Réseaux commutés

MIF21 - réseaux par la pratique

Univ. Claude Bernard Lyon 1

séances 2, 3 et 4

Fabien Rico fabien.rico@univ-lyon1.fr
Jacques Bonneville jacques.bonneville@univ-lyon1.fr
Olivier Glück Olivier.Gluck@univ-lyon1.fr

Objectifs du cours

Introduction

- Réseaux convergeants (données, voix, vidéo...)
- Besoin de fiabilité (redondance, sécurité, ...)
- Flexibilité (Modularité)

Hiérarchie dans le réseau

Cisco propose de définir le réseau local en 3 couches :

Définition (Cœur de réseau)

Le centre du réseau, composé par des switchs performant dont les seuls qualités sont la vitesse et la fiabilité. Il ne doit pas y avoir de manipulation de paquets dans cette zone.

C'est au cœur de réseaux que sont rattachés les routeurs de sortie du réseau et les commutateurs de la couche distribution.

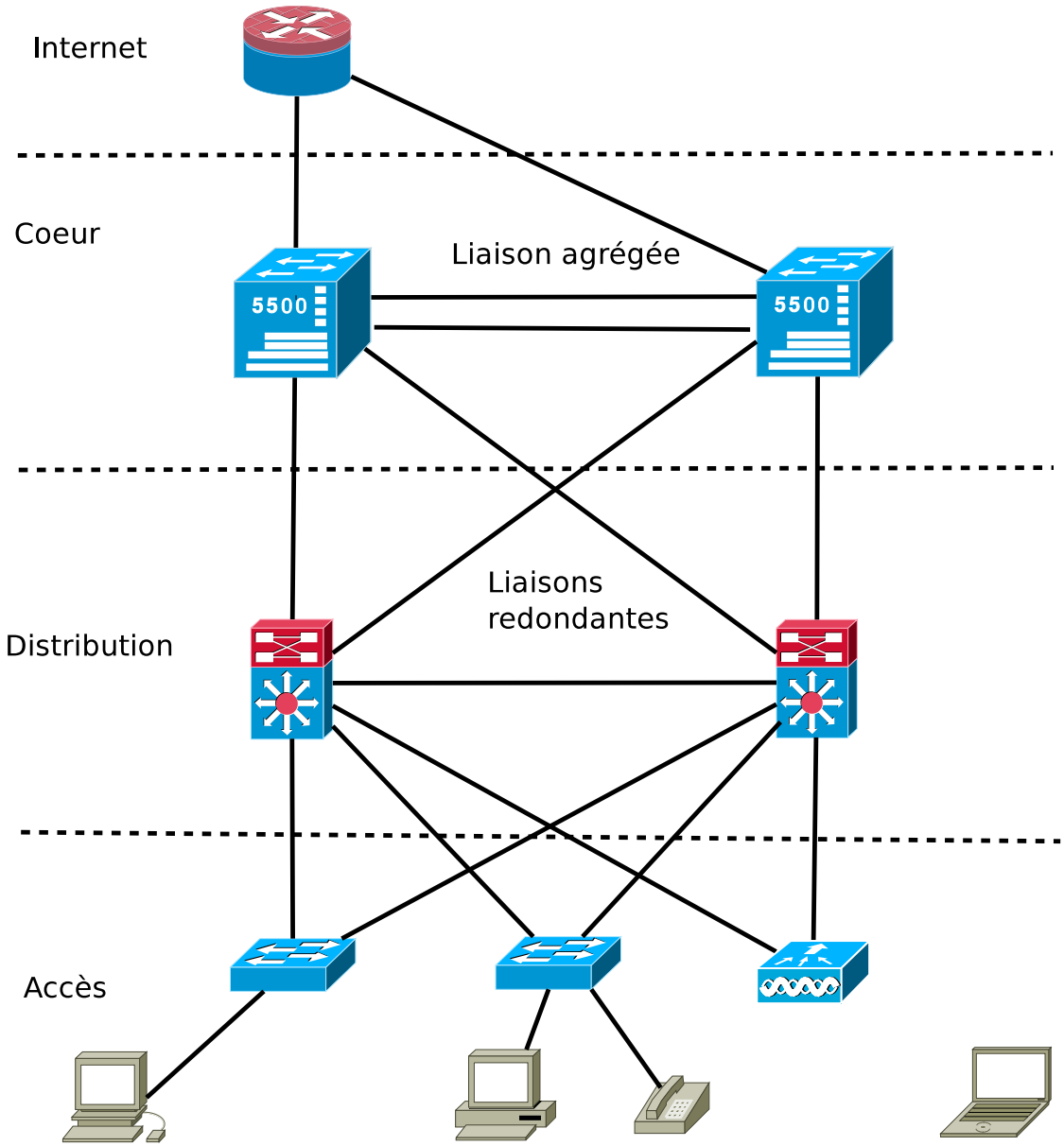
Définition (Couche de distribution)

