

Switch Cisco

Testé sur 2960, 3550 et 3750 avec IOS 12.2 à IOS 15

- Connexion au Switch
- Commandes de base
- Mettre à jour l'IOS
- Supprimer la configuration en mode rommon
- Configuration des VLAN
- Configuration VLAN voix, QOS, LLDP et CDP
- Configuration de Telnet, SSH et WEB
- Configuration de l'Etherchannel
- Configuration du NTP
- Configuration de Syslog
- Configuration des ports
- Configuration de Port-security
- Configuration du STP
- Configuration du DHCP
- Configuration de la bannière
- Configuration 802.1X
- Configuration du SNMP
- Etats des ports
- Importer et Exporter la configuration via TFTP
- Gestion de la table ARP
- Client FTP
- Configuration du VTP
- Copier un IOS en mode rommon

Connexion au Switch

La première fois que l'on démarre un switch, il faut le configurer via le mode CLI en console.

Connexion au switch via le port série

cisco-serial.jpg

Les réglages par défaut du port série sont les suivants :

- Bits : 9600
- Data bits : 8
- Parity : none
- Stop bit : 1
- Flow control : none

Connexion CLI en USB

cisco-usb.jpg

Nous pouvons maintenant utiliser un cordon mini-USB pour se connecter à un switch Cisco.

Ce cordon va créer un port série virtuel avec lequel nous pourrons nous connecter au switch.

Un pilote est requis.

Connexion en Bluetooth

cisco-bluetooth.jpg

Connexion au switch en IP

Sur les nouvelles gammes de switch Cisco (2960L, C1000), il n'est plus nécessaire d'effectuer la configuration en console.

Sur la gamme Catalyst 2960-L Smart Managed

Adresse IP par défaut : https://192.168.1.1

Attention à ne pas le connecter sur votre réseau local si votre box est aussi en 192.168.1.1 !

Username : smartm

Password : c2960lsm

Commandes de base

Passer en mode privilégié

Par défaut, on entre en privilège 1 qui donne accès à des commandes très basiques.

```
switch>show privilege  
Current privilege level is 1  
switch>
```

Passer en privilège maximum 15 :

```
switch>  
switch>enable  
switch#sh pri  
Current privilege level is 15  
switch#
```

Passer en mode de configuration et le quitter

```
switch#  
switch#configure terminal  
switch(config)#  
switch(config)#exit  
switch#
```

Sauvegarder la configuration

```
switch#copy running-config startup-config
```

La startup-config se trouve dans la nvram alors que la running-config se trouve dans la ram. En copiant la configuration de la running-config dans la startup-config, on écrit la conf dans la mémoire non volatile.

ou

```
switch#write memory
```

Afficher la configuration

```
switch#show running-config
```

Redémarrer le switch

```
switch#reload
```

Renommer le switch

```
switch#  
switch#conf t  
switch(config)#hostname Maquette  
Maquette(config)#
```

Attribuer une adresse IP

```
switch#  
switch#conf t  
switch(config)#interface vlan1  
switch(config-if)#ip address 192.168.1.100 255.255.255.0  
switch(config-if)#exit  
switch(config)#exit  
switch#
```

Passerelle par défaut

```
switch(config)#ip default-gateway 192.168.1.1
```

Serveur DNS

```
switch(config)#ip name-server 192.168.1.1
```

Supprimer la configuration

```
switch#erase startup-config
```

Pour compléter automatiquement une commande, utiliser la touche TAB

```
switch(config)#inter
switch(config)#interface
switch(config)#interface gig
switch(config)#interface GigabitEthernet0/0
```

Désactiver le DNS lookup pour ne pas attendre lors d'une mauvaise commande

```
switch(config)#no ip domain-lookup
```

Supprimer une ligne ou un paramètre

```
switch(config)#no vlan
switch(config)#no ntp server 194.2.0.28
switch(config)#no ip address
```

Ajouter "no" devant la ligne pour l'effacer de la configuration

Pour afficher l'aide, utiliser le ? après une commande

```
3750#?
```

Exec commands:

access-enable	Create a temporary Access-List entry
access-template	Create a temporary Access-List entry
archive	manage archive files
cd	Change current directory
clear	Reset functions
clock	Manage the system clock
cns	CNS agents
configure	Enter configuration mode
connect	Open a terminal connection
copy	Copy from one file to another
debug	Debugging functions (see also 'undebug')
delete	Delete a file
dir	List files on a filesystem
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
dot1x	IEEE 802.1X Exec Commands
enable	Turn on privileged commands
eou	EAPoUDP

erase Erase a filesystem
ethernet Ethernet parameters
exit Exit from the EXEC
--More--

Afficher l'état des interfaces

```
3750#sh ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	172.16.3.200	YES	NVRAM	up	up
FastEthernet1/0/1	unassigned	YES	unset	up	up
FastEthernet1/0/2	unassigned	YES	unset	down	down
FastEthernet1/0/3	unassigned	YES	unset	down	down
FastEthernet1/0/4	unassigned	YES	unset	down	down
FastEthernet1/0/5	unassigned	YES	unset	down	down
FastEthernet1/0/6	unassigned	YES	unset	down	down
FastEthernet1/0/7	unassigned	YES	unset	down	down
FastEthernet1/0/8	unassigned	YES	unset	down	down
FastEthernet1/0/9	unassigned	YES	unset	down	down
FastEthernet1/0/10	unassigned	YES	unset	down	down
FastEthernet1/0/11	unassigned	YES	unset	down	down
FastEthernet1/0/12	unassigned	YES	unset	down	down
FastEthernet1/0/13	unassigned	YES	unset	down	down
FastEthernet1/0/14	unassigned	YES	unset	down	down
FastEthernet1/0/15	unassigned	YES	unset	down	down
FastEthernet1/0/16	unassigned	YES	unset	down	down
FastEthernet1/0/17	unassigned	YES	unset	down	down
FastEthernet1/0/18	unassigned	YES	unset	down	down
FastEthernet1/0/19	unassigned	YES	unset	down	down
FastEthernet1/0/20	unassigned	YES	unset	down	down
FastEthernet1/0/21	unassigned	YES	unset	down	down
FastEthernet1/0/22	unassigned	YES	unset	down	down
FastEthernet1/0/23	unassigned	YES	unset	up	up
FastEthernet1/0/24	unassigned	YES	unset	up	up
GigabitEthernet1/0/1	unassigned	YES	unset	down	down
GigabitEthernet1/0/2	unassigned	YES	unset	down	down
GigabitEthernet1/1/1	unassigned	YES	unset	down	down
GigabitEthernet1/1/2	unassigned	YES	unset	down	down

```
3750#
```

Inventaire

Switch#show inventory

NAME: "1", DESCR: "ME-C3750-24TE"

PID: ME-C3750-24TE-M , VID: V07, SN: FDO1521Y24L

NAME: "GigabitEthernet1/1/1", DESCR: "1000BaseSX SFP"

PID: , VID: , SN: OP10G53E1584

NAME: "GigabitEthernet1/1/2", DESCR: "1000BaseSX SFP"

PID: , VID: , SN: H11S478

Mettre à jour l'IOS

Pour mettre à jour un routeur ISR c'est par ici : [Mettre à jour l'IOS \(ISR\)](#)

Etape 1 : Donner une adresse IP au switch

