

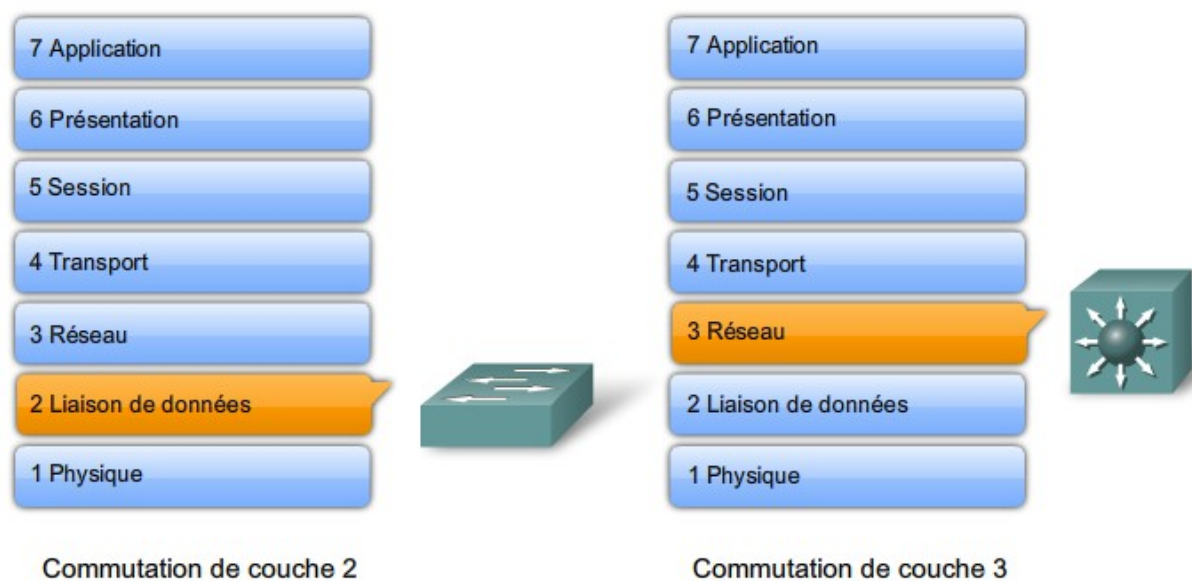
Les concepts de commutations

vue globale de l'environnement des switchs Coeur, Distribution et accès



La principale différence entre la gamme PRO et SMB – small business - réside dans la cohabitation des logiciels de supervisions, CISCO PRIME pour la gamme pro qui est beaucoup plus poussé pour la gestion des infrastructures.

Différence entre « switch d'accès niveau 2 » et « switch distribution niveau 3 »



switch de couche 2 / switch d'access

Effectue une commutation et filtrage en se basant sur les adresses MAC – **couche liaison de donnée** du modèle **OSI** (open system interconnexion), il est transparent pour les protocoles réseau et applications des utilisateurs, il génère une **table MAC ou CAM**, les switch d'accès sont utilisés pour **connectés les PC**

```
DLS1#show mac address-table
      Mac Address Table
-----

```

Vlan	Mac Address	Type	Ports
1	0001.c740.6601	DYNAMIC	Fa0/1
10	0001.c740.6601	DYNAMIC	Fa0/1
30	0001.c740.6601	DYNAMIC	Fa0/1
99	0001.963a.b602	DYNAMIC	Fa0/2
99	0001.c740.6601	DYNAMIC	Fa0/1
99	0060.2fb5.9903	DYNAMIC	Fa0/3

switch de Layer 3 – switch de distribution

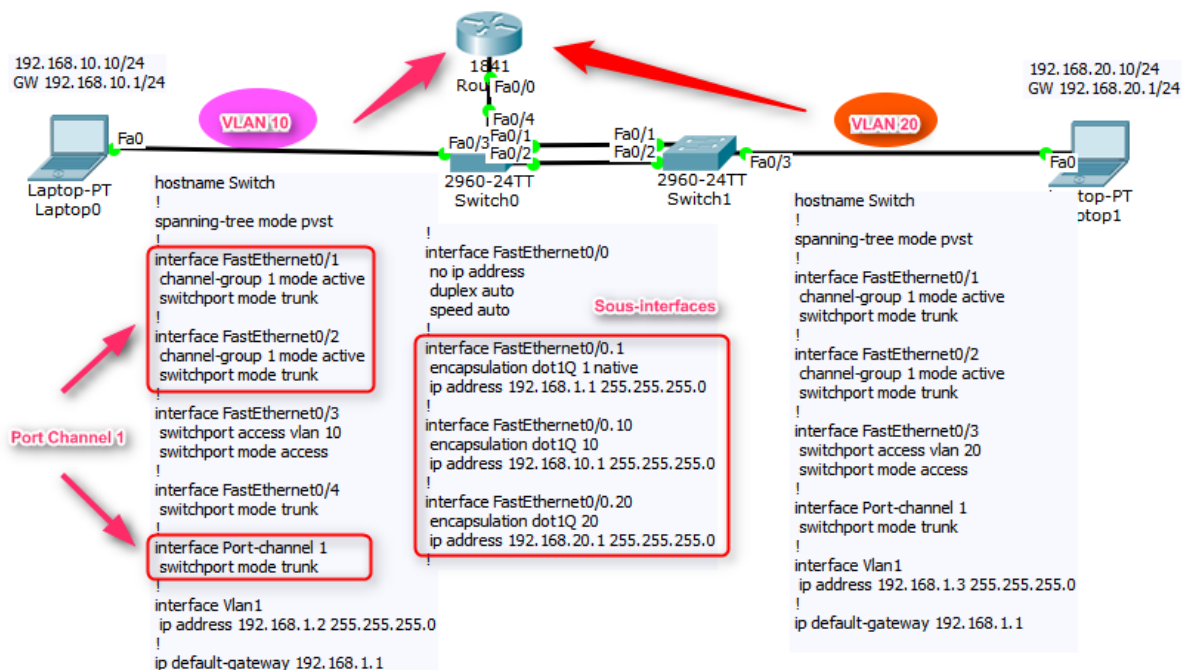
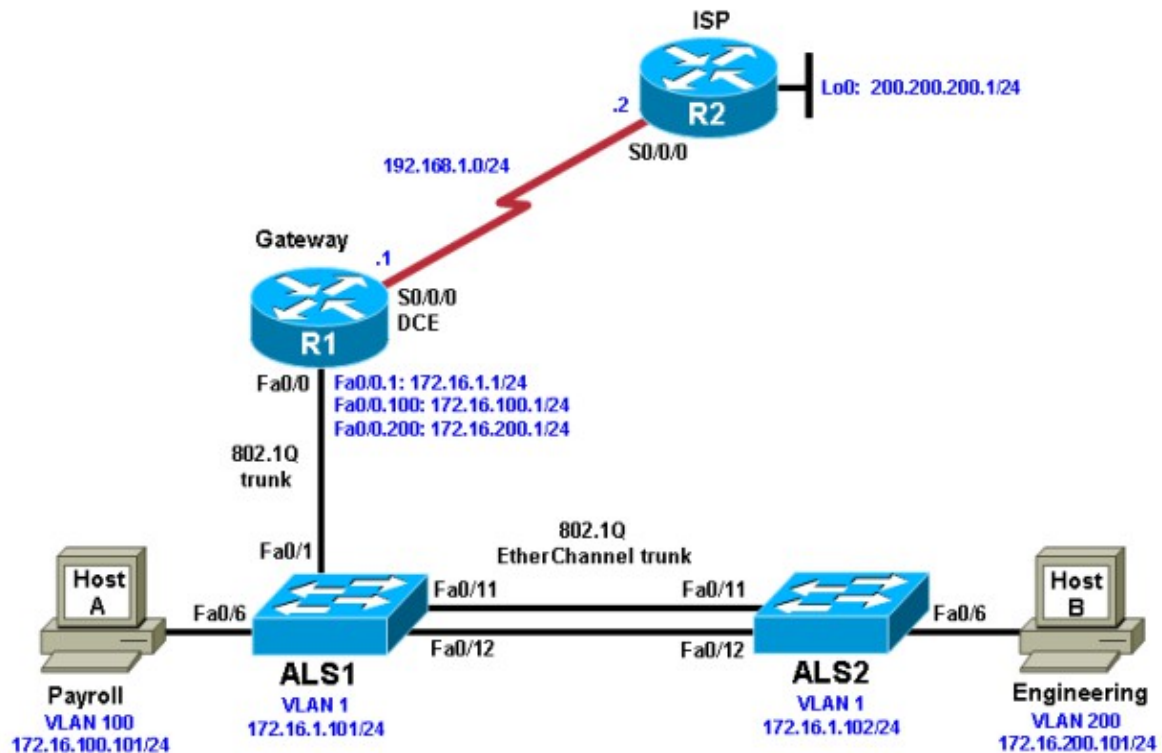
ils exécutent une **fonction de routage** qui permettra de faire du **routage inter-vlan** et filtrage grâce a des **RACL** – **filtre sur les interfaces VLAN SVI** et **VACL** - **filtrage a l'intérieur des vlans**

```
DLS1#sh ip rou
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

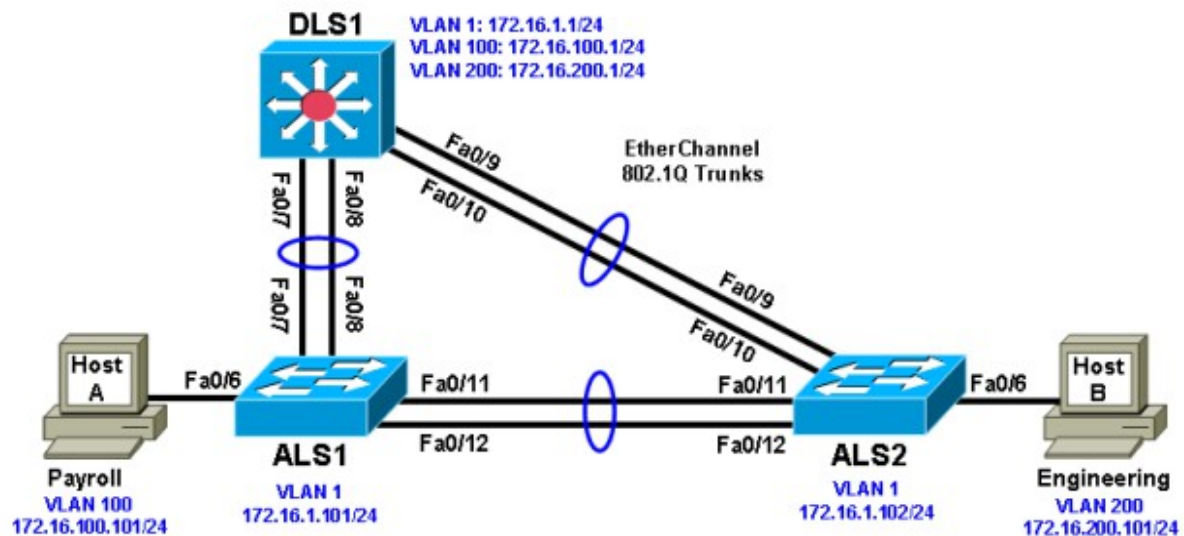
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 4 subnets
C      172.16.1.0 is directly connected, Vlan1
C      172.16.100.0 is directly connected, Vlan100
C      172.16.150.0 is directly connected, Vlan150
C      172.16.200.0 is directly connected, Vlan200
```

