2016
2017

Labo Cisco :

FD

Seo-webranking

20/06/2016

Table des matières

Mise en place de l'environnement

Afin de paramétrer un commutateur Cisco Catalyst 3560G, il nous faut installer un outil de saisie de commande.

Installation de Putty

Sous Windows, Télécharger et installer le logiciel gratuit Putty.

> ***(On pourra aussi utiliser hyperterminal ou tera term pro, ou sous linux minicom)***

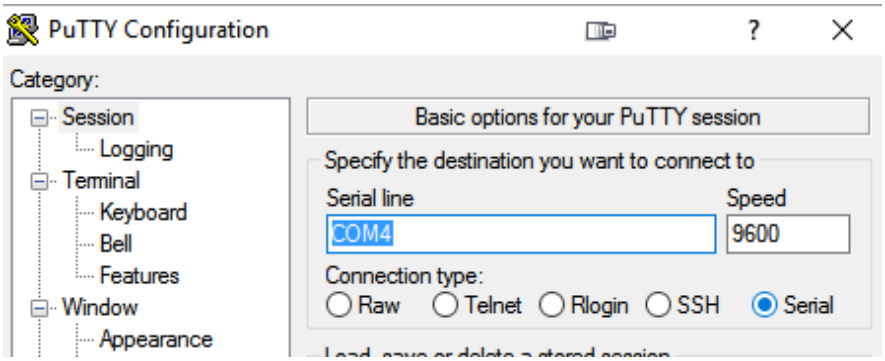
Connectiques

Il faut que votre Pc sous équipé d'une connectique série DB9, ou que vous ayez un adaptateur USB, ainsi qu'un câble console.

Port de communication

Sous Windows, repérer le nom du port de communication, via le panneau de configuration, cependant , ceci peux ne pas être nécessaire.

Connexion depuis le pc



Lancer putty, et sélectionner connexion serial sur le port adéquat.

Initialisation du périphérique

Si le commutateur démarre pour la 1^{ere} fois, il vous sera proposé des questions avec des réponses par défaut.

Paramétrage

Présentation du mode console d'un switch Cisco

Mode avec et sans privilège

Une fois connecté, nous sommes placés dans un mode sans privilège. Il est possible dans ce mode d'effectuer uniquement quelques commandes de diagnostique ou d'information. L'invite de commande du mode sans privilège est la suivante:

```
Switch>
```

Pour pouvoir modifier la configuration, il faut passer en mode privilégié en entrant la commande *"enable"*.
Présentation du passage du mode non privilégié au mode privilégié :

```
Switch>enable
Switch#
```

Console : autres modes

En fonction des commandes entrées, le switch va présenter des invites de commande différentes.
Quelques exemples d'invite de commande en fonction du contexte :

Mode configuration :

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

Mode configuration d'une interface :

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

Navigation entre les modes

La commande *exit* permet d'accéder au contexte précédent.

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

La commande *end* permet d'accéder à la racine du mode privilège.

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#end
Switch#
```

Enfin, la commande *logout* permet la déconnexion.

```
Switch#logout
```

Aide pour la console

Le point d'interrogation affiche les différentes commandes disponibles en fonction du contexte dans lequel nous nous trouvons.

Par exemple :

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

Le *?* affiche les choix possibles lors de la frappe d'une commande.

Par exemple :

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

Enfin, **« *?* »** nous indique les choix possibles lors de la frappe des caractères d'une commande.

Exemple :

```
Switch#sh?
shell show
Switch#sh
```

Commande abrégée

Il est souvent possible d'utiliser les commandes abrégées.

Par exemple les commandes suivantes envoient le même résultat :

```
Switch#wr
Building configuration...
[OK]
-------
Switch#write
Building configuration...
[OK]

Switch#sh ru
Building configuration...
Current configuration : 783 bytes
!
-------

Switch#show running-config
Building configuration...
Current configuration : 783 bytes
```

Complétion automatique des commandes

Il est possible de compléter automatiquement les premiers caractères d'une commande en appuyant sur la touche tabulation.

Comment enregistrer la configuration

Startup-config et running-config, enregistrement de la configuration en cours, suppression de la configuration et redémarrage d'un switch.

Les commandes présentées ci-dessous ont été testées sur les switchs Cisco série 6500, 3750, 2960 et 2950.

Il y a deux types de configuration. La configuration appelée *startup-config* et la configuration appelée *running-config*.

Affichage de la configuration startup-config

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

Affichage de la configuration running-config

```
Switch#show running-config
Building configuration...

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

Différence entre la startup-config et la running-config

- La configuration appelée startup-config est la configuration utilisée au démarrage du switch.
- La configuration dite running-config est la configuration courante utilisée par le switch.

Ainsi, au démarrage du switch, les configurations startup-config et running-config sont les mêmes.

Si une modification de configuration est réalisée, la running-config sera modifiée. Par contre, la startup-config ne sera pas modifiée.

Pour modifier la configuration de démarrage, il faudra enregistrer la configuration courante (running-config) dans la startup-config.

Par conséquent, toute modification effectuée et non enregistrée sera annulée au prochain démarrage du switch.

Cette caractéristique est intéressante en cas de problème grave suite à une modification de configuration (par exemple une perte de lien).

Il suffira de redémarrer le switch pour revenir à l'état précédent la modification.

Enregistrement de la configuration

Les deux commandes suivantes peuvent être utilisées pour enregistrer la configuration courante:

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

switch# write
```

En pratique :

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

Ou bien ;

```
switch# write
Building configuration...
[OK]
switch#
```

En abrégé :

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

Suppression de la configuration - réinitialisation du switch

La commande suivante supprime la configuration de démarrage :

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

La commande suivante supprime les vlans configurés :

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

Il faut ensuite redémarrer le switch.

Redémarrer un switch Cisco avec la ligne de commande

La commande pour redémarrer un switch est :

```
switch# reload
Proceed with reload? [confirm]
```

Redémarrer un switch Cisco avec temporisation

Il peut être intéressant de pouvoir temporiser le redémarrage d'un switch.
Deux méthodes sont possibles :

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

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


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

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

Pour annuler le redémarrage :

```
switch#reload cancel
switch#
switch#


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

switch#
```

Affichage de l'état du redémarrage

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

Configuration de base

Comment configurer le nom du switch, la configuration IP, la passerelle par défaut et création des mots de passe pour l'authentification.

Préparation : Il nous faut :

- Le nom du switch.
- Le nom du domaine DNS.
- L'adresse IP.
- Le masque de sous réseau.
- La passerelle par défaut.
- Un nom de login pour l'administrateur
- Le mot de passe administrateur.

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

Dans l'exemple, le nom du switch est : *3560G* et le domaine est *mondomaine.local*.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#host
Switch(config)#hostname 3560G
3560G(config)#ip domain-name warzone.local
3560G(config)#end
3560G#
*Mar  1 00:03:46.786: %SYS-5-CONFIG_I: Configured from console by console
3560G#wr
Building configuration...
 [OK]
3560G#
```

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

```
3560G(config)#no hostname
Switch(config)#no ip domain-name
Switch(config)#
```

Adressage IP du switch:

L'adressage IP du switch va nous servir à superviser celui ci à distance. Un vlan dédié au management du switch est configuré (dans l'exemple : vlan 99). L'adresse IP sera donc associée au vlan 99.