Elle assure l'acheminement des paquets entre les différents vlans et sous réseaux. Elle est formée de switchs de niveau 3 et de routeurs. Elle s'occupe des filtrage, de la sécurité... On l'appelle aussi couche de groupe de travail.

Définition (Couche d'accès)

Ou couche de bureau, elle permet l'accès au réseau des équipements terminaux (ordinateurs, serveurs, ...).

Hierarchie dans le réseau



Interface de gestion d'un commutateur

Un commutateur peut être joint à distance via une adresse IP (et des accès, http, telnet ou ssh).

```
Switch(config)# interface vlan vlan-id
Switch(config-if)# ip address ip-address subnet-mask
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip default-gateway ip-address
Switch# show ip interface brief
Switch# show ip interface
```

Bien sur, il faut que le commutateur soit accessible dans ce vlan donc qu'il ait au moins un port dans ce vlan (voir plus loin). En général, le vlan par défaut est celui d'identifiant 1.

Configuration

- Configuration du mode privilégié

```
! Soit utilisation mode enable
Switch(config)# enable (password|secret) password
! Soit creation d'un utilisateur
Switch(config)# username nom privilege 0=rien à 15=admin secret mot de passe
```

- Via la console

```
Switch(config) # line console 0
Switch(config-line)# password password
Switch(config-line)# login [local]
Switch(config-line)# logging synchronous
```

- Via l'accès distant (voir ssh plus loin)

```
Switch(config)# line vty 0 15
Switch(config-line)# password password
Switch(config-line)# login [local]
Switch(config-line)# transport input (telnet ssh | ssh)
Switch(config)# service password-encryption
```

- Via l'interface web

```
Switch(config)# ip http authentication (enable|local)
Switch(config)# ip http server
Switch(config)# ip http secure-server
```

Dans tous les cas l'authentification `enable` signifie « avec le mot de passe enable », l'authentification `local` signifie « avec la base d'utilisateurs locaux » (via la commande `username`). `login` sans autre mention signifie avec le mot de passe définie via la commande `password`

Configuration des ports

Les ports peuvent être configurés séparément ou en groupes :

```
Switch(config)# interface type port
Switch(config)# interface range type port - port
```

Les commandes permettent de jouer sur le mode et la vitesse de transmission.

```
Switch(config-if)# duplex (auto | full | half)
Switch(config-if)# speed (auto | value-bps)
```

Normalement pour relier les appareils, certains types de câbles sont nécessaires (droits ou croisés). Comme pour les PC, il est possible de configurer un port pour détecter automatiquement la connexion.

```
Switch(config-if)# mdix auto
```

Les autres commandes, concernant les vlans et la sécurité, seront vues plus loin.

Domaine

Définition (Domaine de collision)

Un domaine de collision est une zone sur laquelle tous les équipements reliés parlent directement, il sont en concurrence et leur message peuvent se mélanger (collision). Il faut donc détecter ou prévenir les collisions.

Pour un commutateur, chacun de ses ports est dans un domaine de collision différents.

Définition (Domaine de diffusion)

C'est la zone dans laquelle une trame de diffusion peut être reçue. Cela représente tout le réseau local.

Un commutateur envoie une trame de diffusion (exemple découverte `DHCP`) à tous les ports sauf celui d'où elle provient.