```
switch>ena
switch#conf t
switch(config)#inter vlan1
switch(config)#ip address 192.168.1.10 255.255.255.0
switch(config)#no shut
switch(config)#exit
switch#sh ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.10	YES	NVRAM	up	up
FastEthernet1/0/1	unassigned	YES	unset	up	up

```
--- more ---
```

Etape 2 : Envoyer le fichier via TFTP

Dans cet exemple mon fichier se nomme : `c3750me-i5-mz.122-35.SE5.bin`

Une fois votre serveur TFTP prêt, nous pouvons envoyer le fichier

```
switch#copy tftp flash
Address or name of remote host[]? 192.168.1.100
Source filename[]? c3750me-i5-mz.122-35.SE5.bin
Destination filename [c3750me-i5-mz.122-35.SE5.bin]?
Accessing tftp://192.168.1.100/c3750me-i5-mz.122-35.SE5.bin...
Loading c3750me-i5-mz.122-35.SE5.bin from 192.168.1.100 (via FastEthernet1/0/1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 47396548 bytes]

47396548 bytes copied in 190.536 secs (248754 bytes/sec)
switch#
```

Ligne 2 : Entrer l'adresse IP de votre serveur TFTP

Ligne 3 : Entrer le nom de la version

Ligne 4 : Faite Entrer

Etape 3 : Vérification que le fichier est bien sur le switch

```
switch#show flash:
```

```
Directory of flash:/
```

```
 3 -rwx   9227723  Mar 1 1993 01:19:47 +01:00  c3750me-i5-mz.122-35.SE5.bin
 4 -rwx      1824  Sep 30 2021 10:28:02 +02:00  config.text
 5 -rwx        5   Sep 30 2021 10:28:02 +02:00  private-config.text
93 -rwx      564   Mar 1 1993 01:00:42 +01:00  vlan.dat
```

```
32514048 bytes total (10499072 bytes free)
```

```
switch#
```

Etape 4 : Démarrer sur la bonne version

```
switch#conf t
```

```
switch(config)#boot system flash:c3750me-i5-mz.122-35.SE5.bin
```

```
switch(config)#do wr
```

```
Building configuration...
```

```
[OK]
```

```
switch(config)#exit
```

```
switch#reload
```

Etape 5 : Vérification de la version

```
switch#sh ver
```

```
Cisco IOS Software, C3750ME Software (C3750ME-I5-M), Version 12.2(35)SE5, RELEASE SOFTWARE (fc1)
```

```
Copyright (c) 1986-2007 by Cisco Systems, Inc.
```

```
Compiled Thu 19-Jul-07 22:47 by nachen
```

```
Image text-base: 0x00003000, data-base: 0x01534800
```

```
ROM: Bootstrap program is C3750 boot loader
```

```
BOOTLDR: C3750ME Boot Loader (C3750ME-HBOOT-M) Version 12.1(14r)AX, RELEASE SOFTWARE (fc1)
```

switch uptime is 6 minutes
System returned to ROM by power-on
System restarted at 10:24:42 GMT+2 Thu Sep 30 2021
System image file is "flash:/c3750me-i5-mz.122-35.SE5.bin"

cisco ME-C3750-24TE (PowerPC405) processor (revision K0) with 118784K/12280K bytes of memory.
Processor board ID FDO1521Y24L
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
4 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
--More--

Etape 6 : Supprimer la version précédente

```
switch#sh flash
```

Directory of flash:/

3	-rwx	9227723	Mar 1 1993 01:19:47 +01:00	c3750me-i5-mz.122-35.SE5.bin
4	-rwx	1824	Sep 30 2021 10:28:02 +02:00	config.text
5	-rwx	5	Sep 30 2021 10:28:02 +02:00	private-config.text
6	-rwx	9047723	Mar 1 1993 01:19:47 +01:00	c3750me-i5-mz.122-35.SE1.bin
93	-rwx	564	Mar 1 1993 01:00:42 +01:00	vlan.dat

32514048 bytes total (10499072 bytes free)

```
switch#delete flash:c3750me-i5-mz.122-35.SE1.bin
```

Delete filename [c3750me-i5-mz.122-35.SE1.bin]?

Delete flash:c3750me-i5-mz.122-35.SE1.bin? [confirm]

```
switch#
```

```
switch#sh flash
```

Directory of flash:/

3	-rwx	9227723	Mar 1 1993 01:19:47 +01:00	c3750me-i5-mz.122-35.SE5.bin
4	-rwx	1824	Sep 30 2021 10:28:02 +02:00	config.text
5	-rwx	5	Sep 30 2021 10:28:02 +02:00	private-config.text
93	-rwx	564	Mar 1 1993 01:00:42 +01:00	vlan.dat

Le switch est maintenant à jour

Supprimer la configuration en mode rommon

Si vous voulez supprimer la configuration d'un switch mais que vous n'avez pas le mot de passe, il faut alors démarrer le switch en mode rommon.

Si le switch est sous tension, débranchez-le. Appuyez sur le bouton "Mode", et maintenez cet appui tout en mettant sous tension le switch. Restez appuyé jusqu'à ce que le voyant "LED STAT" devienne vert fixe puis vert clignotant.

Vous devriez arriver sur ce prompt :

cisco-rommon-1.png

Etape 1 : Initialiser la flash et le boot

```
switch: flash_init
```

```
switch: boot
```

Etape 2 : Lister les fichiers

```
switch: dir flash:
```

Etape 3 : Supprimer le fichier de configuration

```
switch: delete flash:config.text
```

```
Are you sure you want to delete "flash:config.txt" (y/n) ?y
```

Etape 4 : Redémarrer le switch

```
switch: reset
```

cisco-rommon-2.png

Configuration des VLAN

Virtual Local Area Network

Introduction

Nous allons créer et améliorer le réseau suivant :

cisco-vlan-1.png

Configuration du routeur

```
router>ena
router#conf t
router(config)#interface GigabitEthernet0/0
router(config-if)#ip address 192.168.1.1 255.255.255.0
router(config-if)#description lan
router(config-if)#exit
router(config)#interface GigabitEthernet0/1
router(config-if)#ip address 10.0.0.1 255.255.255.0
router(config-if)#description admin
router(config-if)#exit
router(config)#interface Vlan1
router(config-if)#no ip address
router(config-if)#exit
router(config)#
```

Configuration des switches (les interfaces changent en fonction du switch voir le schéma ci-dessus)

```
switch>ena
switch#conf t
switch(config)#hostname switch1
switch1(config)#vlan 100
switch1(config-vlan)#name data
switch1(config-vlan)#exit
switch1(config)#vlan 200
switch1(config-vlan)#name admin
switch1(config-vlan)#exit
```

```
switch1(config)#vlan 300
switch1(config-vlan)#name voix
switch1(config-vlan)#exit
switch1(config)#interface FastEthernet0/1
switch1(config-if)#switchport mode access
switch1(config-if)#switchport access vlan 200
switch1(config-if)#exit
switch1(config)#interface FastEthernet0/2
switch1(config-if)#switchport mode access
switch1(config-if)#switchport access vlan 100
switch1(config-if)#exit
switch1(config)#interface GigabitEthernet0/1
switch1(config-if)#switchport mode trunk
switch1(config-if)#switchport nonegotiate
switch1(config-if)#exit
switch1(config)#interface GigabitEthernet0/2
switch1(config-if)#switchport mode trunk
switch1(config-if)#switchport nonegotiate
switch1(config-if)#exit
switch1(config)#interface Vlan200
switch1(config-if)#ip address 10.0.0.2 255.255.255.0
switch1(config-if)#no shutdown
switch1(config-if)#exit
switch1(config)#
```