La configuration IP choisie est :

- Adresse IP : 192.168.3.230
- Masque de sous-réseau : 255.255.255.0
- Passerelle par défaut : 192.168.3.100

Regarder si des vlans existent :

```
3560G#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                                Gi0/5, Gi0/6, Gi0/7, Gi0/8
                                                Gi0/9, Gi0/10, Gi0/11, Gi0/12
                                                Gi0/13, Gi0/14, Gi0/15, Gi0/16
                                                Gi0/17, Gi0/18, Gi0/19, Gi0/20
                                                Gi0/21, Gi0/22, Gi0/23, Gi0/24
                                                Gi0/25, Gi0/26, Gi0/27, Gi0/28
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
Remote SPAN VLANs
------------------------------------------------------------------------------
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
3560G#
```

Configurer un Vlan

```
3560G(config)#vlan 99
3560G(config-vlan)#exit
3560G(config)#interface vlan99
3560G(config-if)#ip address 192.168.3.230 255.255.255.0
3560G(config-if)#ex
3560G(config)#ip default-gateway 192.168.3.100
```

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

```
3560G(config)#interface vlan99
3560G(config-if)#no ip address
3560G(config-if)#ex
3560G(config)#no ip default-gateway
```

Ajout de mot de passe pour l'authentification

La connexion au switch s'effectue par le port console en utilisant la ligne associée à ce port ou bien à distance en utilisant les lignes virtuelles (appelées VTY).

Par défaut, il n'y a pas de compte créé pour l'authentification.

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

Le mode d'administration par défaut est telnet.

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

Nous allons donc tout d'abord activer le service *encryption-password*, les mots de passe apparaitront alors chiffrés lorsque les commandes d'affichage de la configuration sont entrées.

Affichage des lignes disponibles.

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

0 4 veut dire qu'il y a 5 sessions simultanées qui peuvent avoir lieu , 0 15 16 sessions.

Le nombre dépend du matériel et de l'IOS

```
3560G#sh line
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*    0 CTY              -    -      -    -    -      0       0     0/0       -
     1 VTY              -    -      -    -    -      0       0     0/0       -
     2 VTY              -    -      -    -    -      0       0     0/0       -
     3 VTY              -    -      -    -    -      0       0     0/0       -
     4 VTY              -    -      -    -    -      0       0     0/0       -
     -----              -    -      -    -    -      -       -     ---       -
    12 VTY              -    -      -    -    -      0       0     0/0       -
    13 VTY              -    -      -    -    -      0       0     0/0       -
    14 VTY              -    -      -    -    -      0       0     0/0       -
    15 VTY              -    -      -    -    -      0       0     0/0       -
    16 VTY              -    -      -    -    -      0       0     0/0       -
```

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

Un mot de passe est créé pour se loguer aux différentes lignes.

```
3560G(config)#enable secret erty
3560G(config)#line con 0
3560G(config-line)#password erty
3560G(config-line)#login
3560G(config-line)#exit
3560G(config)#line vty 0 15
3560G(config-line)#password erty
3560G(config-line)#login
3560G(config-line)#end
3560G#
```

Les mots de passe limitent l'accès aux périphériques.

- Ils doivent toujours être configurés pour les lignes de terminal virtuel et pour la ligne de console.
- Les mots de passe sont également utilisés pour contrôler l'accès au mode privilégié pour que seuls les utilisateurs autorisés puissent apporter des modifications au fichier de configuration.

Les commandes suivantes permettent de définir un mot de passe facultatif mais recommandé sur la ligne de console :

```
3560G (config)#line console 0
3560G (config-line)#password
3560G (config-line)#login
```

Pour que les utilisateurs puissent accéder à distance au périphériquesà l'aide de Telnet, un mot de passe doit être défini sur une ou plusieurs lignes de terminal virtuel (VTY).

En règle générale, les routeurs Cisco prennent en charge cinq lignes VTY numérotées de 0 à 4, les commutateurs Cisco prennent en charge cinq lignes VTY numérotées de 0 à 4 bien que chaque plate-forme matérielle prenne en charge des numéros différents sur les connexions VTY.

Le même mot de passe est souvent utilisé pour toutes les lignes, mais il arrive parfois qu'une ligne soit définie pour fournir au périphérique une entrée de secours si les quatre autres connexions sont utilisées. Les commandes suivantes sont utilisées pour définir le mot de passe sur les lignes VTY:

```
3560G (config)#line vty 0 15
3560G (config-line)#password
3560G (config-line)#login
```

Le mot de passe enable et le mot de passe enable secret sont utilisés pour limiter l'accès au mode privilégié.

Seul le mot de passe enable est utilisé si le mot de passe enable secret n'a pas été défini.

Il est recommandé de définir et d'utiliser uniquement le mot de passe enable secret car, contrairement au mot de passe enable, il est crypté. Les commandes suivantes permettent de définir les mots de passe enable :

```
3560G (config)#enable password
3560G (config)#enable secret
```

Il est parfois préférable que les mots de passe ne soient pas affichés en texte clair dans le résultat des commandes **show running-config** ou **show startup-config** . Cette commande permet de crypter les mots de passe dans le résultat de configuration:

Activation du service *password-encryption*

```
3560G(config)#service password-encryption
```

La commande **service password-encryption** applique un cryptage simple à tous les mots de passe non cryptés. La commande **enable secret** utilise un puissant algorithme MD5 pour le cryptage.

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

```
User Access Vérification
Password:
3560G>en
Password:
3560G#
```

Configuration et affichage de l'heure

```
3560G#clock set 12:46:00 8 september 2016
*Sep  8 12:46:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:13:02 UTC Mon
Mar 1 1993 to 12:46:00 UTC Thu Sep 8 2016,
3560G#show clock
```

Configurer SSH

Quel protocole d'administration à distance choisir ?

En général, il y a le choix entre l'administration web sécurisée ou pas (protocole http ou https) et/ou l'administration en ligne de commande sécurisée ou pas (telnet ou ssh).

L'administration du switch en utilisant une interface web peut être pratique.

Mais nous choisirons en priorité l'administration du switch en utilisant la ligne de commande pour les raisons suivantes :

- En cas de coupure réseau, il nous faudra intervenir directement sur le switch, donc autant être habitué à travailler en ligne de commande,
- L'interface web peut être moins stable que l'interface en ligne de commande (CLI),
- Les configurations avancées sont souvent disponibles uniquement au travers de la ligne de commande.