Cheminement dans le domaine de diffusion

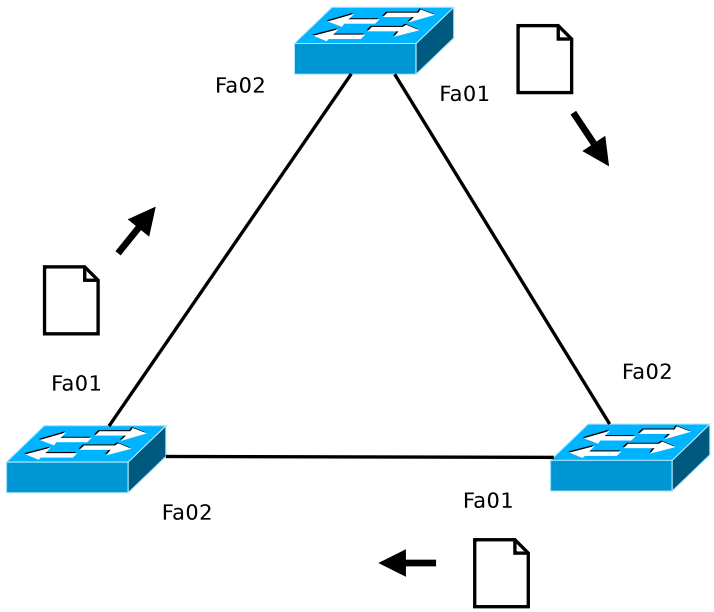
Les commutateurs relient les appareils du LAN en fonction de leur adresse de niveau 2 :

- pour décider vers quel port envoyer une trame, les commutateurs utilisent une table de correspondance @MAC/port la table *Content Addressable Memory* (CAM) ;
- le commutateur doit remplir sa table :
  - lorsqu'il reçoit une trame via un port il stocke son adresse d'origine ;
  - lorsqu'il reçoit une trame pour un destinataire inconnu, il l'envoie a tous les ports sauf celui d'origine.

```
Switch# show mac address-table
Switch(config)# mac address-table static MAC-addr vlan (1-4096 | ALL)
                                                    interface int-id
```

Tempête de *broadcast*

Si il y a plusieurs chemins dans le domaine, les trames de diffusions vont boucler.



Dans le shéma, une trame de diffusion reçue par le port `Fa02` est envoyée sur le port `Fa01` dans chaqu'un des commutateurs. Rien ne permet d'arreter cette diffusion qui va surcharger le réseaux.
Utiliser des *liaisons physiques redondantes* est une bonne chose, mais il faut un moyen de *supprimer automatiquement les cycles*.

Redondance et agrégations

Définition (Redondance)

La *redondance* consiste à doubler les équipements et les liaisons de manière à assurer le fonctionnement du réseau en cas de défaillance.

Par définition elle crée plusieurs chemins permettant d'aller d'un point à un autre :

- il n'y a pas de sécurité permettant d'éviter les boucles (ex : TTL) ;
- la table d'adresse MAC pourrait changer continuellement ;
- les tempêtes de broadcast consomment les ressources.

On doit donc *automatiquement désactiver certains ports de manière à assurer que le graphe des liaisons soit sans cycle*. Un nouveau calcul doit être fait à chaque modification des liaisons (activation d'un nouveau port).