Les ports entre les switches sont des Trunks et les ports entre switch et ordinateur sont des Access

Etudions cette configuration

Créer un VLAN

```
switch#conf t
switch(config)#vlan 100
```

Nommer un VLAN

```
switch#conf t
switch(config)#vlan 100
switch(config-vlan)#name DATA
```

Supprimer un VLAN

```
switch#conf t
switch(config)#no vlan 100
```

ou

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

Lieu de stockage des VLANs

```
switch#dir flash:
Directory of flash:/

 1 -rw-   4670455      <no date> 2960-lanbasek9-mz.150-2.SE4.bin
 4 -rw-    1334       <no date>  config.text
 3 -rw-     736       <no date>  vlan.dat

64016384 bytes total (59343859 bytes free)
switch#
```

Assigner une adresse IP à un VLAN

```
switch#conf t
switch(config)#interface vlan 200
switch(config-if)#ip address 10.0.0.5 255.255.255.0
switch(config-if)#no shut
```

Configurer les ports en mode Access

```
switch#conf t
switch(config)#interface fastethernet 0/1
switch(config-if)#switchport mode access
```

On assigne ensuite un vlan

```
switch(config-if)#switchport access vlan 100
```

Configurer les ports en mode Trunk

```
switch(config)#interface fastEthernet 0/1
switch(config-if)#switchport mode trunk
```


Si cette commande vous retourne :

```
switch(config-if)#switchport mode trunk
```

Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode

Changer le mode d'encapsulation

```
switch(config-if)#switchport trunk encapsulation dot1q
```

Puis désactiver l'envoi de DTP

```
switch(config-if)#switchport nonegotiate
```

Configuration un peu plus poussé

Lorsque l'on passe un port en mode Trunk, il faut paramétrer le VLAN natif

```
switch(config-if)#switchport trunk native vlan 100
```

Nous pouvons aussi autoriser seulement quelques VLAN à passer par le Trunk

```
switch(config-if)#switchport trunk allowed vlan add 200
```

```
switch(config-if)#switchport trunk allowed vlan add 300
```

N'autoriser aucun VLAN à passer par le Trunk

```
switch(config-if)#switchport trunk allowed vlan none
```

Commandes utiles

```
switch#sh vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
100 data	active	Fa0/2
200 admin	active	Fa0/1

```
300 voix active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
switch#
```

```
switch#sh vlan id 100
```

VLAN Name	Status	Ports
-----------	--------	-------

100 data	active	Fa0/2
----------	--------	-------

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
-----------	------	-----	--------	--------	----------	-----	----------	--------	--------

100 enet	100100	1500	-	-	-	-	0	0
----------	--------	------	---	---	---	---	---	---

```
switch#
```

Configuration VLAN voix, QOS, LLDP et CDP

LLDP : Link Layer Discovery Protocol
CDP : Cisco Discovery Protocol

Introduction

Nous allons voir comment implémenter un VLAN voix dans notre topologie. Puis utiliser le LLDP et CDP

cisco-vlan-2.png

J'ai ajouté un serveur voix et deux téléphones IP sur le réseau.

Configuration des switches

Nous avons déjà configuré les Trunks entre les switches donc le VLAN Voix est déjà propagé sur le réseau.

Il nous reste qu'à configurer les ports sur lesquels nous allons brancher nos téléphones IP

Exemple sur le Switch4 port f0/1 (IP Phone1)

```
switch4(config)#int fastEthernet 0/1
switch4(config-if)#spanning-tree portfast
switch4(config-if)#switchport mode access
switch4(config-if)#switchport access vlan 100
switch4(config-if)#switchport voice vlan 300
```

Ou :

```
switch4(config)#int fastEthernet 0/1
switch4(config-if)#spanning-tree portfast
switch4(config-if)#switchport mode trunk
switch4(config-if)#switchport trunk native vlan 100
switch4(config-if)#switchport trunk allowed vlan 300
```

```
switch4(config-if)#switchport trunk allowed vlan add 100
```

On notera que le port du switch3 sur lequel sont branchés à la fois un téléphone IP et un ordinateur a exactement cette configuration

Le port du switch tag les trames voix et laisse passer les trames du vlan data.

Le téléphone va monter automatiquement dans le VLAN voix et le pc dans le VLAN data grâce au protocole CDP ou LLDP

Protocole CDP

Le CDP est un protocole de découverte du réseau propriétaire Cisco. C'est grâce à lui que les périphériques montent dans les bons VLAN

Il est activé par défaut sur les switchs Cisco

Activer le CDP

```
switch#cdp run
```

Désactiver le CDP

```
switch#no cdp run
```

Protocole LLDP

Le CDP est un protocole de découverte du réseau. C'est grâce à lui que les périphériques montent dans les bons VLAN

Activer le LLDP

```
switch#lldp run
```

Désactiver le LLDP

```
switch#no lldp run
```

QOS Voix

Configuration de la QOS sur les ports utilisant le vlan voix

La QOS va de 0 à 7, plus la valeur est élevée plus la trame est prioritaire.

```
switch4(config)#interface fastEthernet 0/1
switch4(config-if)#mls QOS trust cos
switch4(config-if)#mls qos cos 6
```

Exemple avec poste voip Cisco

```
switch(config)#int fa 1/0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 101
switch(config-if)#switchport voice vlan 100
switch(config-if)#mls qos voip cisco-phone
switch(config-if)#spanning-tree portfast
switch(config-if)#mls qos trust cos
switch(config-if)#mls qos trust device cisco-phone
switch(config-if)#srr-queue bandwidth share 10 10 60 20
switch(config-if)#srr-queue bandwidth shape 10 0 0 0
```

La ligne 9 sert à segmenter la mémoire tampon en 4 files d'attentes : Q1, Q2, Q3 et Q4. Les nombres sont des pourcentages. Sur 100% de la mémoire, 10% seront alloué à Q1, 10% à Q2, 60% à Q3 et 20% à Q4.

Configuration de Telnet, SSH et WEB

Configuration de Telnet

Terminal network

Voici comment configurer Telnet sur un switch

```
switch(config)#int vlan 1
switch(config-if)#ip address 192.168.1.1 255.255.255.0
switch(config-if)#exit
switch(config)#line vty 0 15
switch(config-line)#transport input telnet
switch(config-line)#login local
switch(config-line)#password cisco
switch(config-line)#login
switch(config-line)#exit
switch(config)#
```

Configuration de SSH

Secure Shell

Voici comment configurer SSH sur un switch

