---------- ----------
  * 1 52 WS-C3750-48P 12.2(55)SE1 C3750-IPBASEK9-M
  2 52 WS-C3750-48P 12.2(55)SE1 C3750-IPBASEK9-M

  .....

  Switch 02

  Switch Uptime : 5 weeks, 2 days, 22 hours, 11 minutes
  Base ethernet MAC Address : 00:a2:05:8f:23:02
  Motherboard assembly number : 86-9273-22
  Power supply part number : 458-1032-15

  ......

- Affichage du contenu de la mémoire flash du switch 2
  sw-3750#sh flash2:

  Directory of flash2:/

  2 drwx 128 Dec 12 2010 09:05:35 +01:00 c3750-ipbasek9-mz.122-55.SE1

  .....

- **Comment remplacer un switch d'une pile?**
- Tout d'abord, il est préférable que le switch qui va être ajouté ait une version d'IOS identique à celle des autres switchs de la pile.
  Pour remplacer un switch, il faut débrancher ce switch électriquement et l'enlever du stack.
  Ensuite le nouveau switch sera connecté à la pile, puis alimenté électriquement. Il récupère ainsi automatiquement la configuration du switch qui vient d'être retiré.

- **Retirer définitivement un switch d'une pile**
- Il faut tout d'abord débrancher le switch électriquement et enlever les cordons de stack.

  Lorsque le switch est retiré, la configuration concernant les ports de ce switch est toujours présente dans le fichier de configuration. Il faut donc supprimer cette partie de configuration du fichier.

  La séquence de commande suivante affiche les switchs appartenant à la pile (le switch 2 a été retiré). Puis, on affiche un extrait du fichier de configuration et on supprime le switch 2 du fichier de configuration.
  Enfin, on enregistre la configuration (il n'est pas nécessaire de redémarrer la pile).

```
switch-3750#show switch
Switch/Stack Mac Address : 0014.d8b2.3450
H/W Current
Switch# Role Mac Address Priority Version State
----------------------------------------------------------
*1 Master 0014.d8b2.3450 1 0 Ready
2 Member 0000.0000.0000 0 0 Removed

switch-3750#sh running-config | include provision
switch 1 provision ws-c3750-48p
switch 2 provision ws-c3750-48p

switch-3750#configure terminal
switch-3750(config)#no switch 2 provision
switch-3750(config)#^Z
switch-3750#write
Building configuration...
[OK]
```

- **Comment redémarrer un switch d'un stack?**
- La commande suivante redémarre le switch numéro 4:
  sw-3750#reload slot 4

- **Comment renuméroter le switch d'un stack?**
- La commande suivante renumérote le switch numéro 3 en switch numéro 2. Il faut ensuite redémarrer le switch.
  sw-3750(config)#switch 3 renumber 2

- **Comment désactiver le port stack d'un switch**
- La commande suivante désactive le port de stack numéro 2 du premier switch.
  sw-3750#switch 1 stack port 2 disable
  Enabling/disabling a stack port may cause undesired stack changes.
  Continue?[confirm]

- Pour réactiver ce port:
  sw-3750#**switch 1 stack port 2 enable**
  Enabling/disabling a stack port may cause undesired stack changes.
  Continue?[confirm]

- **Comment changer la priorité d'un switch dans le stack**
- Le switch qui a la priorité la plus haute devient le *master*. Le niveau de priorité va de 1 à 15. Le niveau le plus haut étant prioritaire.
  Commande pour modifier le niveau d'un switch puis vérification:
  sw-3750(config)#**switch 2 priority 15**
  Changing the Switch Priority of Switch Number 2 to 15
  Do you want to continue?[confirm]

  sw-3750#sh switch
  Switch/Stack Mac Address : 0024.d96d.e800
  H/W Current
  Switch# Role Mac Address Priority Version State
  ----
  *1 Master 0024.d96d.e800 1 0 Ready
  2 Member 0024.5e23.a290 15 0 Ready
  3 Member 0024.6256.0300 1 0 Ready
  4 Member 0024.2b25.4520 1 0 Ready

- Au prochain redémarrage du switch *master*, le switch 2 sera le *master*.

Commande de diagnostique

- **Comment afficher les switchs voisins?**
- Pour des raisons de sécurité, si nous n'utilisons pas cette fonctionnalité, il est préférable de désactiver les protocoles suivants.