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

Ainsi (revenons au sujet) les interfaces web seront désactivées.
Il nous reste à choisir entre telnet et ssh.
Le second étant nettement plus sécurisé que le premier

Il est préférable (quand cela est possible) d'activer uniquement ssh sur le switch.

Activation / désactivation des interfaces d'administration web

Les commandes suivantes activent puis désactivent l'administration web non sécurisée et sécurisée. Ne fonctionne pas avec IOS Version 12.2(25).

```
3560G(config)#ip http server
3560G(config)#ip http secure-server
3560G(config)#no ip http server
3560G(config)#no ip http secure-server
```

Configuration du protocole ssh pour le switch

- Vérification de la prise en compte du protocole ssh par l'IOS

  Tout d'abord, il faut vérifier que l'IOS du switch supporte ssh.

  La mention k9 (crypto) doit figurer dans le nom de l'IOS.

  La commande pour vérifier la version de l'IOS est:

```
3560G#show version
Cisco IOS Software, C3560 Software (C3560-IPSERVICESK9-M), Version 15.0(2)SE2, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Tue 05-Feb-13 12:24 by prod_rel_team
```

- Configuration du nom d'hôte et du nom de domaine.

  Le nom du switch ainsi que le nom de domaine doivent avoir été configurés.

- Création d'une clé ssh

```
3560G(config)#crypto key generate rsa general-keys modulus 1024
3650G(config)#crypto key generate rsa
The name for the keys will be: 3650G.mondomaine.moi
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]:

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

3560G(config)#
```

- Activation de ssh

```
3560G(config)#ip ssh version 2
```

- Options ajoutées au service ssh

  - les évènements associés aux connexions ssh sont enregistrés.
  - Un timeout de 120 secondes est ajouté pour les sessions ssh en cas d'inactivité.
  - Nous laissons trois essais pour la connexion au switch.

```
~~3560G(config)#ip ssh logging events~~
3560G(config)#ip ssh time-out 120
3560G(config)#ip ssh authentication-retries 3
```

- Configuration de l'authentification et ajout d'un compte administrateur

```
3560G(config)#aaa new-model
3560G(config)#aaa authentication login default local
3560G(config)#username admin secret erty
```

- Désactivation de telnet pour l'accès au switch et acces SSH

```
3560G(config)#line vty 0 15
3650G(config-line)#no login local
3560G(config-line)#transport input ssh
3650G(config-line)#end
```

- Vérification de la configuration

```
Aug  9 16:13:31.988: %SYS-5-CONFIG_I: Configured from console by consoleho
3560G#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

SSH est maintenant activé. Nous pouvons accéder au switch avec un client ssh (par exemple putty pour windows) via son ip.

exemple : Mise en place rapide ssh.

```
User Access Verification

Username: admin
Password:
3650G>en
Password:
3650G#conf t
Enter configuration commands, one per line. End with CNTL/Z.
3650G(config)#crypto key generate rsa
% You already have RSA keys defined named 3650G.mondomaine.moi .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: 3650G.mondomaine.moi
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]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

*mars 1 2:34:41.263: RSA key size needs to be at least 768 bits for ssh version 2
*mars 1 2:34:41.263: %SSH-5-ENABLED: SSH 1.5 has been enabled
3650G(config)#ip ssh authentication-retries 5
3650G(config)#ip ssh time-out 120
3650G(config)#line vty 0 15
3650G(config-line)#no login local
3650G(config-line)#transport input ssh
3650G(config-line)#exit
3650G(config)#ex
3650G#
%SYS-5-CONFIG_I: Configured from console by console
3650G#copy ru st
Destination filename [startup-config]?
Building configuration...
[OK]
3650G#
```

Suppression de ssh

La suppression de la clé entraine la désactivation de ssh.

```
3560G(config)#crypto key zeroize rsa
% All RSA keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
3560G(config)#
```

Vérification:

```
3560G#sh ip ssh
SSH Disabled - version 2.0
%Please create RSA keys to enable SSH (of atleast 768 bits size) to enable SSH v2.
Authentication timeout: 60 secs; Authentication retries: 3
```

Filtrer les connexions ssh avec une liste de contrôle d'accès

La liste de contrôle d'accès va nous permettre de filtrer l'accès ssh en utilisant l'adresse IP source.

Dans la commande suivante, la liste de contrôle d'accès a le numéro 10 et le réseau autorisé à se connecter en ssh est 192.168.3.0/24.

On autorise seulement un poste a se connecte sur la Vty 10 , par exemple,seul l'ip du pc adminstrateur.

```
Switch(config)#access-list 10 permit 192.168.3.10 0.0.0.255
```

Ensuite, on autorise la connexion exclusive de ce réseau sur les terminaux virtuel avec la commande access-class:

```
Switch(config)#line vty 0 15
Switch(config-line)#access-class 10 in
Switch(config-line)#
```

Configuration du port

Configuration les interfaces des switchs (vitesse, duplex, ...) et introduction à l'alimentation électrique (poe).

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

Tout d'abord, quelques mots sur les noms des interfaces.

- Les interfaces 100Mbits/s sont nommées fastethernet,
- Les interfaces 1Gbit/s sont nommées gigabitEthernet,
- Et les interfaces 10Gigabit/s sont nommées TenGigabitEthernet.
  Les numéros des ports ont la syntaxe suivante: 0/1 ou 1/0/1.
  C'est à dire: numéro du module/numéro du port ou bien numéro du switch dans le stack/numéro du module/numéro du port.
  La commande suivante affiche la configuration courante d'une interface. En cas de modification, il faut, bien sur, enregistrer cette configuration...

```
3560G#sh running-config interface fastEthernet 0/1
Building configuration...
Current configuration : 85 bytes
interface FastEthernet0/1
switchport access vlan 7
switchport mode access
end
```

Et voici la commande pour afficher les valeurs des compteurs d'une interface :

```
3560G#show interfaces gigabitEthernet 0/1


GigabitEthernet0/1 is up, line protocol is up (connected)
Hardware is Gigabit Ethernet, address is 0026.3750.2950 (bia 0026.3750.2950)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is 10/100/1000BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
```

```
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 187000 bits/sec, 231 packets/sec
5 minute output rate 1000 bits/sec, 2 packets/sec
225348823 packets input, 188621734150 bytes, 0 no buffer
Received 130125788 broadcasts (87756518 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 87756518 multicast, 0 pause input
0 input packets with dribble condition detected
1222204 packets output, 103305303 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
3560G#
```

Plusieurs infos intéressantes :

- le port est up ou down,

```
3650G(config-line)#no login local
```

- l'interface est de type giga,
- Ell fonctionne en full duplex avec un débit de 100Mbit/s.