```
switch(config)#int vlan 1
switch(config-if)#ip address 192.168.1.1 255.255.255.0
switch(config-if)#exit
switch(config)#hostname dc1-sw0
dc1-sw0(config)#ip domain-name network.net
dc1-sw0(config)#crypto key generate rsa
The name for the keys will be: dc1-sw0.network.net
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]

```
dc1-sw0(config)#  
dc1-sw0(config)#ip ssh version 2  
dc1-sw0(config)#ip ssh authentication-retries 3  
dc1-sw0(config)#ip ssh time-out 120  
dc1-sw0(config)#line vty 0 15  
dc1-sw0(config-line)#transport input ssh  
dc1-sw0(config-line)#login local  
dc1-sw0(config-line)#password cisco  
dc1-sw0(config-line)#login  
dc1-sw0(config-line)#exit
```

Pour configurer SSH, il faut renommer le switch et lui donner un nom de domaine. lignes 4 et 5

Puis générer une clef RSA entre 1024 et 2048 bits

Configuration de l'accès WEB

World Wide Web

Voici comment configurer web sur un switch

```
switch(config)#ip http server  
switch(config)#ip http authentication local  
switch(config)#ip http timeout-policy idle 600
```

ou en HTTPS :

```
switch(config)#ip http secure server  
switch(config)#no ip http server  
switch(config)#ip http authentication local  
switch(config)#ip http timeout-policy idle 600
```

Configuration de l'Etherchannel

Etherchannel permet l'agrégation de lien. Il est utilisé pour augmenter la bande passante entre deux switches.

Introduction

Nous allons utiliser la topologie suivante :cisco-lacp.png

LACP

Configuration sur le 3750

```
3750#conf t
3750(config)#interface range fastEthernet 1/0/1 - 2
3750(config-if-range)#channel-protocol lacp
3750(config-if-range)#channel-group 1 mode active
```

Configuration sur le 3550

```
3550#conf t
3550(config)#interface range fastEthernet 0/1 - 2
3550(config-if-range)#channel-protocol lacp
3550(config-if-range)#channel-group 1 mode active
```

Vérification

```
3750#sh interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
Hardware is EtherChannel, address is 2037.0606.7484 (bia 2037.0606.7484)
MTU 1500 bytes, BW 200000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Full-duplex, 100Mb/s, link type is auto, media type is unknown
input flow-control is off, output flow-control is unsupported
```



```
Members in this channel: Fa1/0/1 Fa1/0/2
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:21:40, 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 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  1153 packets input, 132950 bytes, 0 no buffer
    Received 895 broadcasts (0 multicasts)
      0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 895 multicast, 0 pause input
    0 input packets with dribble condition detected
  490 packets output, 66172 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
```

3750#

- Ligne 2 : Le port-channel 1 est passé UP
- Ligne 4 : BW (bandwidth) est à 200Mbps (2x100Mbps)
- Ligne 9 : Membres Fa1/0/1 et Fa1/0/2

PAGP

Le PAgP est un protocole propriétaire Cisco. Il se configure comme suit :

Configuration sur le 3750

```
3750#conf t
3750(configure)#interface range f1/0/1 - 2
3750(configure-if-range)#channel-group 2 mode auto
3750(configure-if-range)#end
```

Configuration sur le 3550

```
3550#conf t
3550(configure)#interface range f0/1 - 2
3550(configure-if-range)#channel-group 2 mode desirable
```

```
3550(configure-if-range)#end
```

Vérification

```
3750#sh etherchannel summary
```

Flags: D - down P - in port-channel

 I - stand-alone s - suspended

 H - Hot-standby (LACP only)

 R - Layer3 S - Layer2

 U - in use f - failed to allocate aggregator

 u - unsuitable for bundling

 w - waiting to be aggregated

 d - default port

Number of channel-groups in use: 1

Number of aggregators: 1

Group	Port-channel	Protocol	Ports
-------	--------------	----------	-------

2	Po2(SU)	PAgP	Fa1/0/1(P) Fa1/0/2(P)
---	---------	------	-----------------------

```
3750#
```

Load Balancing

Vérification du mode de load balancing

```
3750#sh etherchannel load-balance
```

EtherChannel Load-Balancing Configuration:

 src-mac

EtherChannel Load-Balancing Addresses Used Per-Protocol:

Non-IP: Source MAC address

 IPv4: Source MAC address

 IPv6: Source MAC address

```
3750#
```

Ici la répartition de la charge s'effectue par l'adresse mac source. Ce paramètre est modifiable en fonction du niveau de votre switch. Au niveau 2 la répartition peut se faire à partir des adresses

mac et au niveau 3 via les adresses mac et/ou adresse ip.

```
3750(config)#port-channel load-balance ?  
dst-ip      Dst IP Addr  
dst-mac     Dst Mac Addr  
src-dst-ip  Src XOR Dst IP Addr  
src-dst-mac Src XOR Dst Mac Addr  
src-ip      Src IP Addr  
src-mac     Src Mac Addr
```

```
3750(config)#port-channel load-balance
```

Le 3750 étant un switch de niveau 3, j'ai accès à tous les modes.

Agrégation de niveau 3

Cette partie est en bêta

Configuration sur le 3750

```
3750(config)#interface range fastEthernet 1/0/1 - 2  
3750(config-if-range)#channel-group 3 mode on  
3750(config-if-range)#no switchport  
3750(config-if-range)#exit  
3750(config-if)#exit  
3750(config)#interface port-channel 3  
3750(config-if)#no switchport  
3750(config-if)#ip address 10.0.0.1 255.255.255.0  
3750(config-if)#no shutdown  
3750(config-if)#exit  
3750(config)#ip routing  
3750(config)#router ospf 1  
3750(config-router)#network 10.0.0.0 0.0.0.255 area 0  
3750(config-router)#exit  
3750(config)#do wr
```

Configuration sur le 3550

```
3550(config)#interface range fastEthernet 0/1 - 2  
3550(config-if-range)#channel-group 3 mode on
```

```

3550(config-if-range)#no switchport
3550(config-if-range)#exit
3550(config-if)#exit
3550(config)#interface port-channel 3
3550(config-if)#no switchport
3550(config-if)#ip address 10.0.0.2 255.255.255.0
3550(config-if)#no shutdown
3550(config-if)#exit
3550(config)#ip routing
3550(config)#router ospf 1
3550(config-router)#network 10.0.0.0 0.0.0.255 area 0
3550(config-router)#exit
3550(config)#do wr

```

Vérification de l'OSPF

```
3750#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.3.202	1	FULL/BDR	00:00:30	10.0.0.2	Port-channel3

```
3750#
```

```
3750#sh ip route
```

Codes: C - connected, S - static, 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

i - IS-IS, su - IS-IS summary, 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, 1 subnets

C 172.16.3.0 is directly connected, Vlan1

10.0.0.0/24 is subnetted, 1 subnets

C 10.0.0.0 is directly connected, Port-channel3

Test de ping entre les deux switchs

```
3750#ping 10.0.0.2
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms

```
3750#
```

Configuration du NTP

Network Time Protocol

Introduction

Pour effectuer une synchronisation NTP, il faut tout d'abord que le switch puisse aller sur internet

```
switch>ena
switch#conf t
switch(config)#interface vlan1
switch(config-if)#ip address 192.168.1.200 255.255.255.0
switch(config-if)#exit
switch(config)#ip default-gateway 192.168.1.1
switch(config)#ip name-server 192.168.1.1
switch(config)#exit
switch#
```