Importance de la racine du l'arbre couvrant

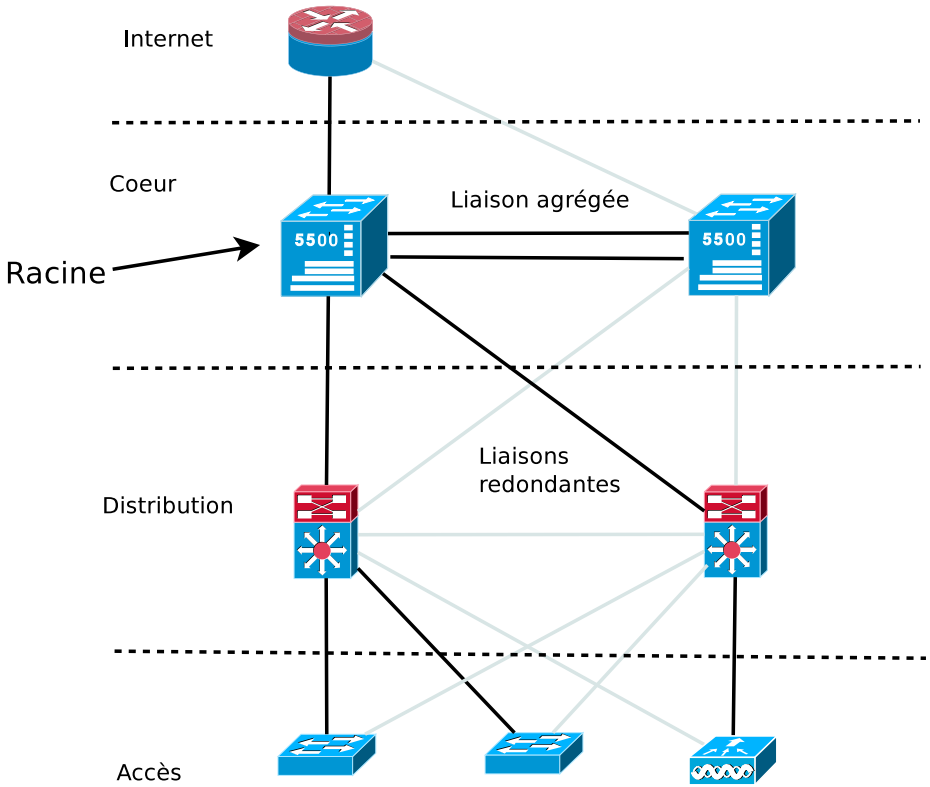


FIGURE: Version efficace

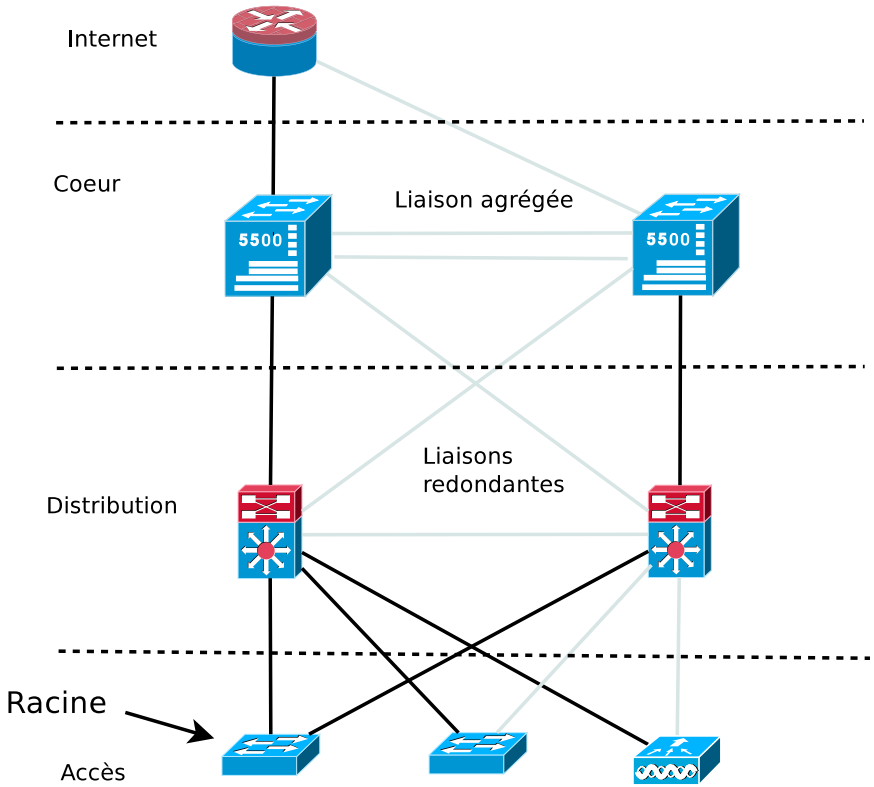


FIGURE: Version inefficace

L'algorithme STP s'assure qu'il n'y a pas de boucle dans le graphe logique des chemins, mais beaucoup de trafic va passer par sa racine.

Racine de l'arbre

Ce n'est pas du routage, les ports sont choisis en fonction du coût pour atteindre la racine, pas du plus court chemin pour atteindre un objectif.