```
Full-duplex, 100Mb/s, media type is 10/100/1000BaseTX
```

Pour les stats, il y a les compteurs concernant le débit et les erreurs.
Ainsi, en cas de modification sur une interface, les deux comandes précédentes permettent de vérifier la prise en compte de la modification.

Résumé des informations pour l'ensemble des ports:

```
3560G#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/1                        connected    1          a-full  a-100 10/100/1000BaseTX
Gi0/2                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/3                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/4                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/5                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/6                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/7                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/8                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/9                        notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/10                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/11                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/12                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/13                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/14                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/15                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/16                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/17                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/18                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/19                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/20                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/21                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/22                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/23                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/24                       notconnect   1            auto   auto 10/100/1000BaseTX
Gi0/25                       notconnect   1            auto   auto Not Present
Gi0/26                       notconnect   1            auto   auto Not Present
Gi0/27                       notconnect   1            auto   auto Not Present
Gi0/28                       notconnect   1            auto   auto Not Present
```

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

Ajout d'une description

```
3560G(config)#int fastEthernet 0/1
3560G(config-if)#description serveur de fichier
3560G(config-if)#end
```

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

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

Paramètre disponible pour une interface 100Mbit/s

```
3560G(config-if)#speed ?
10 Force 10 Mbps operation
100 Force 100 Mbps operation
auto Enable AUTO speed configuration

3560G(config-if)#duplex ?
auto Enable AUTO duplex configuration
full Force full duplex operation
half Force half-duplex operation
```

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

```
3560G(config)#interface fastEthernet 0/1
3560G(config-if)#speed 10
3560G(config-if)#duplex half
3560G(config-if)#end
```

On vérifie dans la conf et sur l'interface :

```
3560G#sh run int fa0/1
Building configuration...

Current configuration : 331 bytes
!
interface FastEthernet0/1
description serveur de fichier
speed 10
duplex half

3560G#sh int fa0/1
FastEthernet0/1 is down, line protocol is down (notconnect)
Description: serveur de fichier
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 10Mb/s, media type is 10/100BaseTX
```

Pour remettre les paramètres par défaut:

```
3560G(config)#int fastEthernet 0/1
3560G(config-if)#speed auto
3560G(config-if)#duplex auto
```

Désactiver et activer une interface

Dans l'exemple, on désactive puis on réactive l'interface fa0/1.

```
Switch(config)#int fa0/1
Switch(config-if)#shut
Switch(config-if)#end
Switch#
*Mar 2 02:38:13.253: %SYS-5-CONFIG_I: Configured from console by console
*Mar 2 02:38:13.849: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#no shut
Switch(config-if)#end
*Mar 2 02:38:29.989: %SYS-5-CONFIG_I: Configured from console by console
*Mar 2 02:38:30.920: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
```

Suppression de la configuration d'un port

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

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

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

switch#
```

Affichage du statut PoE (power over ethernet) des ports

La technologie poe (802.3af) permet l'alimentation électrique de périphérique (téléphone, borne wifi, ...) par les ports des switchs.

Si le switch supporte cette technologie, la commande suivante permet de visualiser le budget électrique général ainsi que le statut de chaque port.

```
3560G#show power inline

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

Comment configurer les Vlans

Configuration des vlans par port sur un switch Cisco.

Les commandes suivantes ont été testées sur des switchs série 2950, 2960, 3750 et 6500 et 3650.

Rappel sur la notion de VLAN (Virtual Local Area Network)

L'objectif d'une configuration de vlan est de permettre la configuration de réseaux différents sur un même switch.

Il existe plusieurs façons de configurer les vlans. Cette page traitera uniquement du vlan par port.

La norme utilisée ici porte l'identifiant 802.1q.

Les avantages principaux de la segmentation par vlan sont la réduction des domaines de broadcast et l'accroissement de la sécurité (si des filtres sont mis en place pour la communication entre les réseaux).

Principe de fonctionnement du vlan par port

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

Type de configuration des ports des switchs Cisco

Le port est configuré en mode *access* ou en mode *trunk*.

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

Le mode *trunk* est utilisé dans le cas ou plusieurs vlans doivent circuler sur un même lien.

C'est par exemple le cas de la liaison entre deux switchs ou bien le cas d'un serveur ayant une interface appartenant à plusieurs vlans.

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

Dans le cas de l'utilisation d'un ordinateur connecté à un téléphone IP (ce dernier étant connecté à un port du switch), le port aura deux vlans (un vlan dédié au réseau donnée et un vlan dédié au réseau voix).

Le port sera configuré en général en mode *access*, une commande sera ajoutée pour la configuration du vlan voix (*voice vlan*).

VLAN non affecté à un port et présent sur le switch

Des vlans peuvent être créés sur un switch et n'être affectés à aucun port. C'est le cas du vlan de management (une adresse IP sera configurée sur ce vlan).

Un switch qui sert de liaison aura également les vlans qui doivent le traverser déclaré dans sa configuration.

Communication entre les vlans

La communication entre les vlans est possible en passant par un routeur ou un switch de niveau 3 (switch-routeur)

Selon l'utilisation, il peut être conseillé de filtrer les réseaux au minimum au moyen d'ACLs (access control list).

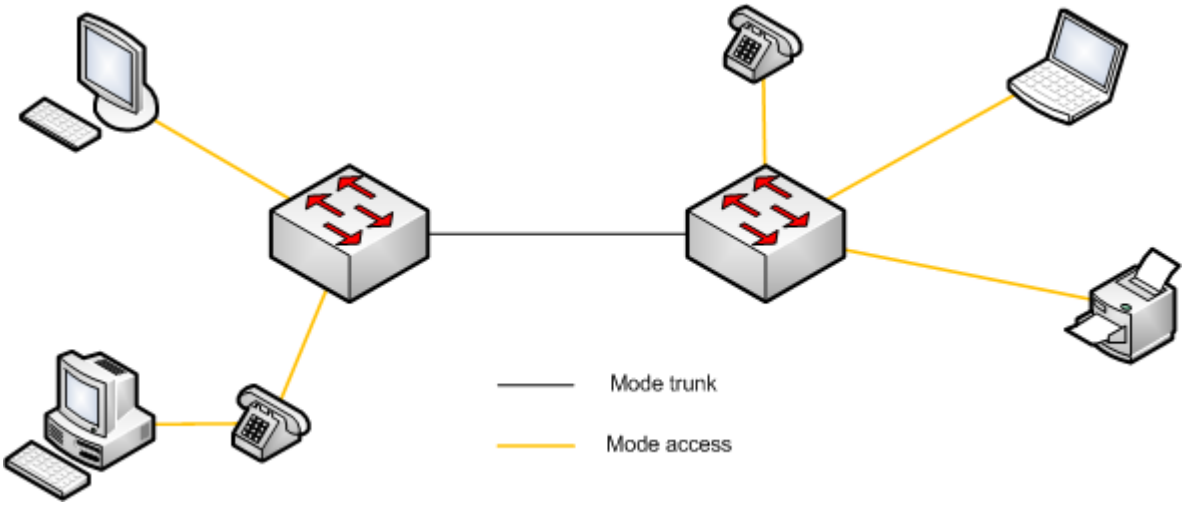
VLAN natif: Le vlan appelé "natif" est le vlan par défaut du switch (en général le vlan 1). Sans configuration, tous les ports du switch sont placés dans ce VLAN.

Ce vlan n'est pas marqué même si il passe sur une liaison trunk.

Configuration type d'un switch:

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

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



Ajout de vlan

Création du vlan 2 puis des vlans 3 à 5