Passons à la configuration du NTP

```
switch#
switch#conf t
switch(config)#ntp server 194.2.0.28 prefer
switch(config)#ntp server 194.2.0.58
switch(config)#clock timezone GMT+1 1
switch(config)#exit
switch#
```

194.2.0.28 et 194.2.0.58 sont les NTP de Orange Business Services

`switch(config)#clock timezone GMT+1 1` Le fuseau horaire GMT+1 Paris suivi de l'offset +1h

Configuration heure d'été/hiver

```
switch(config)#clock summer-time GMT+2 recurring last Sun Mar 3:00 last Sun Oct 3:00
```

Vérification

```
Switch#show ntp status
```

```
Clock is synchronized, stratum 2, reference is 194.2.0.28
```

```
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
```

```
reference time is DC63A7AF.C4F5B5D8 (19:28:31:769 GMT Sun Sep 26 2021)
```

```
clock offset is 0.9588 msec, peer dispersion is 0.08 msec
```

```
Switch#show clock detail
```

```
19:29:41.513 GMT Sun Sep 26 2021
```

```
Time source is NTP
```

```
Switch#show clock
```

```
.19:30:00.251 GMT Sun Sep 26 2021
```

Le switch est maintenant à l'heure

Il est aussi possible de régler l'heure et la date à la main

```
switch#clock set 20:30:00 21 feb 2021
```

Configuration de Syslog

Transmission de journaux

Introduction

Les logs sont classés selon leur gravité :

0	Urgences "emergencies"
1	Alertes "alerts"
2	Critiques "critical"
3	Erreurs "errors"
4	Avertissements "warning"
5	Notifications "notifications"
6	Informationnel "informational"
7	Débogage "debuggin"

Par défaut, tous les messages sont affichés dans la console, si nous voulons afficher seulement les messages importants, il faut utiliser la commande suivante :

```
switch(config)#logging console errors
```

Les messages entre la gravité 0 et 3 seront affichés.

Afficher l'historique des logs

```
switch#show logging history
```

Les logs sont archivés dans la RAM ! Ils sont donc perdus à chaque redémarrage du switch

Envoyer les logs sur un serveur syslog

```
switch(config)#logging 192.168.1.100  
switch(config)#logging trap 7
```


logging trap 7 permet d'envoyer les 8 niveaux de log

Configuration des ports

Introduction

Nous allons voir comment configurer les ports de notre switch

Vitesse

Pour passer un port Giga en 100Mb/s

```
switch(config)#int gig 0/1  
switch(config-if)#speed 100
```

Les commandes disponibles sont :

```
switch(config-if)#speed 10  
switch(config-if)#speed 100  
switch(config-if)#speed 1000  
switch(config-if)#speed auto
```

Duplex

```
switch(config-if)#duplex full  
switch(config-if)#duplex half  
switch(config-if)#duplex auto
```

Description

```
switch(config-if)#description vers switch 2 port 0/3
```

POE

```
switch(config-if)#power inline auto  
switch(config-if)#power inline never  
switch(config-if)#exit  
switch(config)#do sh power inline gig 0/1
```

Port mirroring

Nous allons récupérer le trafic Tx et Rx du port fastEthernet 0/1

```
switch(config)#monitor session 1 source interface fa 0/1 both
```

Et le rediriger vers le port fastEthernet 0/2

```
switch(config)#monitor session 1 destination interface fastEthernet 0/2
```

Afficher les traces

```
switch#sh monitor detail  
No SPAN configuration is present in the system.
```

Désactivation

```
switch(config)#no monitor session all
```

Configuration de Port-security

Introduction

Nous allons voir comment implémenter de la sécurité sur nos switchs

Configuration du Port security

Il faut tout d'abord configurer le port en mode access

```
switch(config)#int fa0/1  
switch(config-if)#switchport mode access
```

Puis activer le port security

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

Pour n'autoriser qu'une seule adresse MAC à se connecter au switch

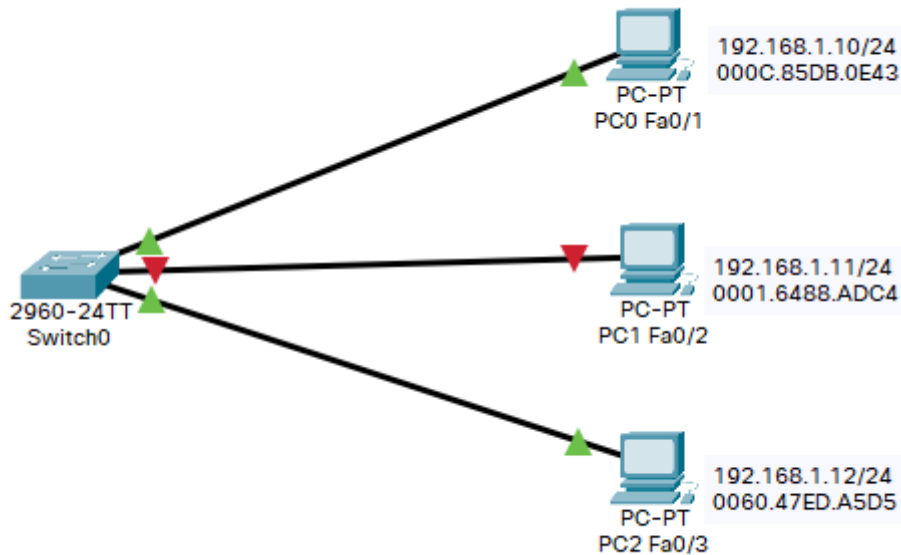
```
switch(config-if)#switchport port-security maximum 1
```

Evidement, s'il y a un téléphone IP + un PC, il faudra mettre le paramètre sur 2

Il existe 3 options pour la gestion des adresses MAC :

1. Dynamic : Le switch apprend les adresses MAC automatiquement
2. Static : Nous devons configurer l'adresse MAC manuellement
3. Sticky : Le switch apprend les adresses MAC automatiquement et les ajoute à la conf

Pour la suite, je vais me baser sur cette topologie :



Configuration de fastEthernet 0/1

```
switch(config)#interface FastEthernet0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport port-security
switch(config-if)#switchport port-security mac-address 000C.85DB.0E43
```

Configuration de fastEthernet 0/2

```
switch(config)#interface FastEthernet0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport port-security
switch(config-if)#switchport port-security mac-address 000C.85DB.0E42
```

Configuration de fastEthernet 0/3

```
switch(config)#interface FastEthernet0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport port-security
switch(config-if)#switchport port-security mac-address sticky
```

Il faut ensuite configurer la violation

Dès qu'une des règles ci-dessus n'est pas respectées, nous avons plusieurs solutions.

1. Mode shutdown : Va désactiver le port
2. Mode protect : les trames des adresses mac non renseignées sont ignorées par le switch

3. Mode restrict : fonctionne comme le mode protect mais en plus, un message snmp est envoyé et peut aussi être récupéré par un serveur syslog

Sur mon exemple, les ports fastEthernet 0/1 et 0/2 ont été configurés en mode shutdown

```
switch(config-if)#switchport port-security violation shutdown
```

le port fastEthernet 0/3 en mode restrict

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

PC0 : L'adresse MAC est entrée en mode statique dans le switch, et elle correspond à l'adresse MAC du pc, donc rien ne se passe

PC1 : L'adresse MAC est entrée en mode statique dans le switch, mais ne correspond à l'adresse MAC du pc, le port est shutdown

PC2 : L'adresse MAC est apprise par le switch et correspond à l'adresse MAC du pc, rien ne se passe. Si toutefois nous branchons un autre pc, le port bloquera tout le trafic et enverra des trames d'erreur.