Topologies d'entreprises n'utilisant que des switch de niv 2 – routage inter-vlan via un routeur



Topologies d'entreprise utilisant des switch de niveau 3 – routage inter-vlan via un switch de distribution



1 - La Latence

Définition:

Le temps mis par une trame/paquet pour aller et venir entre la station d'origine et la destination finale sur le réseau.

Calcul du temps de latence :

Délai carte réseau:

le temps nécessaire à la carte réseau d'origine pour placer des impulsions électriques sur le fil et le temps nécessaire à la carte réseau réceptrice pour interpréter ces impulsions. De l'ordre d'une microseconde.

Délai propagation:

déplacement du signal sur le fil (0,556 microseconde pour 100 mètres de câble UTP de catégorie 5).

Délais unités couches 1, 2 ou 3:

temps de latence du réseau de l'émetteur vers le récepteur en passant par les « **commutateurs et routeurs** ».

Calcul du temps de transmission de différentes trames

Un bit doit avoir une période minimale pendant laquelle il reste «ouvert» ou «fermé» , pour qu'ils soit reconnu par tous les supports optique ou électronique en chiffre numérique 1 ou 0 binaire. ".

La durée d'un bit est de l'ordre 100 ns pour Ethernet 10 Mbits/s

temps de transmission en microsecondes = lg_trame en Octet * 8_bits * 100ns / 1000

Taille d'un trame (Octet)	Temps de transmission (microseconde)
64	51,2
512	410
1000	800
1518	1214 microsecondes

2 - Les Hub / concentrateur - niv 1

Éléments de couche 1 qui **régénèrent** le signal avant de le **transmettre a tous ces ports** sauf sur celui sur lequel il l'a reçu . Il possède un nombre de **ports 4,8,16 ou 32**. Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble de autres ports, il est aussi appelé **répéteur multiports**, il permet aussi de passer d'un média a un autre (cuivre vers optique par exemple)

On distingue 2 catégories de concentrateurs

Les concentrateurs « actifs » , ils sont **alimentés électriquement** et permettent de régénérer le signal sur les différents ports

Les concentrateurs dits « passifs », ils ne permettent que de diffuser le signal a tous les hôtes **sans régénération du signal**

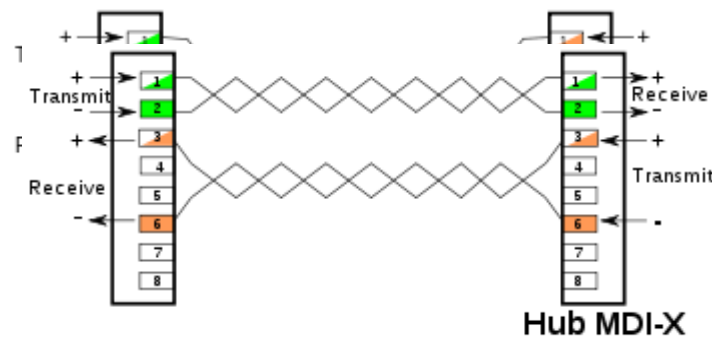
Connexions de plusieurs Hub

Les concentrateurs sont dotés d'un **port UP-LINK** permettant d'utiliser **un câble droit** pour connecter **2 hub ensemble**.

L'option **Auto-MDIX** permettra aux interfaces du hub de détecter si la connexion exigerait un **câble droit** ou **croisé** et choisira automatiquement son mode

Connexion de 2 hub sans ports UP-LINK – utilisation d'un câble croisé

Connexion de 2 hub sans ports UP-link – utilisation de l'option Auto MDI-X avec un câble droit



Les Hub augmentent les **domaines de collisions niv 1** (géré par le CSMA/CD) et de broadcast ARP niv 2



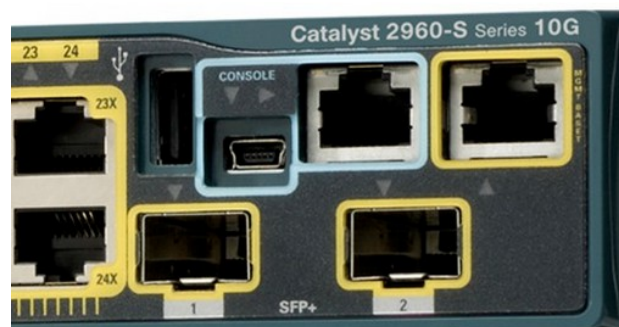
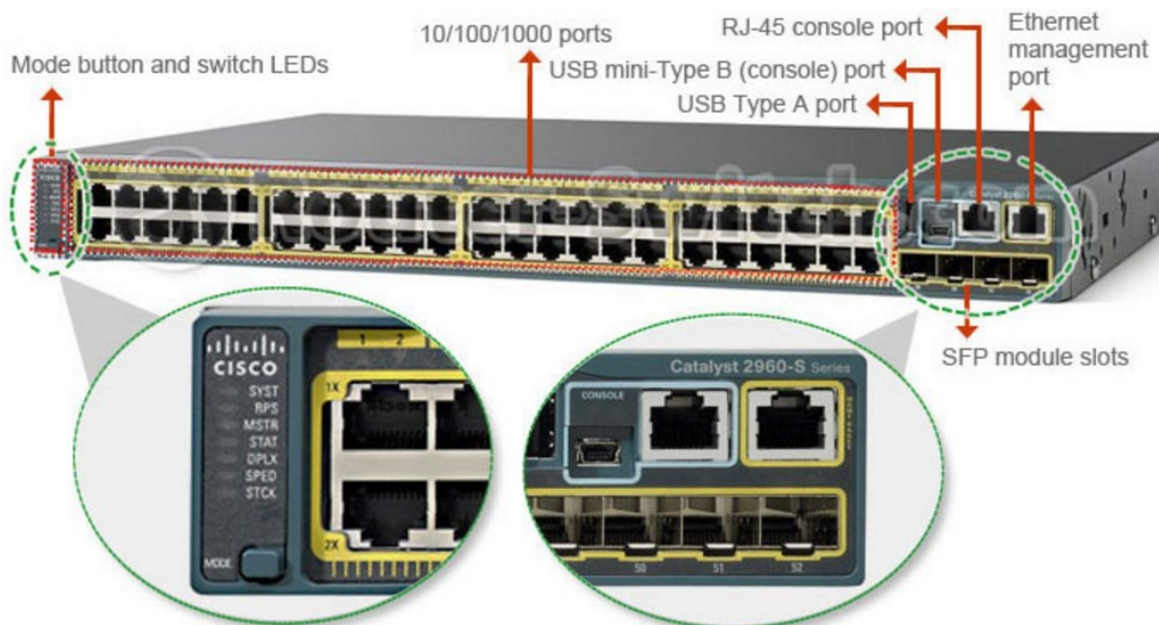
Cisco Small business SF 100-24 24-port 10/100 switch

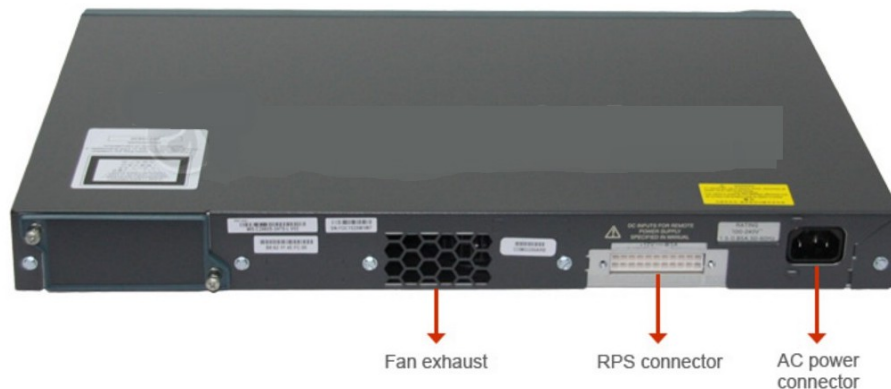
L'utilisation des Hub industriel est utilisé dans le monde industriel pour interconnecter des machines outils.
En entreprise on l'utilisera dans les salles de réunions pour un accès direct a internet via un switch de distribution.

3- Le commutateur

Un commutateur est un équipement dit « intelligent », le commutateur a la capacité d'analyser et gérer le trafic, il gère les adresse MAC par l'intermédiaire de sa table CAM.