```
3560G(config)#vlan 2
3560G(config-vlan)#name administration
3560G(config-vlan)#ex
3560G(config)#vlan 3,4,5
3560G(config-vlan)#ex
3560G(config)#
```

Suppression d'un vlan

```
3560G(config)#no vlan 2
```

Affichage des vlans ainsi que des affectations de port

```
3560G#show vlan

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

Affectation d'un port à un vlan

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

```
3560G(config)#interface fastEthernet 0/1
3560G(config-if)#switchport mode access
3560G(config-if)#switchport access vlan 3
3560G(config-if)#ex
3560G(config)#
```

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

```
3560G(config)#interface range fastEthernet 0/5-8
3560G(config-if-range)#switchport mode access
3560G(config-if-range)#switchport access vlan 4
3560G(config-if-range)#end
3560G#
```

Pour un switch série 6500

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

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

Pour un switch série 2950 et 3750

```
3750(config)#interface gigabitEthernet 1/0/1
3750(config)#switchport trunk encapsulation dot1q
3750(config-if)#switchport mode trunk
3750(config-if)#
```

Pour un switch série 2960

```
3560G(config)#interface gigabitEthernet 1/0/1
3560G(config-if)#switchport mode trunk
3560G(config-if)#
```

Pour un switch série 6500

```
6500(config)#interface gigabitEthernet 1/0/1
6500(config-if)#switchport trunk encapsulation dot1q
6500(config-if)#switchport mode trunk
6500(config-if)#
```

Filtrage des vlans sur un port uplink

Pour les swiths série 2950, 2960, 3750, 6500

(dans l'exemple, on autorise les vlans 2,3 et 10 a être transportés sur le lien).

```
3560G(config)#interface gigabitEthernet 1/0/1
3560G(config-if)# switchport trunk allowed vlan add 2,3,10
3560G(config-if)#
```

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

```
3560G(config-if)#switchport trunk allowed vlan remove 3
3560G(config-if)#
```

Pour supprimer la commande de filtrage:

```
3560G(config-if)#no switchport trunk allowed vlan
3560G(config-if)#
```

Configuration d'un vlan dédié à la téléphonie

Le protocole cdp doit préalablement être activé.

```
3560G(config)#vlan 10
3560G(config-vlan)#name voip
3560G(config-vlan)#ex
3560G(config)#int fastEthernet 0/1
3560G(config)#switchport voice vlan 10
```

Suppression de la configuration d'un port

Comme d'habitude, il suffit de mettre la commande no devant les commandes entrées précédemment.
Par exemple:

```
3560G(config)#int fastEthernet 0/1
3560G(config-if)#no switchport access vlan
3560G(config-if)#no switchport mode acc
3560G(config-if)#end
```

Configuration du protocole VTP (Vlan Transport Protocol) en mode transparent

Le protocole VTP permet la configuration automatique de vlan entre des serveurs VTP et des clients sur un même domaine VTP.
Pour utiliser uniquement la base locale de vlan sur nos commutateurs, on configure VTP en mode transparent.

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


...
```

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

Commande nonegociate

Le protocole DTP (Dynamic Trunking Protocol) permet à deux commutateurs qui sont connectés ensemble de monter un lien trunk automatiquement sous certaines conditions (par exemple la connexion d'un port configuré par défaut en dynamic auto vers un port trunk).

En général, il vaut mieux désactiver cette possibilité.

On désactive donc cette option sur tous les ports access et trunk.

```
Switch(config)#interface range fastEthernet 1/0/1 - 10
Switch(config-if-range)#switchport nonegotiate
```

Vérification sur une interface:

```
3650G#sh int gi0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 100 (trunked)
Trunking Native Mode VLAN: 99
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,99-100
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Comment configurer simplement la qualité de service

Configuration automatique de la qos dédiée à la voip.

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

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

Activation de la Q.O.S. pour les switchs.

Port d'accès:

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

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

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

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

Port de liaison, trunk ou uplink, switch série 2960 et 3750

```
3750(config)#int gi 0/1
3750(config-if)#auto qos voip trust
3750(config-if)#end
```

Activation de la qualité de service pour un port uplink série 6500

Activation générale

```
6500(config)#mls qos
```

Activation pour un port uplink (concerne la qos appliquée sur le niveau 2)

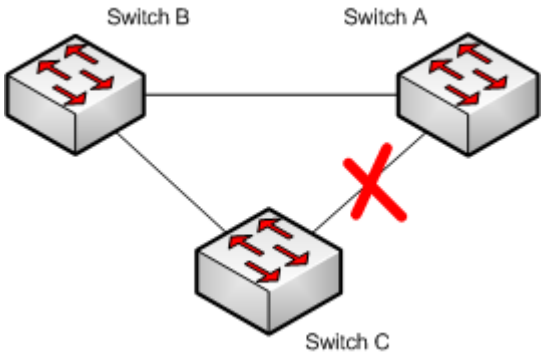
```
6500(config)#int gi 0/1
6500(config-if)#mls qos trust cos
```

Comment configurer le spanning-tree

Configuration du spannnig-tree sur un switch Cisco.
Les commandes suivantes ont été testées sur des switchs série 3750 et 2960.

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

C'est un protocole de niveau 2.



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

Dans certain cas, il est souhaitable de fixer les priorités par défaut.
Le switch qui aura la priorité la plus basse sera élu root. On choisit un switch qui est placé en tête du réseau (backbone) puisque tout le traffic passe par lui et qu'en général, il n'y a pas beaucoup de machine cliente connectée.

De plus, on peut préférer un lien par rapport à un autre, pour des raisons de débit différent par exemple.
La priorité par défaut d'un switch est de 32768. La priorité d'un port par défaut est 128. Si on abaisse le chiffre, le switch ou le port devient prioritaire par rapport aux autres.