- Le commutateur à la racine doit être efficace.
- Il faut prévoir un commutateur racine de remplacement en cas de défaillance.
- Voir plus via un système de priorités.

```
Switch(config)# spanning-tree vlan (vlan/vlan-range) root primary
Switch(config)# spanning-tree vlan (vlan/vlan-range) root secondary
Switch(config)# spanning-tree vlan (vlan/vlan-range) priority value
```

La plus petite valeur de priorité est préférée. En cas de priorité égale, c'est l'adresse MAC la plus faible qui permet de choisir la racine.
Utilisation du protocole *pvst* (per vlan spaning tree)

Rapidité de convergence

Le protocole stp peut mettre

du temps à converger, cela peut poser des problèmes (boot sur le réseau, ...)

- Définition d'un protocole plus efficace *rapid-pvst* :
  - ports *alternatifs ou discarding*, second meilleur chemin vers la racine ;
  - optimisation de la convergeance en cas de découverte d'un meilleur chemin vers la racine ;
  - type de port ;

```
Switch(config)# spanning-tree mode rapid-pvst
Switch(config)# interface type port
Switch(config-if)# spanning-tree link-type (point-to-point|shared)
Switch(config-if)# end
Switch# clear spanning-tree detected-protocols
```

- Les ports connectés à des équipements terminaux peuvent être immédiatement activés (la protection BPDU permet de desactiver le port en cas de réception de trame BPDU).

```
Switch(config-if)# spanning-tree portfast
Switch(config-if)#spanning-tree bpduguard enable
```

Type de port

```
Switch# show spanning-tree [(vlan vlanid | detail | summary | ...)]
```

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     0001.646A.E2E6
              Cost        38
              Port        2(FastEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.B0CA.24AA
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
```

- port racine (vers la racine) ;
- port alternatif (remplaçant en cas de défaillance du port racine) ;
- port designé (plus bas dans l'arbre) ;

Redondance/agrégation

- Redondance
  - STP désactive les ports redondants ⇒ la bande passante est perdue.
  - On peut utiliser plusieurs types de lien pour la redondance.
  - Redondance de lien et de chemin.
- Agrégation
  - L'agrégation permet de répartir la charge sur plusieurs liens.
  - Limité à des liens de type identique entre 2 commutateurs.
  - Limité à 6 liaisons agrégées d'au plus 16 ports.
  - Si un lien physique tombe, les autres prennent le relai automatiquement.

Protocoles

- PAgP (prop. Cisco) : Protocol Agrégation Port
  - *mode on* : entre directement en agrégation ;
  - *mode desirable* : demande si le port de l'autre coté accepte de participer
  - *mode auto* : accepte de participer mais n'initie rien.
- LACP (ouvert) : Link Agregation Protocol
  - *mode on* : entre directement en agrégation ;
  - *mode active* : demande si le port de l'autre coté accepte de participer
  - *mode passive* : accepte de participer mais n'initie rien.

Les modes doivent être compatibles pour que cela fonctionne : active/passive, desirable/auto, on/on, ...

Configuration

- Choisir la méthode de répartition

```
Switch(config)# port-channel load-balance [dst-ip|dst-mac|src-dst-ip|src-dst-mac|src-ip|src-mac]
```

- Configurer les ports (sur les 2 commutateurs)

```
! on peut faire une configuration par lot
Switch(config)# interface range fa0/1 - 4
Switch(config-if-range)# channel-group 1-6 mode (on|active|passive|desirable|auto)
Switch(config-if-range)# exit
```

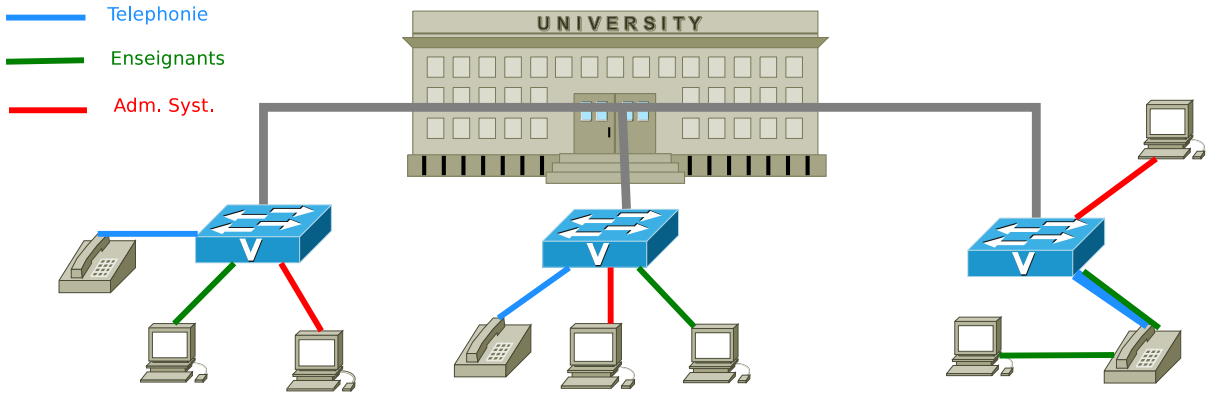
- La commande précedante crée une interface ≪ port-channel ≫ qu'il faut configurer