SWICH 2960-S



Face arrière**Power Supply**

Les commutateurs Catalyst 2960-X possèdent une alimentation fixe et la possibilité d'ajouter en option un mécanisme externe d'alimentation électrique redondant – **RPS2300** – appelé **Power Supply**

Les 2960-XR supportent 2 alimentations électriques redondantes, une alimentation étant fournie par défaut et la deuxième doit être commandée. Chaque alimentations disposent de ventilateur intégrés avec leur propre refroidissement.

**POE - Intelligent Power over Ethernet Plus**

Le POE permet de supprimer les prises de courant d'alimentation des terminaux.

Les 2960-X supportent les standards **IEEE 802.3af Power over Ethernet – POE** et **IEEE 802.3at POE+** qui supportent jusqu'à 30 watt par port pour les déploiements qui intègrent des téléphones IP Cisco, des points d'accès WIFI Aironet, ou d'autres terminaux supportant les standards POE/POE+.

Les normes

IEEE 802.af – POE : l'alimentation électrique fournie par l'équipement commutateur ou injecteur est **15.4Watts au maximum et la tension est de 48Volts**

IEEE 802.at – POE + : est capable de fournir entre **24 et 30 Watts pour une tension de 48Volts**

Le courant passant par le câble ethernet est étant constitué de 4 paires de fils, quand on a une connexion a 100 Mbits, les données transitent sur une paire seulement via les fils 1 2 3 6, les 2 autres paires 4 5 7 8 seront utilisées pour transmettre le courant électrique.

Dans le cas ou le switch ne peut distribuer du POE, on utilisera des **injecteurs ou adaptateur POE** entre le port du switch et l'équipement terminal

Les ports fastethernet Full-Duplex- niv 2

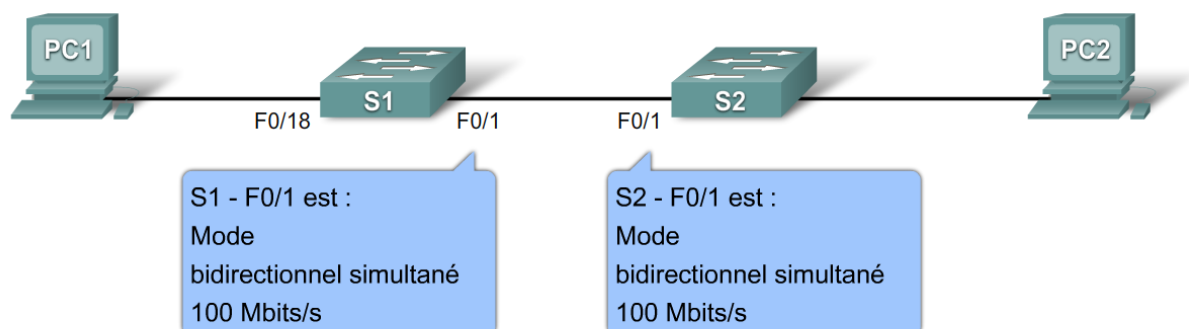
Le commutateur utilise deux paires de fils du câble, en faisant l'établissement d'une connexion directe entre l'émetteur (TX) et le récepteur (RX), générant un domaine sans collision et offrant un débit de 100% de la bande passante dans les deux sens.

Pour un débits de 100Mbps/s en utilisant un commutateur Ethernet full duplex on obtiendra un débits de 200Mbps/s – 100Mbps/s en émission et 100Mbps/s en réception.

Détail sur un ports switch – couche 1 et 2 - Ethernet

```
S2#show interfaces fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 00e0.f73e.b701 (bia 00e0.f73e.b701)
  BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
```

configuration du mode bidirectionnel et vitesse des ports



Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	S1# configure terminal
Passer en mode de configuration d'interface.	S1(config)# Interface fastethernet 0/1
Configurer le mode bidirectionnel d'interface pour activer la configuration bidirectionnelle automatique.	S1(config-if)# duplex auto
Configurer la vitesse bidirectionnelle d'interface et activer la configuration de vitesse automatique.	S1(config-if)# speed auto
Revenir au mode d'exécution privilégié.	S1(config-if)# end
Enregistrer la configuration en cours dans la configuration de démarrage du commutateur.	S1# copy running-config startup-config

Le ports SFP - Small form-factor pluggable

Il est un **émetteur récepteur compact, insérable à chaud**, il interface la carte mère d'un équipement réseau (switch/routeur) à une **fibre** ou **câble de cuivre**. Il est conçu pour supporter les technologies **Gigabit ethernet** et **fiber channel**. Il rend obsolète l'ancien et très répandu gigabit interface converter GBIC, il est appelé **mini-GBIC**. Il sera vu en mode CLI en tant qu'interface **gigabitethernetX/X**

Le port SFP+ - enhanced small form-factor pluggable

Le SFP+ est une version améliorée de SFP. Il garde le même format, mais il supporte un débit de données plus élevé, jusqu'à **10 Gigabit/s**, en mode CLI en tant qu'interface **tengigabitethernetX/X**, limitant les agrégats de liens fibre ou cuivre de 2*10 gigabitethernet0 qui sont utilisés entre les switch d'accès et distribution, les prix n'étant pas les mêmes.

Les transceivers SFP sont disponibles avec de nombreux type d'émetteur récepteur.

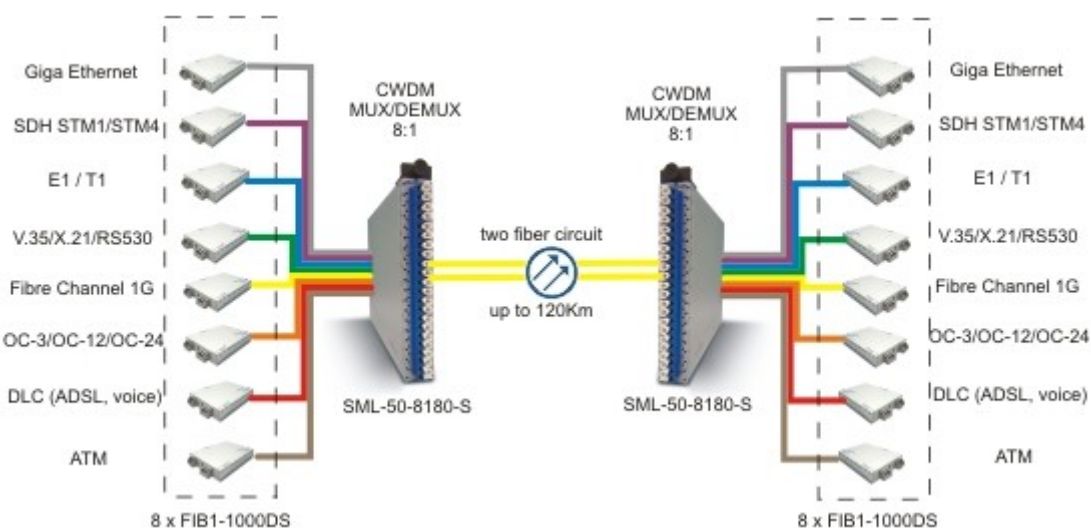
Tranceivers pour les « fibres multimode (led) », avec une levier d'extraction noir ou beige.

•**SX** - 850 nm, pour un maximum de **550 m** a **1.25 Gbit/s** (Gigabit Ethernet) ou **150m** a **4.25 Gbit/s** (Fibre Channel)

Tranceivers pour les « fibres monomode (lazer) », avec un levier d'extraction bleu

- LX** - 1310 nm, pour une distance jusqu'à **10 km**
- EX** - 1310 nm, pour une distance jusqu'à **40 km**
- ZX** - 1550 nm, pour une distance jusqu'à **80 km**
- EZX** - 1550 nm, pour une distance jusqu'à **120 km**
- BX** - 1490 nm/1310 nm, SFP gigabit sur un brin de fibre Bi-Directionnelle , sur deux brins fibre avec BS-U et BS-D pour respectivement la montée et la descente, avec une distance jusqu'à 10km.
- 1550 nm 40 km (XD), 80 km (ZX), 120 km (EX or EZX)

•**CWDM et DWDM**, transceivers à plusieurs longueurs d'ondes permettant d'atteindre les distances les plus élevées, **utilisés par les Opérateurs pour les liaisons inter-NRA et POP, ou liaisons entre les centre de peering**



Tranceivers Pour câblage en paire de cuivre torsadées.

- 10Base-T** - ce module permet d'atteindre 10 Mb/s sur 2 paires de cuivre.
 - 100Base-TX** - ce module permet d'atteindre 100 Mb/s sur 2 paires de cuivre.
 - 1000Base-T** - ce module permet d'atteindre 1 Gigabit/s sur 4 paires de cuivre.
 - 1000Base-TX** - ce module permet d'atteindre 1 Gigabit/s sur 2 paires de cuivre de catégorie 6
- Le SFP contient un circuit imprimé qui s'enfiche dans le connecteur électrique du slot SFP dans le système hôte.

SFP pin-out

Pin	Function	Pin	Function
20	VeeT	1	VeeT
19	TD-	2	TxFault
18	TD+	3	TxDisable
17	VeeT	4	MOD-DEF(2)
16	VccT	5	MOD-DEF(1)
15	VccR	6	MOD-DEF(0)
14	VeeR	7	RateSelect
13	RD+	8	LOS
12	RD-	9	VeeR
11	VeeR	10	VeeR

MOD-DEF 0,1,2 sont les pins de définition de mode.