CDP
Cisco se sert du protocole CDP (cisco discovery protocol) pour afficher les informations sur les voisins (en général d'autres commutateurs connectés). Il faut donc, pour que la commande fonctionne, que le protocole cdp soit activé sur les switchs.
La commande suivante active le protocole cdp puis affiche les voisins.

```
sw-3750(config)#cdp run
sw-3750(config)#end
sw-3750#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform Port ID
sw-2960 Gig 1/0/1 178 S I WS-C2960G Gig 0/
```

- **LLDP**
  Tout comme cdp, lldp (link layer discovery protocol) est un protocole qui permet d'échanger des informations avec les matériels voisins. Ce protocole est normalisé par l'IEEE (802.1ab).

  lldp est utilisé par de nombreux constructeurs. C'est donc le protocole à utiliser en cas de parc hétérogène.

  Activation du protocole lldp puis affichage des voisins:
  switch-3750(config)#lldp run
  switch-3750(config)#^Z
  switch-3750#show lldp neighbors
  Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

  Device ID Local Intf Hold-time Capability Port ID
  switch-hp Gi1/0/1 120 B 52

  Total entries displayed: 1

- Affichage des détails:
  switch-3750#
  switc-3750#show lldp neighbors detail

  Chassis id: 0025.b852.c4200
  Port id: 72
  Port Description: 1
  System Name: switch-hp

  System Description:
  ProCurve J9451A Switch 6600

  Time remaining: 97 seconds
  System Capabilities: B,R
  Enabled Capabilities: B
  Management Addresses:
  IP: 192.168.2.6
  Auto Negotiation - supported, enabled
  Physical media capabilities:
  1000baseX(FD)

  Total entries displayed: 1

  switc-3750#

- Désactivation de lldp
  switch-3750(config)#no lldp run
  switch-3750(config)#

- **Sans commentaire**
- sw-3750#ping
  Protocol [ip]:
  Target IP address: 192.168.1.1
  Repeat count [5]:
  Datagram size [100]:
  Timeout in seconds [2]:
  Extended commands [n]:
  Sweep range of sizes [n]:
  Type escape sequence to abort.
  Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
  !!!!!
  Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
  sw-3750#

- **Affichage des adresses Mac**
- sw-3750#sh mac address-table
  Mac Address Table

  .....
  Vlan Mac Address Type Ports
  ---- ----------- -------- -----
  100 0020.23a8.cafe DYNAMIC Fa2/0/20
  100 0020.12a7.bebe DYNAMIC Fa2/0/1

  ......

- **Mirroring d'un port**
- Le mirroring d'un port ou Cisco SPAN (Switched Port Analyzer) permet la copie des paquets d'un port vers un autre.

  Dans l'exemple:
  Le port en écoute porte le numéro 1 (interface source).
  Le port ou sera connecté le PC muni d'un analyseur de trame (wireshark par exemple) est le port 4 (interface destination)
  La session a le numéro 1.
  sw-2960(config)#monitor session 1 source interface fastEthernet 0/1
  sw-2960(config)#monitor session 1 destination interface fastEthernet 0/4

- Affichage des interfaces surveillées:
  switch#sh monitor Session 1

  Type : Local Session
  Source Ports :
  Both : Fa0/1
  Destination Ports : Fa0/4
  Encapsulation : Native
  Ingress : Disabled

- Désactivation du mirroring
  switch2(config)#no monitor session 1

- **Afficher les compteurs pour les interfaces**
- Switch#show interfaces counters

  Port InOctets InUcastPkts InMcastPkts InBcastPkts
  Fa1/0/1 0 0 0 0
  Fa1/0/2 0 0 0 0
  Fa1/0/3 0 0 0 0
  Fa1/0/4 0 0 0 0
  Fa1/0/5 91200 10 112 657
  Fa1/0/6 0 0 0 0
  Fa1/0/7 55738 8 121 413

- **Quelques informations sur le fonctionnement du système**
- Switch#show env all
  FAN is OK
  TEMPERATURE is OK
  SW PID Serial# Status Sys Pwr PoE Pwr Watts
  -- ----------------- --------- -------------- ------- ------- -----
  1 Built-in Good

  SW Status RPS Name RPS Serial# RPS Port#
  -- ------------ ---------------- ----------- ---------
  1 Not Present <>

  Switch#

Configuration du protocole ssh - switch Cisco

- Quel protocole choisir pour l'administration du switch, configuration du protocole ssh. Les commandes suivantes ont été testées sur des switchs série 3750 et 2960.