```
Switch(config)# interface port-channel 1
Switch(config-if)# description liaison agrégée vers ...
Switch(config-if)# ...
```

- Vérification de la configuration

```
!!! afficher les infos de l'interface virtuelle Port-channel
Switch# show interface Port-channel
!!! afficher les interfaces physiques utilisant etherchannel
Switch# show interfaces etherchannel
!!! afficher des informations sur etherchannel
Switch# show etherchannel [summary|port-channel]
```

Vlan



Les différents services peuvent êtres mélanger physiquement, pour séparer leurs réseaux il faudrais multiplier les liaisons.

- Les commutateurs sont capables de faire une séparation logique : les *réseaux locaux virtuelles* ;
- moins couteux ;
- plus souples.

Utilisation des vlan

- Les vlan peuvent être attribués dynamiquement (wifi/radius).
- Les ports d'accès sont souvent attribués à un vlan.
- Les liaisons entre commutateurs doivent transmettre plusieurs vlans
  - vlan autorisés ;
  - vlan natif ;
- Certains vlans ont un rôle particulier :
  - vlan par défaut (vlan 1) ;
  - vlan de gestion (celui utilisé par les interfaces des commutateurs).
- Il y a possibilité de numéroter 4096 vlans :
  - de 1 à 1005 la plage normale, gérée par VTP et le fichier vlan.dat ;
  - de 1002 à 1005 plage non utilisable avec ethernet ;
  - de 1006 à 4096 la plage étendue non gérée par VTP et dans le fichier de configuration normal.

Création d'un vlan

Un vlan doit être actif pour être utilisé.

- Création

```
Switch(config)# vlan vlanid
Switch(config-vlan)# name nom
```

- Affichage

```
Switch# show vlan [brief | id vlanid | name nomvlan]
Switch# show interfaces [interfaceid | vlan vlanid
                                     | switchport]
```

- Avant de partir **ne pas oublier**

```
Switch# delete flash:vlan.dat
```

Protocole VTP

C'est un protocole CISCO permettant de transmettre la déclaration des vlans sur tous les commutateurs.

```
Switch(config)# vtp mode (server | client | transparent)
Switch(config)# vtp domain domain-name
Switch(config)# vtp password password
Switch(config)# vtp version (1 | 2)
Switch(config)# vtp pruning
Switch# show vtp status
Switch# show vtp counters
Switch# show interfaces trunk
```

Et surtout ne pas oublier

```
Switch# delete flash:vlan.dat
```

Port d'accès

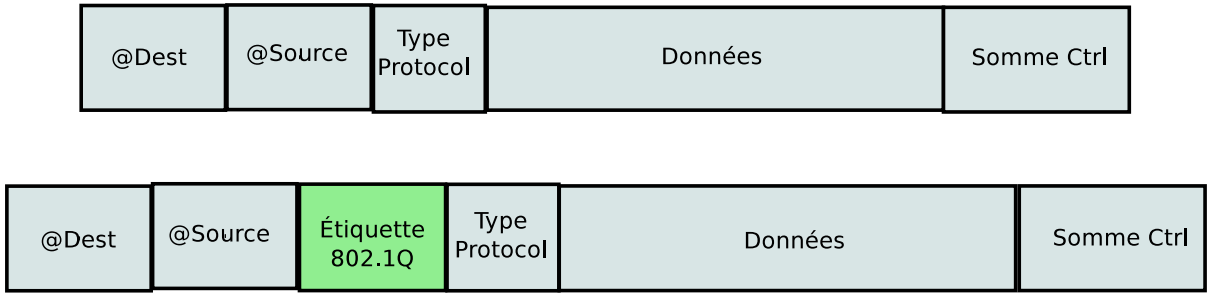
Pour les équipements terminaux, les vlans dépendent du port utilisé