- MOD-DEF 0 est mis a la masse pour indiquer que le module est présent.
- MOD-DEF 1 est la patte d'horloge SCL pour le Bus I²C de l'EEPROM d'identification
- MOD-DEF 2 est la patte data SDA pour le bus I²C de l'EEPROM d'identification

Le stack

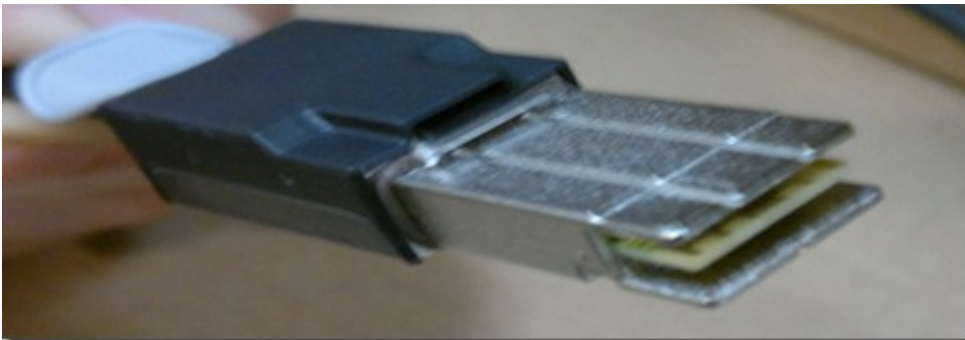
Les switch stackable chez cisco sont la gamme des Cisco Catalyst 2960-X Series Switches comme le WS-C2960X-48FPD-L et switch de layer 3 type 3750 et 3650, ils possèdent un emplacement pour intégrer une carte stack de référence – C2960X-STACK : Catalyst 2960-X FlexStack Plus Stacking Module- le système est appelé Flexstack.



Module stack



cable stack référence - CAB-STK-E-0.5M Cisco FlexStack 50 cm stacking cable, existe en 1 mètre



Les ports que l'on utilisera **entre les switches d'une pile** sont les ports stackwise qui ont un débit suivant le matériel d'un peu près **32 Gigabit/s Ethernet et plus**.

Sur le principe du câblage en croise d'un switch l'autre switch du port 1 au port 2 de l'autre switch idem pour les switch d'extrémités

Pourquoi utiliser le stack :

Le débit/bande passante entre les switchs sera supérieur à 32 Gbits/s contre 1 ou 10 Gbits en façade via les ports uplink SFP et SFP+ que l'on pourra étendre à 8 liens physique maximum en etherchannel.

On pourra administrer la pile de switch via une seule adresse IP par le vlan d'administration

Comment ce passe la numérotation des ports :

Les ports du switch numéro 1 seront accessibles via 1/0/X

Les ports du switch numéro 2 seront accessibles via 2/0/X

etc.

La commande show interfaces status nous permettra d'afficher la liste de tous les ports

un seul fichier de configuration pour tous les switch

Redondance de panne d'alimentation, chaque switch peut être alimenté par les 2 autres qui l'entour

Le switch Maître

Le switch qui sera l' élu , plusieurs cas sont possible mais nous partirons du principe ou nous mettons l'ensemble de la pile en production, et l'on **positionnera au maître la priorité la plus haute**, il perdra son rôle dans le cas ou il est redémarré ou éteint, retiré de la pile ou hors service

L'affichage d'un Master stack au démarrage après le POST – Power on self test (auto test au démarrage) du pgm constructeur cisco

```
UPB MBIST Test Passed.
POST: MA BIST : End, Status Passed

POST: TCAM BIST : Begin
POST: TCAM BIST : End, Status Passed

extracting front_end/front_end_ucode_info (43 bytes)
Waiting for Stack Master Election...
POST: Thermal, Fan Tests : Begin
POST: Thermal, Fan Tests : End, Status Passed

POST: PortASIC Stack Port Loopback Tests : Begin
POST: PortASIC Stack Port Loopback Tests : End, Status Passed

POST: PortASIC Port Loopback Tests : Begin
POST: PortASIC Port Loopback Tests : End, Status Passed

POST: EMAC Loopback Tests : Begin
POST: EMAC Loopback Tests : End, Status Passed

Election Complete
Switch 1 booting as Master
Waiting for Port download...Complete
```

L'action d'après se fera des switch participants au stack lesquels redémarre et récupèrent les paramètres du maître

État du stack et priorités : **show switch detail**

Switch#	Role	Mac Address	Priority	Current State
*1	Master	0015.c6f5.6000	15	Ready
2	Member	0015.63f6.b700	5	Ready
3	Member	0015.c6c1.3000	1	Ready

Pour vérifier l'état des ports de stack :

```
Cisco2960S-Stack#show switch stack-ports
```

Switch #	Port 1	Port 2
1	Ok	Ok
2	Ok	Ok
3	Ok	Ok

Les **IOS des switch doivent être les mêmes** afin de ne pas avoir de commandes différentes ou les mêmes mais ayant subi une mise à jour avec des arguments/variables et algo différents pour éviter les erreurs .

Pour mettre à jour les IOS sur tous les switches on va recopier l'ios du switch comportant la dernière version vers l'autre switch avec la commande : **ARCHIVE COPY**

Copier l'image système du membre 1 vers le 2 du stack, puis reload du switch 2

Archive copy -sw /destination-system 2 1

La pile de switch sont stack et ses priorités

Dans la cas d'un reboot pour divers raisons du switch Maître, il faut qu'il puissent reprendre sa place, on appliquera une priorité.

Les priorités vont de 1 à 15, on positionnera les **switchs other/non maîtres a 1** , le **backup a 10** par exemple et le **maître a 15** pour être sur qu'il n'y est pas d'ambiguïté au reboot.

La commande à insérer après vérification de son numéro de stack dans la pile

Swich X_switch_number priority Y_1_a_15 → switch 3 priority 1

il est possible de **modifier le numéro de switch** avec la commande

switch 3 renumber 4

Par contre un switch qui est numéroté 2 mais qui est inséré dans une pile ou il existe des switch 1 2 3 connectés il se verra attribuer le numéro 4 à l'instant ou il va redémarrer pour recevoir la configuration du maître du stack

L'ajout d'un switch dans une pile

Dans le fichier de configuration on retrouve la configuration du stack

```
Cisco2960S-Stack#sh running-config | include provision
```

```
switch 1 provision ws-C2960S-48FPD-L
```

```
switch 2 provision ws-C2960S-48FPD-L
```

```
switch 3 provision ws-C2960S-48FPD-L
```

L'ajout ou la suppression d'un switch pourra se faire via la commande

```
Cisco2960S-Stack(config)#switch 4 provision ws-C2960S-48LPD-L  
ou  
Cisco2960S-Stack(config)#no switch 4 provision
```

Procédure de retrait d'un switch

débrancher le câble électrique, puis de câble stack et supprimer la ligne dans la configuration avec no

Afficher le numéro du switch dans la pile dans la baie



Appuyer sur le bouton mode pour sélectionner la led stack a gauche, le numéro du fastethernet allumé indiquera le numéro du switch

Les Ports utilisateurs

La configuration des port utilisateurs sur les switches d'accès 2960 est laissé en auto négociations - full duplex, 10/100/1000 Mbits/s

Les Liens / raccords entre Switchs

a- Lien entre 2 piles de switch de distribution/coeur de réseau hors châssis

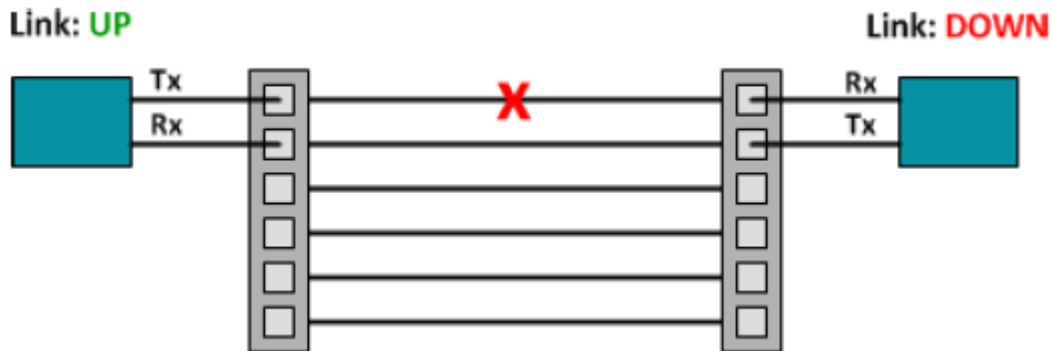
Le lien entre « 2 piles » de switchs de distribution type 3560 utilisant la technologie stackwise se fera via un **double attachement** en etherchannel via le protocole LACP norme standart (PAGP – protocole Cisco)

b- Raccord de switchs d'accès sur une pile de switchs

Dans le cas ou l'on **rajoute en « cascade » des switch d'accès** sur une pile de switch pour le raccord d'une salle de réunion ou d'un bureau on fera un « **simple attachement** » via le **port « UPLINK » du switch bout de ligne**, (utilisé pour empiler des hub ou switch, il peut être un port **Gbits ou port SFP** avec des trancivers) en utilisant un câble droit et si il **n'existe pas de port « UPLINK » (le switch est dit stand-alone)** on **utilisera un port standart Fast ethernet ou Gigabit Ethernet via un câble croisée** , on n'utilisera pas la technologie Etherchannel (LACP) que l'on réserve pour des liens de backbone, entre les piles de switch et chassis.

Le Protocole UDLD

Lien Fibre et protocole UDLD - unidirectionnal link detection



Détection de liaison unidirectionnelle (**UDLD**) est une couche **Cisco-propriétaire** de deux protocoles conçu pour détecter automatiquement la perte de communication bidirectionnel sur un lien. Il est souvent mentionné au niveau du spanning-tree, mais n'a pas de relation directe avec IEEE 802.1D.

UDLD peut fonctionner à la fois sur la **fibres optique** et les **liaisons de cuivre à paire torsadée (exemple ci-dessous)**. Bien que **UDLD est un protocole propriétaire niv 2**, son fonctionnement et le format des paquets sont définis dans la **RFC 5171**.