- **Quel protocole d'administration à distance choisir?**
- En général, il y a le choix entre l'administration web sécurisée ou pas (protocole http ou https) et/ou l'administration en ligne de commande sécurisée ou pas (telnet ou ssh).
  L'administration du switch en utilisant une interface web peut être pratique. Mais nous choisirons en priorité l'administration du switch en utilisant la ligne de commande pour les raisons suivantes:
- En cas de coupure réseau, il nous faudra intervenir directement sur le switch, donc autant être habitué à travailler en ligne de commande,
- L'interface web peut être moins stable que l'interface en ligne de commande (CLI),
- Les configurations avancées sont souvent disponibles uniquement au travers de la ligne de commande,
- Je vous laisse trouver d'autres arguments...
-

  Pour avoir un compte rendu graphique des objets du switch, nous nous tournerons vers une solution de supervision du réseau qui allie les avantages de la ligne de commande à une présentation graphique des objets du réseau. En général, ces logiciels fonctionnent grace au protole SNMP.

  Ainsi (revenons au sujet) les interfaces web seront désactivées.
  Il nous reste à choisir entre telnet et ssh. Le second étant nettement plus sécurisé que le premier, il est préférable (quand cela est possible) d'activer uniquement ssh sur le switch

- **Activation / désactivation des interfaces d'administration web**
- Les commandes suivantes active puis désactive l'administration web non sécurisée et sécurisée.
  2960-RG(config)#ip http server
  2960-RG(config)#ip http secure-server
  2960-RG(config)#no ip http server
  2960-RG(config)#no ip http secure-server

- **Configuration du protocole ssh pour le switch**
- Vérification de la prise en compte du protocole ssh par l'IOS
- Tout d'abord, il faut vérifier que l'IOS du switch supporte ssh. La mention k9 (crypto) doit figurer dans le nom de l'IOS.
  La commande pour vérifier la version de l'IOS est: 2960-RG#show version
  Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(55)SE, RELEASE SOFTWARE (fc2)
  Technical Support: http://www.cisco.com/techsupport
  Copyright (c) 1986-2010 by Cisco Systems, Inc.
  Compiled Sat 07-Aug-10 23:04 by prod_rel_team

- onfiguration du nom d'hote et du nom de domaine.
- Le nom du switch ainsi que le nom de domaine doivent avoir été configurés.
  Création de la clé
- 2960-RG(config)#crypto key generate rsa general-keys modulus 1024
  The name for the keys will be: 2960-RG.mondomaine.fr
  % The key modulus size is 1024 bits
  % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

  2960-RG(config)#
  *Mar 1 00:42:43.625: %SSH-5-ENABLED: SSH 1.99 has been enabled

- Activation de ssh
-

  RG-2960(config)#ip ssh version

- Options ajoutées au service ssh
- - les évènements associés aux connexions ssh sont enregistrés.
  - Un timeout de 60 secondes est ajouté pour les sessions ssh en cas d'inactivité .
  - Nous laissons trois essais pour la connexion au switch.

  clem(config)#ip ssh logging events
  clem(config)#ip ssh time-out 60
  clem(config)#ip ssh authentication-retries 3

- Ajout d'un compte administrateur
- clem(config)#username admin secret P@55w0rd

- Désactivation de telnet pour l'accès au switch
- clem(config)#line vty 0 15
  clem(config-line)#login local
  clem(config-line)#transport input ssh

- Vérification de la configuration
- 2960-RG#show ip ssh
  SSH Enabled - version 2.0
  Authentication timeout: 60 secs;
  Authentication retries: 3

- SSH est maintenant activé. nous pouvons accéder au switch avec un client ssh (par exemple putty pour windows).

- **Suppression de ssh**
- La suppression de la clé entraine la désactivation de ssh.
  2960-RG(config)#crypto key zeroize rsa
  % All RSA keys will be removed.
  % All router certs issued using these keys will also be removed.
  Do you really want to remove these keys? [yes/no]: yes
  2960-RG(config)#

- Vérification:
  2960-RG#sh ip ssh
  SSH Disabled - version 2.0
  %Please create RSA keys to enable SSH (of atleast 768 bits size) to enable SSH v2.
  Authentication timeout: 60 secs; Authentication retries: 3