```
Switch(config)# interface type port
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan vlan-id
```

- Le vlan sera transparent pour les équipements branchés sur ces ports.
- Si le vlan est désactivé, le ports n'est plus utilisable.

Port trunk

Pour les liaisons, multiplexées, il faut un moyen de différencier les vlans.



La version utilisée est IEEE 802.1Q.
Les trames ethernet sont modifiées pour ajouter une étiquette de vlan contenant :

- identifiant de protocole (16bits, 0x8100 pour 802.1Q) ;
- priorité (3 bits) ;
- Canonical Format Identifier (1 bits) pour compatibilité avec tokenRing ;
- Identifiant de vlan (12bits).

Configuration

```
Switch(config)# interface type port
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan vlan-id
Switch(config-if)# switchport trunk allowed vlan vlan-id
                                              [,vlan-id,vlan-id...]
Switch(config-if)# switchport trunk allowed vlan add vlan-id
Switch# show interfaces id-interface switchport
Switch# show interfaces trunk
```

Attention :

- Le vlan natif est le vlan des trames sans étiquette, il doit être le même des 2 cotés.
- « `allowed vlan add` » ajoute un vlan, « `allowed vlan` » remplace tous les vlans existant *ne pas confondre*.

Dynamic Trunking Protocol

Pour configurer les port on peut utiliser un protocole propriétaire CISCO

```
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport mode dynamic auto
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# switchport nonegociate
Switch# show dtp interface type port
```

`auto` et `desirable` ont le même sens que pour etherchannel (desirable initie la négociation, auto l'accepte).
C'est une configuration par défaut, attention à la sécurité !

Routage inter-vlan

Les vlans servent à séparer les réseaux. Il faut pouvoir passer de l'un à l'autre.

- On peut utiliser un routeur avec plusieurs interfaces physiques : ancienne méthode.
- On peut utiliser un routeur avec une seule interface physique : *Router-on-a-stick*.
- On peut utiliser un commutateur de niveau 3 via les *Switch Vlan Interface*.

Router on a stick

- une seule interface physique du routeur ;
- configuration de sous interfaces ;
- utilisation du trunk et de l'encapsulation 802.1Q.

```
Router(config)# interface type interface-number
Router(config-if)# no shutdown
Router(config)# interface type interface-number.subinterface-number
Router(config-subif)# encapsulation dot1q vlan-id [native]
Router(config-subif)# ip address ip-address subnet-mask
```

Il faut que le vlan natif corresponde avec celui du commutateur qui est relié à cette interface.

Exemple router on a stick

Il y a les vlan 2 (10.0.2.0/24) et 3 (10.0.3.0/24). Le 2 est vlan natif.

```
Router(config)# interface Fa 0/1
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface Fa 0/1.2
Router(config-subif)# encapsulation dot1q 2 native
Router(config-subif)# ip address 10.0.2.0 255.255.255.0 Router(config)#
interface Fa 0/1.3
Router(config-subif)# encapsulation dot1q 3
Router(config-subif)# ip address 10.0.2.0 255.255.255.0
```

Routage par commutateur

On peut utiliser les commutateurs multicouches

- plus rapide car effectuée matériellement ;
- pas de liaisons avec un routeur (via une liaison limitée) ;
- latence plus faible.

Cela n'est possible qu'avec certains type de commutateur : Catalyst 3560, 4500 et 6500.

Configuration

- Il faut activer le routage

```
Switch(config)# ip routing
```

- et une interface pour chaque vlan à router

```
Switch(config)# interface vlan 2
Switch(config-if)# ip address 234.15.2.1 255.255.255.0
Switch(config-if)# no shutdown
```

```
Switch(config)# interface vlan 3
Switch(config-if)# ip address 234.15.3.1 255.255.255.0
Switch(config-if)# no shutdown
```

Sécurisation du réseaux

Différents type d'attaques

- virus, vers, chevaux de troie ;
- attaques « psychologique » ;
- attaques par reconnaissance ;
- attaques par accès ;
- Denis de service.

Sécurité des accès

- Les mots de passe d'accès console et vty ne peuvent pas être crypté efficacement `service password-encryption` n'est pas sécurisé. Il faut utiliser les utilisateur locaux l'authentification aaa.