L'avantage d'utiliser UDLD sur les interfaces en fibres est évidente. La Fibre utilise la lumière pour transporter des données, qui ne nécessitent pas un parcours en boucle (un lien) pour compléter un circuit comme le fait un moyen électrique comme Ethernet à paire torsadée (dans lequel chaque paire dans le câble est un circuit physique). **Il est possible d'avoir un lien à l'échec dans un seul sens.**

On implémente UDLD sur tous les liens fibres optique, UDLD permettra de suivre l'état physique des liens fibre optique.

UDLD permet de **détecter une coupure fibre** grâce a des **packets « hello packets »** envoyés régulièrement, entraînant une communication unidirectionnelle.

UDLD est un **protocole de niveau 2**, si une **coupure** se produit le **packet hello envoyé ne reçoit pas d'acquittement** et le port du switch passe a l'état « **error disabled** »

UDLD mode normal :

En **mode normal**, lors de la **détection de la perte d'un voisin**, UDLD envoie **sept informations** supplémentaires (une par seconde). L'interface est toujours considéré comme opérationnel par les protocoles de couche supérieure et le **commutateur peut encore être tenté d'envoyer du trafic à l'extrémité éloignée**.

UDLD mode agressif :

Comme alternative au mode normal, nous pouvons **configurer UDLD en mode agressif**. Mode agressif diffère en ce que **si un lien est détectée comme étant unidirectionnel**, l'interface est placé dans l'état erreur et cesse d'envoyer du trafic.

```
Switch(config)# interface f0/13
Switch(config-if)# udld port
```

```
Switch# debug udld events
UDLD events debugging is on
Switch#
00:18:07: allNeighborsAgedOutEvent during link up. (Fa0/13)
00:18:07: Phase set from ADV to LUP because all neighbors aged out (Fa0/13)
00:18:07: prev = 0 entry = 3790AEC next = 0 exp_time = 0 (Fa0/13)
00:18:07: udsb->cache = 0x2F80128 (Fa0/13)
00:18:07: timeout timer = 7 (Fa0/13)
00:18:08: timeout timer = 6 (Fa0/13)
00:18:09: timeout timer = 5 (Fa0/13)
00:18:10: timeout timer = 4 (Fa0/13)
00:18:11: timeout timer = 3 (Fa0/13)
00:18:12: timeout timer = 2 (Fa0/13)
00:18:13: timeout timer = 1 (Fa0/13)
00:18:14: timeout timer = 0 (Fa0/13)
00:18:14: Phase set to udld_advertisement from phase udld_link_up. (Fa0/13)
00:18:14: Phase set to udld_advertisement after timer_expired. (Fa0/13)
Switch# show udld f0/13

Interface Fa0/13
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Advertisement
Message interval: 7
Time out interval: 5
No neighbor cache information stored
```

```
Switch(config)# interface f0/13
Switch(config-if)# udld port aggressive
```

```
Switch# show udld f0/13

Interface Fa0/13
---
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7
Time out interval: 5

Entry 1
---
Expiration time: 43
Device ID: 1
Current neighbor state: Bidirectional
Device name: CAT0746Z0WN
Port ID: Fa0/16
Neighbor echo 1 device: CAT1032NJ69
Neighbor echo 1 port: Fa0/13

Message interval: 15
Time out interval: 5
CDF Device name: S2
```

Après une simulation de panne à l'autre bout, nous pouvons voir que maintenant UDLD répond en plaçant l'interface locale dans l'état erreur

```
Switch# show udld f0/13

Interface Fa0/13
---
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Unknown
Current operational state: Disabled port
Message interval: 7
Time out interval: 5
No neighbor cache information stored
Switch# show interfaces f0/13
FastEthernet0/13 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0018.ba98.688f (bia 0018.ba98.688f)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
...
```

Après avoir résolu l'erreur, nous pouvons restaurer l'interface en la réactivant, soit en exécutant la commande globale « **UDLD reset** » pour restaurer automatiquement toutes les interfaces en « **err-disable** »

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

4 - La commutation

La gestion des opérations de commutation:

Un commutateur crée et gère des **tables de commutation**.

En règle générale, les ponts assurent la commutation au niveau logiciel (Sur un PC avec 2 cartes Ethernet en les sélectionnant avec CTRL vous pouvez générer un pont logiciel sous windows), les commutateurs au niveau matériel.

La commutation de niveau 2 et de niveau 3

Processus qui consiste à prendre une trame entrante sur une interface et à l'acheminer par une autre interface. Les **routeurs** utilisent la **commutation de couche 3** pour acheminer un **paquet**, les **commutateurs** utilisent la **commutation de couche 2 et 3** pour acheminer les **trames**

A l'opposé de la commutation de couche 3, la commutation de couche 2 ne regarde pas à l'intérieur d'un paquet pour y trouver les informations de couche réseau (IP). La commutation de couche 2 regarde l'adresse MAC de destination contenue dans une trame. Elle envoie les informations à la bonne interface, si elle connaît l'emplacement de l'adresse de destination. La commutation de couche 2 crée et met à jour une **table de commutation** qui consigne les **adresses MAC associées à chaque port ou interface**.

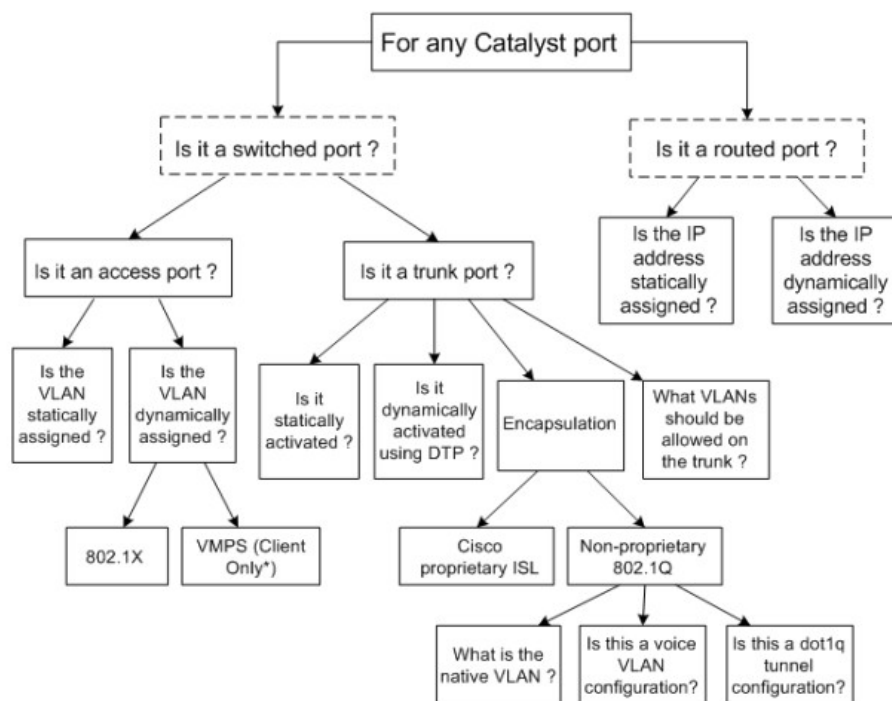
```

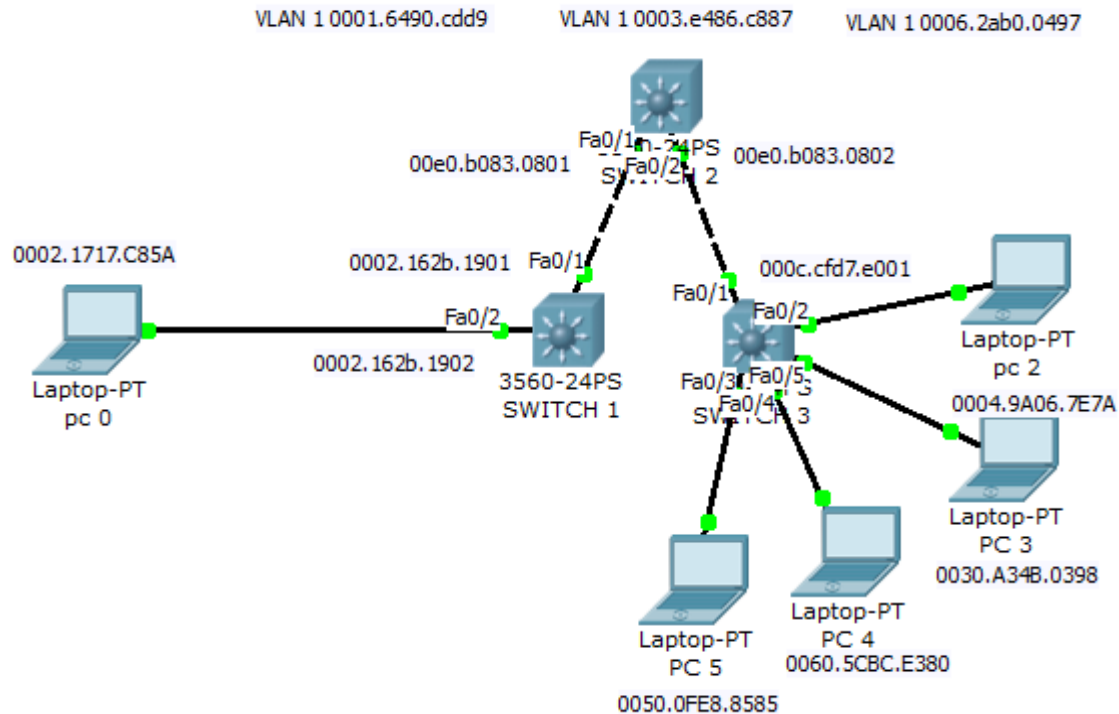
S3#sh mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0005.5e25.d802    DYNAMIC   Fa0/2
10      0001.c7c4.5cd3    DYNAMIC   Fa0/2
10      0005.5e25.d802    DYNAMIC   Fa0/2
20      0005.5e25.d802    DYNAMIC   Fa0/2
20      0040.0b9c.a1c6    DYNAMIC   Fa0/2
30      0001.c7ca.e31c    DYNAMIC   Fa0/2
30      0005.5e25.d802    DYNAMIC   Fa0/2
99      0005.5e25.d802    DYNAMIC   Fa0/2
99      0050.0fc2.2320    DYNAMIC   Fa0/2

```

Dans le cas où le commutateur ne sait pas où envoyer la trame, il l'envoie par tous ses ports au réseau (sauf sur le port d'origine) pour connaître la bonne destination. Lorsque la réponse est renvoyée, le commutateur prend connaissance de l'emplacement de la nouvelle adresse et ajoute les informations à la table de commutation.