Configuration du STP

Spanning Tree Protocol

Introduction

Le Spanning Tree est un protocole qui permet d'éviter les boucles réseau.

Par défaut, le Spanning Tree est activé sur tous les switchs Cisco.

```
switch#sh run | include spanning-tree
spanning-tree mode pvst
spanning-tree extend system-id
switch#
```

Pour l'exemple, je vais utiliser le schéma ci-dessous :

cisco-stp-1.png

Je possède de 3 switchs, un 3750, un 3550 et un 2960. Je les ai relié entre eux comme ci-dessus.

Comme le STP est activé par défaut, nous voyons que le port 1/0/23 du 3750 a été shutdown par le STP pour éviter une boucle réseau.

Dans cette configuration, le 3550 a été élu RootBridge. Mais comment se déroule cette élection ?

Par défaut, les switchs ont tous la même priorité qui est de 32769 donc ils sont tous égaux.

```
3750#sh spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
    Root ID    Priority    32769
              Address     000e.83c5.be80
```

Quand les priorités des switchs sont les mêmes, l'élection va se baser sur la plus petite adresse mac. Dans mon cas c'est le 3550 qui a la plus petite donc qui gagne le rôle de RootBridge.

Le 2960 n'a pas de liaison active vers le 3750, donc les flux doivent passer par le 3550 pour atteindre le 3750.

Au niveau des switch :

```
3750#sh spanning-tree
```

```
VLAN0001
```

```
Spanning tree enabled protocol rstp
```

```
Root ID   Priority   32769
```

```
Address   000e.83c5.be80
```

```
Cost      19
```

```
Port      26 (FastEthernet1/0/24)
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority   32769 (priority 32768 sys-id-ext 1)
```

```
Address   2037.0606.7480
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Aging Time 300
```

```
Interface      Role Sts Cost      Prio.Nbr Type
```

```
-----
```

```
Fa1/0/23      Altn BLK 19      128.25  P2p
```

```
Fa1/0/24      Root FWD 19      128.26  P2p
```

```
3750#
```

```
2960#sh spanning-tree
```

```
VLAN0001
```

```
Spanning tree enabled protocol rstp
```

```
Root ID   Priority   32769
```

```
Address   000e.83c5.be80
```

```
Cost      19
```

```
Port      7 (FastEthernet0/7)
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority   32769 (priority 32768 sys-id-ext 1)
```

```
Address   0027.0c3a.fc00
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Aging Time 300 sec
```

```
Interface      Role Sts Cost      Prio.Nbr Type
```



```
-----
Fa0/7      Root FWD 19    128.7  P2p
Fa0/8      Desg FWD 19    128.8  P2p
```

2960#

3550#sh spanning-tree

VLAN0001

Spanning tree enabled protocol rstp

Root ID Priority 32769

Address 000e.83c5.be80

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 000e.83c5.be80

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300 sec

```
Interface      Role Sts Cost    Prio.Nbr Type
-----
```

```
Fa0/23      Desg FWD 19    128.23  P2p
```

```
Fa0/24      Desg FWD 19    128.24  P2p
```

3550#

Ici nous avons les informations :

- Les deux ports du 3550 sont en mode DESG "Désigné"
- Le port 0/7 du 2960 est en mode ROOT et le 0/8 en DESG
- Le port 1/0/24 du 3750 est en mode ROOT et le 1/0/23 en ALTN "Alternatif"

Les ports qui font face au switch RootBridge sont automatiquement en mode ROOT.

Nous apprenons aussi que le switch 3550 est le RootBridge [This bridge is the root] .

Dans cette configuration, si le câble RJ45 entre les switch 3550 et 2960 est déconnecté, le rétablissement du port 1/0/23 du 3750 va prendre un certain temps. Cependant, nous pouvons accélérer le processus.

Mode rapid-pvst

Afin de rendre le processus Spanning Tree plus rapide, nous allons mettre en place le protocole Rapid PVST.

Cette commande sera à passer sur tous les switchs

```
Switch(config)#spanning-tree mode rapid-pvst
```

Une fois le rapid-pvst activé, le rétablissement de port alternatif prend maximum 15sec

Mode port-fast

Nous pouvons désactiver le STP sur les ports où sont connectés les PC / Serveur pour éviter que le port mette 30sec à monter.

```
switch#conf t
switch(config)#interface fastEthernet 0/1
switch(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet1/0/1 but will only
have effect when the interface is in a non-trunking mode.
```

Storm Control

Il existe une fonctionnalité qui permet de limiter les tempêtes de broadcast.

Cette commande permet de limiter à 10% la bande passante utilisée par le broadcast

```
switch(config)#interface FastEthernet 0/1
switch(config-if)#storm-control broadcast level 10
```

En cas d'excès de broadcast, nous pouvons bloquer le port en question

```
switch(config)#interface FastEthernet 0/1
switch(config-if)#storm-control action shutdown
```

Avec cette commande, le trafic de broadcast sera bloqué s'il dépasse 30%, et ne sera autorisé à nouveau que s'il tombe en dessous de 10%

```
switch(config)#interface FastEthernet 0/1
switch(config-if)#storm-control broadcast level 30 10
```

Choisir le switch RootBridge

```
switch#conf t
switch(config)#spanning-tree vlan 1 root primary
switch(config)#do show run | include priority
spanning-tree vlan 1 priority 24576
switch(config)#
```

On peut aussi fixer la priorité à la main

```
switch(config)#spanning-tree vlan 1 priority 4096
```

Je viens de passer le 3750 RootBridge, voici ce qu'il se passe :

cisco-stp-2.pngcisco-stp-3.png

Le 3750 est bien passé RootBridge et sa priorité est passée de 32769 à 24576

```
switch#show run | include priority
spanning-tree vlan 1 priority 24576
```

Coût des interfaces

Bande passante	Coût STP	Coût RSTP
10 Mbps	250	5.000.000
100 Mbps	19	200.000
1 Gbps	4	20.000
10 Gbps	2	2.000
100 Gbps	1	200

Encore une fois avec la commande show spanning-tree, nous pouvons voir le coût des interfaces.

```
3750#sh spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    24577
             Address     2037.0606.7480
```

```
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 24577 (priority 24576 sys-id-ext 1)
Address 2037.0606.7480
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type

Fa1/0/23	Desg	FWD	19	128.25	P2p
Fa1/0/24	Desg	FWD	19	128.26	P2p

```
3750#
```

Mes deux liens sont en 100 Mbps ce qui correspond à un coût de 19.

Nous pouvons modifier ce coût avec la commande

```
switch#conf t
switch(config)#interface FastEthernet 1/0/23
switch(config-if)#spanning-tree cost 50
switch(config-if)#exit
```

résultat :

```
3750#sh spanning-tree

VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 24577
Address 2037.0606.7480
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24577 (priority 24576 sys-id-ext 1)
Address 2037.0606.7480
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
```

```
-----  
Fa1/0/23      Desg FWD 50      128.25  P2p  
Fa1/0/24      Desg FWD 19      128.26  P2p
```

```
3750#
```

BPDU "Bridge Protocol Data Unit"

Les trames BPDU sont utilisées par le STP pour vérifier l'état des liens entre les switchs. Elle ne sont cependant pas utiles sur les ports faisant face à des machines.

En activant le BPDU Guard sur un port, ce dernier va se désactiver s'il reçoit une trame BPDU.