Activation du rapid spanning-tree sur le switch

```
3560G(config)#spanning-tree mode rapid-pvst
```

Vérification des informations

```
3650G#sh spanning-tree
VLAN0010
Spanning tree enabled protocol rstp
Root ID Priority 32778
Address 00D0.BAB5.B302
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
Address 00D0.BAB5.B302
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1 Desg FWD 4 128.25 P2p
Fa0/10 Desg FWD 19 128.10 P2p
Fa0/11 Desg FWD 19 128.11 P2p

VLAN0011
Spanning tree enabled protocol rstp
Root ID Priority 32779
Address 00D0.BAB5.B302
```

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

Bridge ID Priority 32779 (priority 32768 sys-id-ext 11)
Address 00D0.BAB5.B302
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/10 Desg BLK 19 128.10 P2p
Fa0/11 Desg BLK 19 128.11 P2p

VLAN0020
Spanning tree enabled protocol rstp
Root ID Priority 32788
Address 00D0.BAB5.B302
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32788 (priority 32768 sys-id-ext 20)
Address 00D0.BAB5.B302
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/20 Desg BLK 19 128.20 P2p
Fa0/21 Desg BLK 19 128.21 P2p
Gi0/1 Desg BLK 4 128.25 P2p

VLAN0099
Spanning tree enabled protocol rstp
Root ID Priority 32867
Address 00D0.BAB5.B302
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32867 (priority 32768 sys-id-ext 99)
Address 00D0.BAB5.B302
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1 Desg FWD 4 128.25 P2p
Fa0/1 Desg FWD 19 128.1 P2p

VLAN0100
Spanning tree enabled protocol rstp
Root ID Priority 32868
Address 00D0.BAB5.B302
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32868 (priority 32768 sys-id-ext 100)
Address 00D0.BAB5.B302
```

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

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1 Desg BLK 4 128.25 P2p
```

Il est possible, entre autre, de préciser une interface à la suite de la commmande *sh spanning-tree*.

Fixer le switch root

Dans la copie d'écran suivante le switch est root pour les vlans 1 à 100. Puis on affiche les données spanning-tree pour le vlan 4.

```
switch(config)#spanning-tree vlan 1-100 root primary
switch(config)#end
switch#show spanning-tree vlan 4

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

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

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


switch#
```

Configurer une priorité sur un port

Dans l'exemple, l'interface prioritaire sera gi0/1 pour les vlans 1 à 100. On affiche ensuite les informations pour le vlan 4.

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

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

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

```
Aging Time 300 sec

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

switch#
```

Configuration des ports d'accès reliés à un switch

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

```
3560G(config)#int range fa0/1 - 8
3560G(config-if-range)#spanning-tree portfast
```

Vérification

```
3560G#sh run int fa0/1
Building configuration...

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

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

```
3560G(config)#int fa0/1
3560G(config-if)#no spanning-tree portfast
3560G(config-if)#end
3560G#sh run int fa0/1
Building configuration...

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

3560G#
```

Configuration des services syslog, snmp, ntp.

Configuration de l'accès aux services syslog, NTP et SNMP.

Commande pour afficher les logs

```
3560G#show log
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

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

Configuration du service syslog

Le pré-requis est d'avoir installé un serveur type syslog (adresse 192.168.0.123 dans l'exemple).
Configuration du niveau d'information demandée: dans l'exemple, on demande le maximum d'information.

```
3560G(config)#logging trap ?
<0-7> Logging severity level
alerts Immediate action needed (severity=1)
critical Critical conditions (severity=2)
debugging Debugging messages (severity=7)
emergencies System is unusable (severity=0)
errors Error conditions (severity=3)
informational Informational messages (severity=6)
notifications Normal but significant conditions (severity=5)
warnings Warning conditions (severity=4)
3560G(config)#logging trap debugging
3560G(config)#
```

Puis on configure l'étiquette associée à chaque message (ici local4) ainsi que l'adresse IP du serveur syslog.

```
3560G(config)#logging facility local4
3560G(config)#logging 192.168.0.123
```

Configuration du service NTP

Synchronisons maintenant les informations horaires du switch à un serveur NTP (network time protocol).

Nous indiquons dans un premier temps l'adresse IP du serveur NTP, puis on configure le fuseau horaire ainsi que le moment de passer à l'heure d'été (dans l'exemple: pour la France).

```
3560G(config)#ntp server 192.168.0.124
3560G(config)#clock timezone cet 1
3560G(config)#clock summer-time cest recurring last Sun Mar 3:00 last Sun Oct 3:00
```

Quelques commandes de vérification: les associations avec le serveur ntp et l'affichage de la date et de l'heure courante:

```
3560G#sh ntp associations

address ref clock st when poll reach delay offset disp
*~192.168.0.124 208.52.173.46 2 0 64 1 1.7 4.27 15875.
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
3560G#sh clock
16:51:03.048 cet Thu Jan 27 2011
3560G#
```

Configuration du service SNMP

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

Nous configurons tout d'abord une liste d'accès pour autoriser uniquement la connexion du serveur de management SNMP, puis nous indiquons le nom de la communauté SNMP ainsi que les droits associés (lecture (ro) ou lecture/écriture (rw)).

```
3560G(config)#access-list 1 permit 192.168.1.2
3560G(config)#snmp-server community macomm ro 1
3560G(config)#exit
3560G#show snmp community
```

Comment mettre à jour le switch.

Commande pour afficher le modèle du switch, la version de l'IOS, pour mettre à jour le switch et pour sauvegarder la configuration.

Les commandes suivantes ont été testées avec les switchs série 2950, 2960 et 3750.

Affichage de la version de l'IOS

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

```
3560G#show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(55)SE1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Thu 02-Dec-10 08:16 by prod_rel_team
Image text-base: 0x00003000, data-base: 0x01800000

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

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

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

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

Affichage des fichiers présents dans la flash:

```
3560G#dir flash:
Directory of flash:/

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

27998208 bytes total (18131456 bytes free)
3560G#
```

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

Mise à jour d'un IOS

Nous avons besoin d'un IOS (disponible chez Cisco) et d'un serveur tftp.

La commande suivante simplifie la mise à jour puisqu'elle fait tout toute seule (configuration des variables, suppression de l'ancien IOS, et installation du nouvel IOS). Il ne reste plus qu'a redémarrer le switch (il peut aussi redémarrer tout seul en option).

Bien sur, durant la mise à jour, il ne faut pas débrancher le switch sous réserve de devoir passer au plan B qui est nettement plus long...

L'adresse du serveur tftp est dans notre cas 192.168.1.123.