« Routed port » ou « switched port » sur un commutateur de couche 3



Exemple :

Des ping sont effectués a partir de PC0 a destination PC2 a PC5

pc 1 -> TOUS PC

```

1 0002.1717.c85a DYNAMIC Fa0/2
1 0004.9a06.7e7a DYNAMIC Fa0/1
1 0030.a34b.0398 DYNAMIC Fa0/1
1 0050.0fe8.8585 DYNAMIC Fa0/1
1 0060.5cbc.e380 DYNAMIC Fa0/1
1 00e0.b083.0801 DYNAMIC Fa0/1

1 0002.162b.1901 DYNAMIC Fa0/1
1 0002.1717.c85a DYNAMIC Fa0/1
1 0004.9a06.7e7a DYNAMIC Fa0/2
1 000c.cfd7.e001 DYNAMIC Fa0/2
1 0030.a34b.0398 DYNAMIC Fa0/2
1 0050.0fe8.8585 DYNAMIC Fa0/2
1 0060.5cbc.e380 DYNAMIC Fa0/2

1 0002.1717.c85a DYNAMIC Fa0/1
1 0004.9a06.7e7a DYNAMIC Fa0/2
1 0030.a34b.0398 DYNAMIC Fa0/5
1 0050.0fe8.8585 DYNAMIC Fa0/3
1 0060.5cbc.e380 DYNAMIC Fa0/4
1 00e0.b083.0802 DYNAMIC Fa0/1

```

Affichage de la table Mac de Switch1 / Switch 2 / Switch 3

Conclusion : on s'aperçoit que tous les switch connaissent toutes les adresses MAC de l'ensemble des équipements

5 - Sécurités des ports

Protection des services de commutation (Attaque Mac Flooding)

Cette attaque cherche à impacter le bon fonctionnement de la commutation de niveau 2 afin de pouvoir écouter le trafic réseau. Elle consiste à envoyer sur le port d'un commutateur un grand nombre d'adresses MACs pour remplir sa table de commutation (CAM), et donc bloquer son fonctionnement normal. Si la table CAM est pleine, le commutateur est obligé de renvoyer sur tous les ports les paquets à destination des adresses MAC inconnues, « **le commutateur se met en mode HUB** ». Cette attaque peut être une technique pour capturer un flux qui en fonctionnement normal n'aurait jamais pu être écouté car non destiné à l'attaquant.

Pour éviter ce type d'attaque, Cisco met à disposition au sein de ses commutateurs une fonction qui se nomme « **Port-Security** ». Cette fonction permet entre autre de **limiter le nombre d'adresses MAC** sur un port et donc **protège contre le «Mac Flooding** ».

Il est possible de configurer le ou les ports d'un commutateur pour qu'il accepte 1 ou 2 ou plus des adresses MAC des périphériques de façon dynamique et bloque le trafic venant d'hôtes non valides en cas de violation.

La fonction 'Port Security' offre plusieurs déclinaisons de configuration sur un port :

- **Configuration statique des adresses MACs autorisées sur un port**, ce qui permet d'éviter qu'un port connecté sur une imprimante ou dans un lieu en libre accès soit utilisé par une tierce personne.
- **Configuration du nombre d'adresses MAC maximal que peut apprendre un commutateur sur un port**. En limitant à un sur des ports PC, 2 pour PC + téléphone et supérieur (par exemple 12) pour des salles de réunions, il deviendra impossible à un attaquant de remplir la table CAM du commutateur.

Configuration du port-security

```
Comm1(config-if)#switchport mode access
Comm1(config-if)#switchport port-security
Comm1(config-if)#switchport port-security maximum 2

//activation de l'apprentissage des adresses mac
Comm1(config-if)#switchport port-security mac-address sticky
//Tous les paquets n'ayant pas pour adresse MAC source celle apprise seront dropés
Comm1(config-if)#switchport port-security violation protect
```

Exemple de configuration d'entreprise sur des switch d'accès

```
Switch(config)# interface range fastethernet 0/1 – 48

//nb d'adresse mac maximum apprise par port , généralement un PC + téléphone IP
Switch(config-if)# switchport port-security maximum 3

Switch(config-if)# switchport port-security

//Si aucun trafic de donné n'est envoyé ou reçu par une adresse source pendant une période de 2 minutes
« aging time » , le switch supprimera l'adresse MAC de sa table Mac-adresse-table, et pourra apprendre
de nouvelle @MAC
```



```
Switch(config-if)# switchport port-security aging time 2
```

// Dans le cas ou il y a dépassement du nombre de MAC adresses détecté , le switch va droper les paquets envoyés par les Mac adresses inconnues.

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

//limiter le temps de validité d'une adresse, permettant d'ajouter ou de supprimer des machines sans avoir a se soucier de la gestion des adresses mac, tout en gardant un nombre maximum d'adresse par port

2 modes :

absolute : les adresses Mac sont toutes supprimés après un certains temps

inactivity : les adresses mac sont supprimés après un certain temps d'inactivités

```
Switch(config-if)# switchport port-security aging type inactivity
```

Dans le cas ou on utilisera dans une salle de réunion un 2960 pour l'accès aux utilisateurs, on le raccordera sur un des switch de distribution 3650 stacké, il faudra augmenter le port concerné du 3650 a autant d'adresses MAC apprises qu'aura de ports le 2960.

Le Broadcast Storm

Pour limiter le taux de « broadcast » et « multicats » MAC des ports Ethernet des switches d'accès utilisateurs

Pour avoir une tempête, il faut réunir deux conditions :

1. il y a une ou plusieurs boucles de niveau 2
2. un équipement ou service applicatif – logiciel métier ou service DNS par exemple génère au moins une trame qui doit être diffusée sur toutes les interfaces

La trame va aussi être émise sur chaque interface de la boucle et reçue, donc diffusée, à nouveau ... et cela sans fin.

Dans la pratique, les tempêtes sont liées à des trames dont l'adresse de destination porte le bit « Group address ». Cela correspond à une valeur impaire du premier octet de l'adresse mac destination. On observe en fait deux valeurs pour cet octet : la valeur « FF » et la valeur « 01 ».

La valeur « FF » correspond à des trames « broadcast »

La valeur « 01 » correspond à des trames « multicast »

Exemples de trames

•« broadcast » : les ARP request, DHCP request, le protocole NETBIOS des réseaux Microsoft., les protocoles ISO ...

•« multicast » : les protocoles de niveau 2 comme STP, CDP, VTP, etc, mais aussi certaines applications.

la configuration

Avec le « storm-control », le flux « broadcast » et « multicast » qui entre dans le switch reste dans des limites acceptables.

Sur Catalyst 3750G, configurer sur toutes les interfaces :

storm-control broadcast level 5.00 ! en % du débit de l'interface

•storm-control multicast level 5.00

Sur Catalyst 4500, configurer sur toutes les interfaces :

•storm-control broadcast include multicast

•storm-control broadcast level 5.00

Sur Catalyst 4500, le storm control limite le flux à la valeur indiquée. La tempête n'est pas stoppée, elle est limitée. On va dire que ce n'est plus une tempête, mais un courant d'air. Le trafic limité généré par la tempête est continuellement diffusé par le switch.

Il ne faut pas mettre des valeurs trop grandes. Par exemple, 10% d'un Gigabit Ethernet, ce serait trop, car cela fait 100% d'un FastEthernet

```
Switch(config)# interface range fastethernet 1/0/1 - 48
```

```
Switch(config-if)# storm-control broadcast level 5.0
```

```
Switch(config-if)# storm-control action trap
```

//Active la remontée d'information SNMP lorsqu'une tempête de broadcast détecté sur les ports

```
Switch(config)#snmp-server enable traps storm-control trap-rate 0
```

//Configure le nombre maximum de contrôle de tempêtes envoyés par minute. La plage est de 0 à 1000; la valeur par défaut est 0 (aucune limite n'est imposée, une alerte est envoyée à chaque occurrence).

Storm-Control sur les port TRUNK : il faudra limiter a moins de 50% de la bande passante

Les mécanismes de sécurité mis en place sur un switch CISCO 3650

Sécurisation des ports

Il est possible de restreindre le nombre d'adresses MAC possibles sur chacun des ports. Ce faisant on se protège des attaques par MAC flooding

Pour l'activer :

```
Switch(config)# interface gigabitethernet0/1
```

```
Switch(config-if)# switchport mode access
```

```
Switch(config-if)# switchport port-security
```

```
Switch(config-if)# switchport port-security maximum 3
```

dans cette configuration 3 adresses sont possibles

En présence de VLAN il est possible de les répartir

```
Switch(config-if)#switchport port-security maximum 2 vlan 3
```

// 2 Adresses MAC pour VLAN 3

```
Switch(config-if)#switchport port-security maximum 1 vlan 4
```

//une @Mac apprise pour VLAN 4

Il est en outre possible de paramétrer des durées

```
Switch(config-if)# switchport port-security aging time 2
```

```
Switch(config-if)# switchport port-security aging type inactivity
```

```
Switch(config-if)# switchport port-security aging static
```

Limiter les requêtes ARP

Pour se prémunir d'un **DOS (deni of service)** il est recommandé de **limiter au niveau de chacun des ports les requêtes ARP ainsi que leurs réponses**

Pour l'activer :

```
Switch(config)#ip arp inspection limit rate 70
```

Dans ce cas la valeur **70** correspond au **nombre de paquets par seconde**.

pendant la réception de la trame et sera plus élevée dans le cas des grandes trames. Le commutateur dispose de beaucoup de temps pour vérifier les erreurs (détection d'erreurs-CRC) en attendant de recevoir toute la trame.