```
switch#conf t  
switch(config)#interface fastEthernet 0/1  
switch(config-if)#spanning-tree bpduguard enable
```

Nous pouvons aussi désactiver l'envoi de trames

```
switch#conf t  
switch(config)#interface fastEthernet 0/1  
switch(config-if)#spanning-tree bpdufilter enable
```

Commandes utiles

```
3750#sh spanning-tree summary  
Switch is in rapid-pvst mode  
Root bridge for: VLAN0001  
EtherChannel misconfig guard is enabled  
Extended system ID      is enabled  
Portfast Default        is disabled  
PortFast BPDU Guard Default is disabled  
Portfast BPDU Filter Default is disabled  
Loopguard Default       is disabled  
UplinkFast              is disabled  
BackboneFast            is disabled  
Configured Pathcost method used is short
```

```
Name          Blocking Listening Learning Forwarding STP Active  
-----  
VLAN0001      0      0      0      3      3
```

1 vlan 0 0 0 3 3

3750#

Configuration du DHCP

DHCP: Dynamic Host Configuration Protocol

Introduction

Nous allons voir comment configurer un serveur DHCP sur un switch

Configuration

```
switch(config)#ip dhcp pool lan-data
switch(dhcp-config)#default-router 192.168.1.1
switch(dhcp-config)#network 192.168.1.0 255.255.255.0
switch(dhcp-config)#dns-server 192.168.1.1
switch(dhcp-config)#exit
switch(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.2
```

Si le serveur dhcp se trouve sur un autre réseau

Il faut activer le DHCP Relay

```
switch(config)#int vlan 100
switch(config-if)#ip helper-address 172.16.3.100
```

vérification

```
switch#sh ip dhcp relay information trusted-sources
List of trusted sources of relay agent information option:
```

DHCP Snooping

Le DHCP Snooping permet de filtrer les messages DHCP sur le switch. Il existe deux modes :

1. Trusted : Un serveur DHCP peut se trouver sur ce port
2. unTrusted : Un serveur DHCP ne peut pas se trouver sur ce port

```
switch(config)#ip dhcp snooping
switch(config)#ip dhcp snooping vlan 1
```

```
switch(config)#interface fa 0/1  
switch(config-if)#ip dhcp snooping trust  
switch(config-if)#ip dhcp snooping untrust
```

Vérification

```
switch#sh ip dhcp snooping  
switch#sh ip dhcp snooping database  
switch#sh ip dhcp snooping statistics  
switch#sh ip dhcp snooping statistics detail
```


Configuration de la bannière

Introduction

Nous allons voir comment configurer la bannière.

Bannière MOTD

La banner MOTD est affichée à chaque connexion à l'équipement.

```
switch(config)#banner motd #  
Enter TEXT message. End with the character '#'  
*****  
  
* accès interdit aux personnes non autorisées *  
*****  
  
#  
switch(config)#
```

Bannière LOGIN

La banner login est affichée à chaque connexion avec un identifiant

```
switch(config)#banner login #  
Enter TEXT message. End with the character '#'  
*****  
  
* accès interdit aux personnes non autorisées *  
*****  
  
#  
switch(config)#
```

Configuration 802.1X

Introduction

L'IEEE 802.1X permet d'authentifier les utilisateurs sur le réseau.

Configuration

Activation de AAA

```
switch(config)#aaa new-model
```

Spécifiez l'adresse du serveur RADIUS et sa clef

```
switch(config)#radius-server host 192.168.1.100 key P@ssw0rd
```

Activation de l'authentification par RADIUS sur le switch

```
switch(config)#aaa authentication dot1x default group radius
```

Activation de 802.1X

```
switch(config)#dot1x system-auth-control
```

Configuration des ports

```
switch(config)#interface fastEthernet 0/1  
switch(config-if)#switchport mode access  
switch(config-if)#dot1x port-control auto
```

Option

Il est possible de mettre un nombre maximum d'authentifications

```
switch(config-if)#dot1x max-reauth-req 3
```

Création des vlans guest et auth-fail

Les clients non compatibles avec le 802.1X seront placés dans ce vlan

```
switch(config-if)#dot1x guest-vlan 100
```

Les clients qui ne sont pas parvenus à s'authentifier seront placés dans ce vlan

```
switch(config-if)#dot1x auth-fail vlan 101
```

Vérification

```
switch#show dot1x all summary
```

Configuration du SNMP

SNMP : Simple Network Management Protocol

Introduction

Nous allons voir comment configurer le SNMP V1,V2 et V3. Le SNMP permet de superviser des matériels à distance.

SNMP V1 et V2

Renseignez les communautés

```
switch(config)#snmp-server community public ro
switch(config)#snmp-server community private rw
```

RO pour Read Only et RW pour Read Write

Renseignez les informations du switch

```
switch(config)#snmp-server location DC1T5B2C1
switch(config)#snmp-server contact Administrateur
```

Envoi des infos vers un serveur

```
switch(config)#snmp-server host 192.168.1.100 version 2c private
switch(config)#snmp-server enable traps
switch(config)#snmp-server source-interface traps vlan 1
```

La source-interface doit avoir une adresse IP !

Vérification

```
switch#sh snmp
Chassis: FOC1335V3AP
Contact: administrateur
Location: DC1T5B2C1
0 SNMP packets input
```

```
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
0 Get-next PDUs
0 Set-request PDUs
0 Input queue packet drops (Maximum queue size 1000)
2 SNMP packets output
0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
0 Response PDUs
2 Trap PDUs
SNMP global trap: enabled

SNMP logging: enabled
  Logging to 192.168.1.100.162, 0/10, 2 sent, 0 dropped.
SNMP agent enabled
```

SNMP V3

Il existe trois niveaux de sécurité en SNMP V3 :

1. **noAuthNoPriv** : l'authentification se fait sur le nom d'utilisateur
2. **authNoPriv** : l'authentification se fait sur l'utilisateur et le mot de passe
3. **authPriv** : comme authNoPriv mais avec chiffrement

En mode noAuthNoPriv :

```
switch(config)#snmp-server group groupe1 v3 noauth
switch(config)#snmp-server user admin groupe1 v3
switch(config)#snmp-server host 192.168.1.100 version 3 noauth admin
```

En mode authNoPriv :

```
switch(config)#snmp-server group groupe1 v3 auth
switch(config)#snmp-server user admin groupe1 v3 auth sha P@ssw0rd
switch(config)#snmp-server host 192.168.1.100 version 3 auth admin
```

En mode authPriv

```
switch(config)#snmp-server group groupe1 v3 priv
```

```
switch(config)#snmp-server user admin groupe1 v3 auth sha P@ssw0rd priv des56 P@ssw0rd
```