```
3560G#archive download-sw /overwrite tftp://192.168.1.123/c2960-ipbasek9-tar.122-
55.SE1.tar
Loading /c2960-ipbasek9-tar.122-55.SE1.tar from 192.168.1.123 (via Vlan2):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Lorsque le switch a terminé sa mise à jour, vérifions que la nouvelle image est en place par un *dir flash:*, puis vérifions que le nouvel IOS est bien pris en compte dans les variables de démarrage:

```
3560G#show boot
BOOT path-list : flash:/c2960-lanbasek9-mz.122-55.SE1/c2960-lanbasek9-mz.122-55.SE1.bin
Config file : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break : no
Manual Boot : no
HELPER path-list :
Auto upgrade : yes
Auto upgrade path :
NVRAM/Config file
buffer size: 65536
Timeout for Config
Download: 0 seconds
Config Download
via DHCP: disabled (next boot: disabled)
3560G#
```

Si tout est OK, redémarrons le switch, la commande *show version* permet de vérifier la version de la nouvelle image installée.

Sauvegarde de la configuration

Sauvegarde du fichier de configuration en utilisant un serveur tftp.

```
3560G#copy flash:config.text tftp://192.168.2.1/
Address or name of remote host [192.168.2.1]?
Destination filename [config.text]?2960-conf.cfg
```

Configuration d'une pile de switch 3750.

Pourquoi stacker des switchs?

- Simplifier l'administration (l'ensemble des switchs apparaissent pour l'administrateur comme un seul switch),
- Améliorer la bande passante entre les switches,
- Améliorer la redondance en cas de panne.

Comment faire?

Il suffit de connecter le cable de stack à l'arrière des switches. Pour le 2960s, un module doit également être ajouté. Pour optimiser la bande passante et pour améliorer la redondance, l'architecture stackée formera une boucle. Ci dessous, un exemple d'un stack composé de deux switchs.

Pré-requis pour stacker des switches sans problème

Puisque les switchs appartenant à une pile seront vus comme un seul switch, les versions d'IOS doivent être identiques pour tous les switchs. Avant de stacker des switchs, on vérifiera les versions d'IOS de chaque switch.

Et si un switch est ajouté à une pile, il est préférable que l'IOS de ce switch corresponde à celui du stack en place.

Autre solution: Si il y a uniquement une différence de version entre les IOS et que ceux ci sont récents (je vous laisse chercher la version minimum), le switch peut lancer une mise à jour automatique.

Dans l'exemple suivant, le switch 2 a été ajouté, la version courante de l'IOS ne convient pas (*mismatch*). Le switch lance la procédure de mise à jour automatique.

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

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

Si l'autoconfiguration ne se lance pas, on peut toujours tenter de recopier l'IOS sur le switch qui a été ajouté.

La commande suivante recopie l'IOS du switch 1 vers le switch 2 (*destination-system*). Il faudra ensuite rédémarrer le switch.

```
cisco-3750#archive copy-sw /destination-system 2 1
```

fonctionnement et configuration des switchs de la pile

Un switch maitre est élu et gère le controle de la pile de switch.

Lorsqu'un switch est ajouté à une pile, les ports s'ajoutent à la configuration en cours. Ainsi, les ports du switch numéro 1 de la pile auront comme numéro 1/0/x, les ports du switch numéro 2 de la pile auront comme numéro 2/0/x, etc ... Les autres paramètres de configuration sont communs.

Il y a donc un seul fichier de configuration pour l'ensemble des switchs. Les numéros de ports apparaissent dans ce fichier.

La commande suivante affiche la configuration du port 5 du deuxième switch du stack:

```
sw-3750#show running-config interface fastEthernet 2/0/5
Building configuration...

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

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

Quelques commandes de supervision

Affichage des switchs appartenant à la pile ainsi que la correspondance des ports reliés entre eux.

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



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

sw-3750#
```

Quelques commandes d'affichage de statistique sur les ports de stacks:

```
sw-3750#sh switch stack-ring speed

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

```
sw-3750#sh switch stack-ring activity

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

Total frames sent to stack ring : 4502782552
```

```
sw-3750#sh switch stack-ports summary

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

Comment afficher la version les informations administratives d'un switch appartenant à un stack

La commande d'affichage suivante permet de visualiser la version de l'ios ou encore le numéro de série de chaque switch.

```
sw-3750#sh version

.....

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

.....

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

......
```

Affichage du contenu de la mémoire flash du switch 2

```
sw-3750#sh flash2:

Directory of flash2:/

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

.....
```

Comment remplacer un switch d'une pile?

Tout d'abord, il est préférable que le switch qui va être ajouté ait une version d'IOS identique à celle des autres switchs de la pile.

Pour remplacer un switch, il faut débrancher ce switch électriquement et l'enlever du stack.

Ensuite le nouveau switch sera connecté à la pile, puis alimenté électriquement. Il récupère ainsi automatiquement la configuration du switch qui vient d'être retiré.

Retirer définitivement un switch d'une pile

Il faut tout d'abord débrancher le switch électriquement et enlever les cordons de stack.

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

La séquence de commande suivante affiche les switchs appartenant à la pile (le switch 2 a été retiré).

Puis, on affiche un extrait du fichier de configuration et on supprime le switch 2 du fichier de configuration.

Enfin, on enregistre la configuration (il n'est pas nécessaire de redémarrer la pile).

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

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

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

Comment redémarrer un switch d'un stack?

La commande suivante redémarre le switch numéro 4:

```
sw-3750#reload slot 4
```

Comment renuméroter le switch d'un stack?

La commande suivante renumérote le switch numéro 3 en switch numéro 2. Il faut ensuite redémarrer le switch.

```
sw-3750(config)#switch 3 renumber 2
```

Comment désactiver le port stack d'un switch

La commande suivante désactive le port de stack numéro 2 du premier switch.

```
sw-3750#switch 1 stack port 2 disable
Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]
```

Pour réactiver ce port:

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

Comment changer la priorité d'un switch dans le stack

Le switch qui a la priorité la plus haute devient le *master*. Le niveau de priorité va de 1 à 15. Le niveau le plus haut étant prioritaire.

Commande pour modifier le niveau d'un switch puis vérification:

```
sw-3750(config)#switch 2 priority 15
Changing the Switch Priority of Switch Number 2 to 15
Do you want to continue?[confirm]

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

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

Quelques commandes de diagnostique

Comment afficher les switchs voisins?

Pour des raisons de sécurité, si nous n'utilisons pas cette fonctionnalité, il est préférable de désactiver les protocoles suivants.

CDP

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

La commande suivante active le protocole cdp puis affiche les voisins.

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

Device ID Local Intrfce Holdtme Capability Platform Port ID
sw-2960 Gig 1/0/1 178 S I WS-C2960G Gig 0/2
```

Il est aussi possible d'afficher les détails sur le voisin, notamment l'adresse IP et le modèle de ce dernier.

```
sw-3750#sh cdp neighbors gigabitEthernet 1/0/2 detail
```

LLDP

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

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

Activation du protocole lldp puis affichage des voisins:

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

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

Total entries displayed: 1
```

Affichage des détails:

```
switch-3750#
switc-3750#show lldp neighbors detail
------------------------------------------------
Chassis id: 0025.b852.c4200
Port id: 72
Port Description: 1
System Name: switch-hp

System Description:
ProCurve J9451A Switch 6600

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

Total entries displayed: 1

switc-3750#
```

Désactivation de lldp

```
switch-3750(config)#no lldp run
switch-3750(config)#
```

Sans commentaire

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

Affichage des adresses Mac

```
sw-3750#sh mac address-table
Mac Address Table
-------------------------------------------


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

Mirroring d'un port

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

Dans l'exemple:

Le port en écoute porte le numéro 1 (interface source).