```
Switch(config)# username login privilege 0-15
secret mot-de-passe
Switch(config)# line vty 14 15
Switch(config-line)# login local
```

- Il faut appliquer une politique de sécurité sur les mots de passe

```
Router(config)# security password min-length 8
Switch(config)# login block-for tempsDeBlocage
attempts nbDeTentatives within intervalleDeTemps
```

Le second permet d'éviter les attaque en force brutte en bloquant l'accès après un petit nombre de tentatives échouées pendant un cours laps de temps.

Sécurité des accèes

Il faut réserver certaines lignes telnet à des accès spéciaux en cas de problème et penser au ACL dans ce cas (voir plus loins)

```
Switch(config)# username root privilege 15 secret
cisco
Switch(config)# line vty 0 13
Switch(config-line)# exec-timeout 10
Switch(config-line)# password motDePasseNonSecurise
Switch(config-line)# login
Switch(config)# line vty 14 15
Switch(config-line)# exec-timeout 10
Switch(config-line)# login local
```

Configuration de SSH

Telnet est un protocole peu sécurisé, les version récente d'IOS permettent d'utiliser ssh pour la connexion

- Pour cela il faut avoir un domaine par défaut

```
Switch(config)# ip domain-name nomdedomain.fr
```

- générer une clef pour que le serveur s'authentifie

```
Switch(config)# crypto key generate rsa
```

- utiliser un login/mot de passe et imposer ssh pour l'accès vty

```
Switch(config)# username root privilege 15 secret
cisco
Switch(config)# line vty 0 15
Switch(config-line)# transport input ssh
Switch(config-line)# login local
```

- Pour les vérifications

```
Switch# show ip ssh
Switch# show ssh
```

Attaques

- Attaque par inondation mac :
  - un pirate crée de fausse trame avec des adresses mac fictives,
  - la table mac des switch est remplie et il ne peuvent pas stocker les correspondances @/ports,
  - pour acheminer une trame légitime, le commutateur doit inonder ses ports,
  - le commutateur devient un concentrateur.
- Attaque par usurpation dhcp :
  - DHCP est le protocole permettant d'attribuer automatiquement une configuration réseaux,
  - un pirate installe un faut serveur dhcp,
  - il configure les route par défaut pour détourner les paquets.
- Utilisation de cdp
  - cdp est un protocole cisco pour simplifier les configuration (ex incohérence entre trunk)
  - il permet d'intérroger les switch du voisinage pour obtenir des informations.

Sécurité MAC

- On peut limiter le nombre d'addresse mac qui sont associée à un port

```
Switch(config)# interface Fast 0/1
Switch(config-if)# switchport mode access vlan idVlan
Switch(config-if)# switchport port-security maximum nbAdrMax
```

- On peut fixer les adresses ou les apprendre dynamiquement

```
Switch(config-if)# switchport port-security mac-address H.H.H
Switch(config-if)# switchport port-security mac-address sticky
```

- Et il faut choisir la réaction si le nombre maximum est atteint

```
Switch(config-if)# switchport port-security violation
                                    (protect|restrict|shutdown)
```

`protect` ne laisse pas passer les trames, `restrict` génère en plus un log et `shutdown` éteint le port qui doit être réactivé.

- Vérification de la sécurité

```
Switch# show port-security interface type port
```

Sécurité DHCP

- Il faut démarrer la surveillance DHCP

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan vlanId-ou-Range
```

- Marquer les ports vers le serveur DHCP

```
Switch(config)# interface Fast 0/1
Switch(config-if)# ip dhcp snooping trust
```

- Et celle qui ne doivent pas transmettre de requête ou de réponses DHCP

```
Switch(config)# interface range Fast 0/2 - 24
Switch(config-if)# ip dhcp limit rate nbPacket/Seconde
```

A faire en plus

- Ne pas activer CDP sur les interface d'accès

```
Switch(config-if)# no cdp enable
```

- Activer la protection bpdu sur les ports d'accès

```
Switch(config-if)# spanning-tree bpduguard
```

- Désactiver la négociation DTP sur les port trunk

```
Switch(config-if)# switchport nonegociate
```