Configuration d'une adresse ip pour une gestion sécurisé

Une adresse de couche 3 doit être affectée au commutateur pour une gestion avec tcpip. Vlan1 est l'interface de gestion par défaut, par sécurité on crée un autre réseau local VLAN 99 ou 150 que l'on affecte à un port.

```
Configure terminal / interface vlan99 / ip address 172.17.99.11 255.255.255.0 / no shutdown / end / configure terminal / interface fastethernet 0/18 / switchport mode access vlan 99 / end
```

show ip interface vlan1 → @ip + @mac de l'interface virtuelle du commutateur

Par défaut la commande « no shutdown » est configurée sur le vlan 1

Si aucun port n'est à l'état UP dans le vlan 1, l'interface de celui-ci est désactivée

```
Switch#show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
```

configuration d'une passerelle par défaut :

```
ip default-gateway 172.17.99.1          //routeur de sortie du vlan1
show ip interface brief                //vérification
```

```
Switch#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Prot
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/2	unassigned	YES	unset	up	up
Vlan1	192.168.1.1	YES	manual	up	up

```
Switch#
```

configuration du mode bidirectionnel et vitesse

interface fastethernet 0/1 / duplex auto / speed auto

```
S2#show interfaces fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 00e0.f73e.b701 (bia 00e0.f73e.b701)
  BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
```

Activation de l'interface web :

Feature	Requirement	Configuration Example
Secure access	SSH and HTTPS	<pre>Router(config)# ip http secure-server Router(config)# ip http authentication local Router(config)# line vty 0 15 Router(config)# login local Router(config-line)# transport input ssh Router(config-line)# transport output ssh</pre>
Nonsecure access	Telnet and HTTP	<pre>Router(config)# ip http server Router(config)# ip http authentication local Router(config)# line vty 0 15 Router(config)# login local Router(config-line)# transport input telnet Router(config-line)# transport output telnet</pre>
User privilege level	15	<pre>Router(config)# username cisco privilege 15 secret 0 cisco</pre>

Les commandes SHOW

show ip interface | http | arp | mac-address-table

Sauvegarde

```
copy system:running-config flash:startup-config
copy runn start
copy startup-config flash:config.bak
```

restauration

```
copy flash:config.bak startup-config
reload
```

suppression des fichiers de configuration

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

suppression des vlan

```
Switch#delete flash:/vlan.dat
Delete filename [/vlan.dat]?
Delete flash:/vlan.dat? [confirm]

Switch#
```

Configuration des accès telnet en environnement de Laboratoire

Dans un environnement de Lab pour des switches ou routeurs, il est possible de configurer les lignes VTY pour accepter toutes les connections telnet immédiatement, sans demander de mot de passe et placera l'utilisateur dans le mode Privilege Exec directement.

```
SYNAPSSWITCH(config)# enable secret cisco
```

```
SYNAPSSWITCH((config)# line vty 0 15
```

```
SYNAPSSWITCH((config-line)# no login
```

```
SYNAPSSWITCH((config-line)# privilege level 15
```

Sécurité des accès Administratif Telnet – ssh

Mise en place de ssh sur les lignes VTY

Changer le nom de votre Switch

```
hostname testssh
```

Créer un domaine test.com

```
ip domain-name test.com
```

Créer une base de donnée utilisateurs locaux avec un accès administrateur pour un accès SSH

```
username test privilege 15 secret test
```

configurer les lignes VTY pour autoriser uniquement les accès SSH et la base de donnée local d'authentification

```
line VTY 0 15
```

```
transport input ssh
```

```
login local
```

Générez la clé de chiffrement RSA avec un modulus de 1024

```
FM(config)#crypto key generate rsa
% You already have RSA keys defined named FM.test.com .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: FM.test.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

FM(config)#
```


Voir la configuration SSH

```

FM#
%SYS-5-CONFIG_I: Configured from console by console
sh ip ssh
FM#sh ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
FM#

```

Voir la clé RSA partagée

```

FM#sh crypto key ?
  mypubkey  Show public keys associated with this router
FM#sh crypto key m
FM#sh crypto key mypubkey rs
FM#sh crypto key mypubkey rsa
% Key pair was generated at: 2:41:20 UTC mars 1 1993
Key name: FM.test.com
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
00004319 00001dc8 00005586 00006cd7 00006977 0000714f 0000504d
000040ae
000034af 000001b2 00007646 000041a0 00007082 00004c7b 00006c62
00006828
00003d90 0000119e 00004d52 00001487 00002a26 00005902 000028f8 6067
% Key pair was generated at: 2:41:20 UTC mars 1 1993
Key name: FM.test.com.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
00004d57 0000713d 0000181b 000033bf 0000184e 00004ba0 0000385e
000020f6
000051e2 00005973 00002473 00004c4b 0000706b 00004e81 00003c8c
00006274
000045d4 00006cd8 00005312 00006285 000031f2 00003dca 0000119a 3f14
FM#

```

Réglage de la tempo avant déconnexion de l'utilisateur de 75 secondes avec 2 tentatives d'essai

```
S1(config)# ip ssh time-out 75
```

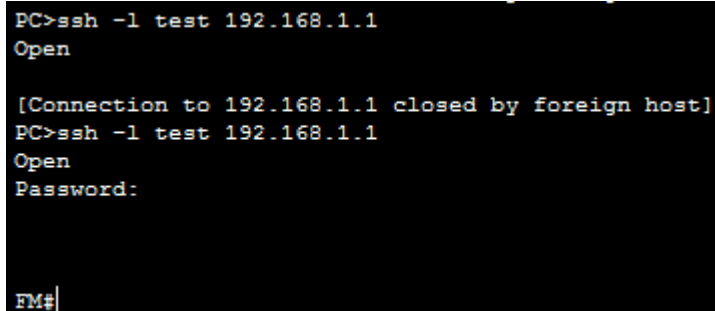
```
S1(config)# ip ssh authentication-retries 2
```

voir la nouvelle configuration

```
FM(config)#do show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 75 secs; Authentication retries: 2
```

Lancer une connexion SSH a partir d'un PC

ssh -l nom_user_local @ip_switch_ou_router



```
PC>ssh -l test 192.168.1.1
Open

[Connection to 192.168.1.1 closed by foreign host]
PC>ssh -l test 192.168.1.1
Open
Password:

FM#
```

Une des solutions pour remplacer les accès telnet et activer l'accès ssh sur le vlan de gestion uniquement**service password-encryption**

```
!
logging buffered 16384
enable secret ciscoenpa55
!
username admin secret cisco
!
banner motd $*** swithc entreprise***$
!
no ip domain lookup
!
aaa new-model // activation du service d'authentification
aaa authentication login default local //n'autoriser que les users local de ce switch
aaa authentication login CONSOLE none //pas d'authentification mode console
aaa authorization exec default local
*
```

```
vlan 100
name MGMT //vlan de management
*
ip telnet source-interface Vlan100      //on rattache les accès telnet au VLAN 100
ip ssh source-interface Vlan100         //on rattache les accès SSH au VLAN 100
*
line con 0
exec-timeout 60 0
login authentication CONSOLE
logging synchronous
line vty 0 4
exec-timeout 60 0
transport input telnet ssh
line vty 5 15
no transport input
```

Remarque sur les routeur on utilisera les interfaces de loopback

Faire une sauvegarde automatique sur un serveur TFTP avec « write memory »

L'exemple suivant montre comment activer la journalisation de configuration avec un maximum de 200 entrées dans le journal de configuration . Dans l'exemple , la sécurité est accrue par la suppression de l' affichage des informations de mot de passe dans la configuration journaux dossiers avec la commande hidekeys , et les notifications syslog sont activées avec la commande syslog aviser

```
archive                // mode archive
log config              // activation du mode de configuration de l'enregistrement
logging size 50         // nb maximum de ligne d'entrées dans le journal de configuration
notify syslog           // envoi des notifications de modifications de configuration à un syslog
                        // distant
hidekeys                // supprime l'affichage des informations de mot de passe dans les fichiers
                        // journaux de configuration
path tftp://10.1.50.1/$h-archive-config
write-memory
file prompt quiet
```

La commande « archive » permet de sauvegarder la configuration des équipements à intervalle régulier ou au moment de « write memory » - sauvegarde de la configuration du running-config en nvram

Device# **show archive log config 1 2**

idx	sess	user@line	Logged command
1	1	user1@console	logging enable
2	1	user1@console	logging size 200

Device# **show archive log config all provisioning**

```
archive
log config
logging enable
logging size 200
```

Device# **show archive log config statistics**

Config Log Session Info:

```
Number of sessions being tracked: 1
Memory being held: 3910 bytes
Total memory allocated for session tracking: 3910 bytes
Total memory freed from session tracking: 0 bytes
```

Config Log log-queue Info:

```
Number of entries in the log-queue: 3
Memory being held in the log-queue: 671 bytes
Total memory allocated for log entries: 671 bytes
Total memory freed from log entries:: 0 bytes
```

switch#configure terminal

switch(config)#archive

switch(config-archive)#path tftp://172.16.1.10/\$h-archive-config

switch(config-archive)#write-memory

Sauvegarde de la configuration du switch dans un dossier partagé tftp

\$h concatène le nom du switch au fichier – switch-archive-config

6 - STP (Spanning Tree Protocol)

Le stp est un protocole de niveau 2 permettant de déterminer une topologie réseau sans boucle appelé arbre

Assure la commutation des trames de broadcast arp

Empêche les boucles arp

Permet les liaisons redondantes

Supporte les changements topologique et les pannes d'unité

Les BPDU - Bridge protocol data units :

Les **informations du protocole spanning tree** sont transportés dans des unités de trame de données nommées **BPDU**, les BPDU sont échangés toutes les 2 secondes et permettent aux commutateur de garder une trace des changements sur le réseau pour activer ou désactiver les ports requis.

Lorsqu'un commutateur est raccordé au réseau, il commence par envoyer des BPDU pour déterminer la topologie (switch/routeurs) du réseau avant de transférer des données.

3 types de BPDU :

CBPDU : pour le calcul du spanning tree

TCN : annoncé les changements topologiques, mise en place d'un nouveau switch par exemple

TCA : acquittement de changement de notifications de la topologie

Les BPDU sont envoyés à l'adresse de multicast MAC : 01:80:C2:00:00:00

Les 5 états du STP

- **Listening** - le switch "écoute" les BPDUs et détermine la topologie réseau
- **Learning** - le switch construit une **table MAC** mappant les adresses MAC au numéro de port
- **Forwarding** - un port reçoit et envoie des données, opération normale
- **Blocking** - un port provoquant une boucle, aucune donnée n'est envoyée ou reçue mais le port peut passer en mode forwarding si un autre lien tombe
- **Disabled** - désactivé, un administrateur peut manuellement désactiver un port s'il le souhaite

Quand un client tel qu'un ordinateur, une imprimante ou un serveur est connecté au réseau, son port se mettra automatiquement en "forwarding mode" après un délai de 50 secondes où il va se mettre en mode *listening* puis *learning*.

Les acteurs Logiciels Cisco

Cisco Network Assistant

Il s'agit d'une application de management réseau Cisco conçue pour les petites et moyennes entreprises avec jusqu'à 250 utilisateurs connectés, et qui s'installe simplement sur PC, tablette ou même smartphone. Cisco Network Assistant (CNA) offre la possibilité de manager et de configurer globalement le réseau (routeurs, commutateurs et point d'accès) à travers une interface graphique conviviale. Pour davantage d'informations sur Cisco Network Assistant, visitez cisco.com/go/cna.

Ciscoview

affiche une vue physique du commutateur, utiliser configurer et consulter des informations d'état et de performance. Application autonome ou intégrée à la plateforme snmp (simple network management protocol) .

cisco configuration professionnall: idem que cna

Cisco Prime Infrastructure

Les solutions Cisco Prime™ fournissent une solution complète pour la supervision et le management pour toutes les phases d'opération du réseau (déploiement, mises à jour, opération courante, ajout de services, résolution de problèmes...) Cisco Prime Infrastructure fournit une suite exhaustive de fonctionnalités pour automatiser le déploiement initial du réseau ainsi que tous les autres déploiements consécutifs (extensions, nouveaux services...)

Cisco Prime bénéficie de la connaissance complète des matériels et logiciels ainsi que de l'expertise sur les opérations pour offrir un ensemble complet de processus automatisés permettant de configurer, superviser, analyser le réseau. Pour plus de détails sur Cisco Prime, visitez cisco.com/go/prime.

Cisco Prime et ses différents modules :

- -Cisco Prime Network Network Analysis Module (NAM)
- -Cisco Prime LAN Management Solution (LMS):
 - à partir de la version 4.1 C'est l'évolution de l'ancien Ciscoworks LMS, dont l'interface a été entièrement repensée en version 4.0, et qui est maintenant disponible également sous forme de Virtual Appliance.
- -Cisco Prime Network Control System (NCS) 1.0:
 - C'est le successeur de Wireless Control System (WCS), le gestionnaire des environnements WiFi. Etant plus performant, son nom a été amené à changer.
- Cisco Prime Collaboration Manager (CM) 1.0:
 - la gestion des environnements de collaboration.

Gestion de la puissance électrique

Les commutateurs de la série 2960-X offrent de nombreuses fonctionnalités inédites sur le marché pour réduire et contrôler la consommation de courant électrique.

- **Switch Hibernation Mode (SHM)** est une innovation Cisco disponible sur l'ensemble des commutateurs 2960-X. Cette fonctionnalité va mettre le commutateur en hibernation et **réduire ainsi considérablement sa consommation électrique durant les périodes de fermeture (soir et week-ends par exemple)**. L'hibernation du commutateur peut être pilotée par tout logiciel de management **EnergyWise**.

- **IEEE 802.3az EEE (Energy Efficient Ethernet)** permet aux de **détecter dynamiquement les périodes d'inactivité sur les ports** et ports et de les placer les cas échéant dans un mode nécessitant moins de puissance électrique, réduisant ainsi la consommation électrique globale.

- Des règles **Cisco EnergyWise** peuvent être utilisées pour contrôler l'alimentation, et la puissance consommée par des terminaux alimentés en PoE, et bien d'autres terminaux disponibles sur le marché. Pour plus d'information sur Cisco EnergyWise, visitez cisco.com/go/energywise

Spécifications techniques des 2960-X

Spécifications matérielles	
Flash memory	128 MB pour LAN Base & IP Lite SKUs, 64 MB pour LAN Lite SKUs
DRAM	512 MB
CPU	APM86392 600MHz dual core
Console Ports	USB (Type-B), Ethernet (RJ-45)
Storage Interface	USB (Type-A) for external flash storage
Network Management Interface	10/100 Mbps Ethernet (RJ-45)

Cisco Catalyst 2960-X Series Performance

Performance and Scalability			
	2960-X LAN Lite	2960-X LAN Base	2960-XR IP Lite
Forwarding bandwidth	50 Gbps	108 Gbps	108 Gbps
Switching bandwidth*	100 Gbps	216 Gbps	216 Gbps
Maximum active VLANs	64	1023	1023
VLAN IDs available	4096	4096	4096
Maximum transmission unit (MTU) - L3 packet	9198 bytes	9198 bytes	9198 bytes
Jumbo frame - Ethernet frame	9216 bytes	9216 bytes	9216 bytes

* La bande passante est mesurée en full-duplex

Performance de commutation série 2960-X

Débit de transmission: Paquets L3 de 64 octets	
Famille Catalyst 2960-X	
Cisco Catalyst 2960X-48FPD-L	130.9 Mpps
Cisco Catalyst 2960X-48LPD-L	130.9 Mpps
Cisco Catalyst 2960X-24PD-L	95.2 Mpps
Cisco Catalyst 2960X-48TD-L	130.9 Mpps
Cisco Catalyst 2960X-24TD-L	95.2 Mpps
Cisco Catalyst 2960X-48FPS-L	107.1 Mpps
Cisco Catalyst 2960X-48LPS-L	107.1 Mpps
Cisco Catalyst 2960X-24PS-L	71.4 Mpps
Cisco Catalyst 2960X-24PSQ-L	71.4 Mpps
Cisco Catalyst 2960X-48TS-L	107.1 Mpps
Cisco Catalyst 2960X-24TS-L	71.4 Mpps
Cisco Catalyst 2960X-48TS-LL	104.2 Mpps
Cisco Catalyst 2960X-24TS-LL	68.5 Mpps
Famille Catalyst 2960-XR	
Cisco Catalyst 2960XR-48FPD-I	130.9 Mpps
Cisco Catalyst 2960XR-48LPD-I	130.9 Mpps
Cisco Catalyst 2960XR-24PD-I	95.2 Mpps
Cisco Catalyst 2960XR-48TD-I	130.9 Mpps
Cisco Catalyst 2960XR-24TD-I	95.2 Mpps
Cisco Catalyst 2960XR-48FPS-I	107.1 Mpps
Cisco Catalyst 2960XR-48LPS-I	107.1 Mpps
Cisco Catalyst 2960XR-24PS-I	71.4 Mpps
Cisco Catalyst 2960XR-48TS-I	107.1 Mpps
Cisco Catalyst 2960XR-24TS-I	71.4 Mpps

Annexes :**BPDU** (Bridge Protocol Data Unit)

Message de données échangé entre deux commutateurs Ethernet. Les données échangées décrivent diverses informations relatives aux ports du commutateur. L'objectif est de détecter de possibles boucles infinies au sein de la topologie réseau

Protocole 802.1d : Pour gérer la tolérance de pannes dans les liaisons inter-commutateurs on met en place des **liaisons redondantes**. Les liaisons redondantes doivent être invalidées quand elles ne sont pas utiles et validées en cas de rupture d'une liaison

Le **spanning tree protocol** (aussi appelé **STP**) est un protocole réseau permettant une topologie réseau **sans boucle** dans les LAN avec pont. Le Spanning Tree Protocol est défini dans la norme IEEE 802.1D.

Les commandes de gestion de base d'un commutateur

Test / Commande	Description	Objectifs
Routeur Cisco		
sh arp	Affiche le cache ARP (adresses IP / MAC)	Vérifier que le cache n'est pas corrompu. Détecter les entrées invalides (adresses <i>incomplete</i>)
sh interface status	Montre l'état et la vitesse des ports	Vérifier si un port est actif, sa vitesse (suite à l'auto-négociation), etc.
sh interface description	Montre l'état et le descriptif des port	Affiche l'état du port pour un serveur donné
sh ip interface brief	Montre l'état et l'adresse IP par port	Montre les adresses IP configurées pour les ports en mode routé
clear arp-cache	Vide le cache ARP	Vérifier que le niveau 2 remonte correctement
sh interfaces fastEthernet 0	Affiche l'état d'un port	Vérifier la vitesse, les pertes, etc.
Switch Cisco		
sh mac-address-table	Affiche la table de switching (adresses MAC par port du switch)	Vérifier qu'il n'y a pas de corruption au niveau des adresses MAC
clear arp-cache	Vide le cache ARP	Vérifier que le niveau 2 remonte correctement
clear mac-address-table	Efface la table de commutation	Si le vidage du cache ARP n'a pas donné de résultat
sh interfaces fastEthernet 0	Affiche l'état d'un port	Vérifier la vitesse, les pertes, etc.