```
switch(config)#snmp-server host 192.168.1.100 version 3 priv admin
```

Etats des ports

Introduction

Nous allons voir l'état des liens sur un switch (couleur des voyants)

Explications

Désactivé	Aucun lien, ou le port a été fermé administrativement.
Vert	Lien présent.
Ambre (Orange)	Le port est bloqué par le protocole Spanning Tree (STP) et ne transfère pas de données.
Ambre clignotant	Le port est bloqué par le STP et n'envoie aucun paquet
Vert clignotant	Activité. Le port envoie ou reçoit des données.
Vert-Ambre alterné	Défaut de liaison. Les trames d'erreur peuvent affecter la connectivité, et les erreurs telles que les collisions excessives, les erreurs de contrôle de redondance cyclique (CRC) et les erreurs d'alignement et de jabber sont surveillées pour une indication de défaut de liaison.

Importer et Exporter la configuration via TFTP

Importer une configuration depuis un serveur TFTP

```
Switch#copy tftp: startup-config  
Address or name of remote host []? 192.168.1.200  
Source filename [conf.txt]?  
Destination filename [startup-config]?  
Accessing tftp://192.168.1.200/conf.txt...
```

Exporter une configuration vers un serveur TFTP

```
Switch#copy startup-config tftp:  
Address or name of remote host []? 192.168.3.206  
Destination filename [switch-config]? config_sw_cisco.txt  
!!  
1386 bytes copied in 1.073 secs (1292 bytes/sec)  
Switch#
```


Gestion de la table ARP

Voir la table ARP

```
Switch#show arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.3.202	6	000c.29a9.2bb8	ARPA	Vlan1
Internet	192.168.3.200	0	001a.4b0b.89c5	ARPA	Vlan1
Internet	192.168.3.206	1	000c.2921.2df0	ARPA	Vlan1
Internet	192.168.3.199	-	2037.0606.74c0	ARPA	Vlan1

Effacer la table ARP

```
Switch#clear arp-cache interface fastEthernet 1/0/1
```

ou total

```
Switch#clear arp-cache
```

Client FTP

FTP : File Transfer Protocol

Introduction

Les switchs Cisco intègrent un client FTP

Explication

```
switch#copy ftp:192.168.1.10 flash:<répertoire de destination>
```

```
Address or name of remote host []? 192.168.1.10
```

```
Destination filename [config.txt]?
```

Configuration du VTP

VLAN Trunking Protocol

Introduction

Le VTP sert à propager les configurations de VLAN sur tous les switchs du réseau

Topologie du réseau :

Les liens entre les switchs doivent être des Trunks

cisco-vtp-1.png

Le 3750 aura le rôle du serveur et les deux autres de clients

Configuration de VTP

Configuration du 3750 mode serveur

```
3750(config)#vtp version 2
3750(config)#vtp domain wikidunn
3750(config)#vtp mode server
3750(config)#vtp pruning
3750(config)#vtp password cisco
```

Vérification

```
3750#sh vtp status
VTP Version                : 2
Configuration Revision      : 5
Maximum VLANs supported locally : 1005
Number of existing VLANs    : 9
VTP Operating Mode          : Server
VTP Domain Name             : wikidunn
VTP Pruning Mode            : Enabled
VTP V2 Mode                 : Enabled
VTP Traps Generation        : Disabled
```

```
MD5 digest          : 0x11 0xBC 0x91 0xDD 0x01 0xCB 0x4E 0x9C
Configuration last modified by 10.0.0.1 at 3-1-93 00:35:31
Local updater ID is 10.0.0.1 on interface VI1 (lowest numbered VLAN interface found)
3750#
```

Configuration du 3550 et 2960 en mode client

```
3550(config)#vtp version 2
3550(config)#vtp domain wikidunn
3550(config)#vtp mode client
3550(config)#vtp password cisco
```

```
2960(config)#vtp version 2
2960(config)#vtp domain wikidunn
2960(config)#vtp mode client
2960(config)#vtp password cisco
```

Retournons sur le 3750 et ajoutons des vlans

```
3750(config)#vlan 10
3750(config-if)#name admin
3750(config-if)#exit
3750(config)#vlan 100
3750(config-if)#name voix
3750(config-if)#exit
3750(config)#vlan 101
3750(config-if)#name data
3750(config-if)#exit
3750(config)#vlan 200
3750(config-if)#name wifi
3750(config-if)#exit
```

```
3750#sh vlan
```

VLAN Name	Status	Ports
1 default	active	Fa1/0/2, Fa1/0/3, Fa1/0/4 Fa1/0/5, Fa1/0/6, Fa1/0/7 Fa1/0/8, Fa1/0/9, Fa1/0/10 Fa1/0/11, Fa1/0/12, Fa1/0/13

Fa1/0/14, Fa1/0/15, Fa1/0/16
Fa1/0/17, Fa1/0/18, Fa1/0/19
Fa1/0/20, Fa1/0/21, Fa1/0/22
Fa1/0/23, Fa1/0/24, Gi1/0/1
Gi1/0/2, Gi1/1/1, Gi1/1/2

10	admin	active
100	voix	active
101	data	active
200	wifi	active
1002	fddi-default	act/unsup
1003	trcrf-default	act/unsup
1004	fddinet-default	act/unsup
1005	trbrf-default	act/unsup

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2

1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
100	enet	100100	1500	-	-	-	-	-	0	0
101	enet	100101	1500	-	-	-	-	-	0	0
200	enet	100200	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	trcrf	101003	4472	1005	3276	-	-	srb	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trbrf	101005	4472	-	-	15	ibm	-	0	0

VLAN AREHops STEHops Backup CRF

1003 7 7 off

Remote SPAN VLANs

Primary	Secondary	Type	Ports

3750#

Au bout de quelques secondes, allons voir le 2960

2960#sh vlan

VLAN Name	Status	Ports
-----------	--------	-------

1	default	active	Fa0/1, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Gi0/1
10	admin	active	
100	voix	active	
101	data	active	
200	wifi	active	
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
-----------	------	-----	--------	--------	----------	-----	----------	--------	--------

1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
100	enet	100100	1500	-	-	-	-	-	0	0
101	enet	100101	1500	-	-	-	-	-	0	0
200	enet	100200	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	trcrf	101003	4472	1005	3276	-	-	srb	0	0

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
-----------	------	-----	--------	--------	----------	-----	----------	--------	--------

1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trbrf	101005	4472	-	-	15	ibm	-	0	0

VLAN AREHops STEHops Backup CRF

1003	7	7	off
------	---	---	-----

Remote SPAN VLANs

Primary	Secondary	Type	Ports

2960#

Tous les vlans ont été créés !

Mode transparent

Il existe un 3^e mode de fonctionnement, le mode transparent.

Je reprends mon exemple et configure le 3550 en mode transparent

```
3550(config)#vtp version 2
3550(config)#vtp password cisco
3550(config)#vtp mode transparent
```

En mode transparent, le switch ne fera que relayer le VTP et ne touchera pas à ses vlans

Suppression du VTP

```
switch(config)#no vtp mode
```

Copier un IOS en mode rommon

Initialiser la flash :

```
switch: flash_init
```

Copier l'IOS en mode xmodem :

```
switch:set baud 9600  
switch: copy xmodem: flash:c3750me-i5-mz.122-35.SE5.bin
```

Dans votre logiciel terminal, sélectionner transfère de fichier > XMODEM > ENVOYER >