Le port ou sera connecté le PC muni d'un analyseur de trame (wireshark par exemple) est le port 4 (interface destination)

La session a le numéro 1.

```
sw-2960(config)#monitor session 1 source interface fastEthernet 0/1
sw-2960(config)#monitor session 1 destination interface fastEthernet 0/4
```

Affichage des interfaces surveillées:

```
switch#sh monitor Session 1
---------
Type : Local Session
Source Ports :
Both : Fa0/1
Destination Ports : Fa0/4
Encapsulation : Native
Ingress : Disabled
```

Désactivation du mirroring

```
switch2(config)#no monitor session 1
```

Afficher les compteurs pour les interfaces

```
Switch#show interfaces counters

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

Quelques informations sur le fonctionnement du système

```
Switch#show env all
FAN is OK
TEMPERATURE is OK
SW PID Serial# Status Sys Pwr PoE Pwr Watts
-- ------------------ ---------- --------------- ------- ------- -----
1 Built-in Good
SW Status RPS Name RPS Serial# RPS Port#
-- ------------- ---------------- ----------- ---------
1 Not Present <>
Switch#
```

Routage intervlan

Comment configurer le routage intervlan sur un switch de niveau 3 ?

Le routage doit tout d'abord être activé sur le switch. On vérifie ensuite l'affichage de la table de routage.

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

Création et configuration des vlans

```
Switch(config)#vlan 2,3,4,100
Switch(config-vlan)#ex
Switch(config)#interface vlan 2
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Switch(config)#interface vlan 3
Switch(config-if)#ip address 192.168.3.1 255.255.255.0
Switch(config)#interface vlan 4
Switch(config-if)#desc secretariat
Switch(config-if)#ip address 192.168.4.1 255.255.255.0
Switch(config)#interface vlan 100
Switch(config-if)#desc interco
Switch(config-if)#ip address 192.168.100.254 255.255.255.0
Switch(config-if)#^Z
Switch#
```

Configuration de la route par défaut

```
Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
Switch(config-if)#^Z
```

Vérification: commande d'affichage de la table de routage

```
Switch#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 192.168.1.1 to network 0.0.0.0

C 192.168.4.0/24 is directly connected, Vlan4
C 192.168.1.0/24 is directly connected, Vlan100
C 192.168.2.0/24 is directly connected, Vlan2
C 192.168.3.0/24 is directly connected, Vlan3
S* 0.0.0.0/0 [1/0] via 192.168.1.1
Switch#
```

Les autres switchs sont connectés au commutateur de niveau 3 avec des liens trunk des deux cotés.

Les autres techniques qui concernent le routage (acl, dhcp, ospf, ...) s'appliquent dans le cas ci-dessus aux interfaces logiques vlan au lieu de s'appliquer aux interfaces physiques.

Annexes

Howto switchs Cisco

Nous utilisons principalement des switchs Cisco Catalyst 2950/2960/2970/3750 et cette documentation sera orientée pour ces modèles.

Stackable ou non-Stackable ?

Les switchs -S Series permettent de stacker plusieurs switchs : c'est-à-dire que plusieurs switchs seront vus comme un seul, offrant ainsi des facilités en terme d'administration (mais pas forcément en terme de sécurité).

Cela se fait par exemple avec plusieurs switch 2960-S et des modules Cisco FlexStack? : ces modules s'ajoutent à l'arrière de chaque switch, il suffit ensuite de les relier avec des câbles Cisco FlexStack?

Astuce : un switch stackable (S Series) est parfois moins cher qu'un non-stackable... et il peut pourtant très bien être utilisé tout seul !

Administration de switchs Cisco Catalyst

Configuration initiale

Avec un port série (old-school)

Raccorder le port d'administration du switch au port série d'un poste Linux à l'aide du câble fourni (couleur bleu ciel)

Installer minicom et créer le fichier de configuration /etc/minicom/minirc.cisco avec un contenu du type :

```
pu port             /dev/ttyS0
pu baudrate         9600
pu bits             8
pu parity           N
pu stopbits         1
pu rtscts           No
```

Note : Avec un adaptateur USB, le device est /dev/ttyUSB0 (ou autre numéro).

Exécuter la commande minicom cisco et observer l'initialisation du switch. A la question Would you like to enter the initial configuration dialog?, répondre no

Passer en mode administrateur avec la commande enable, et afficher la configuration par défaut avec show running-config

Avec un câble Ethernet

Pour un switch récent, une fois allumé pour la 1ère fois, on appuye 3 à 4 secondes sur le bouton MODE ce qui le fait passer en mode Express Setup. Note : cela ne fonctionne que si le switch n'a jamais été configuré.

On branche un câble sur n'importe quel port et on lance un client DHCP sur un ordinateur :

```
# dhclient -d eth0
Internet Systems Consortium DHCP Client 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/f0:de:f1:12:c9:d2
Sending on   LPF/eth0/f0:de:f1:12:c9:d2
Sending on   Socket/fallback
```

```
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPNAK from 10.0.2.3
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
DHCPOFFER from 10.0.2.3
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 10.0.2.3
bound to 10.0.2.2 -- renewal in 271 seconds.
```

On obtient ainsi l'adresse IP actuelle du switch : 10.0.2.3 et l'on peut se connecter en telnet sans mot de passe, ou en HTTP avec cisco/cisco. Le plus simple est a priori de le faire en HTTP où l'on renseigne une configuration IP de base et les mots de passe, et l'on sort du mode Express Setup une fois terminé.

Commandes de base

Commandes de bases sous IOS :

```
Switch# show version
Switch# show mem
Switch# show processes
Switch# show process cpu
Switch# show flash
Switch# show clock
Switch# show history
Switch# show logging
Switch# show inventory
Switch# show interfaces
Switch# show interfaces status
Switch# show interfaces st
Switch# show interfaces counter
Switch# show interfaces counter errors
Switch# show interfaces Gi0/11
Switch# show interfaces Gi0/11 status
Switch# show interfaces Gi0/11 counter
Switch# show interfaces Gi0/11 counter errors
Switch# show interfaces trunk
Switch# show interfaces description
```

Gestion de base de la configuration

Configuration en Flash

```
Switch# show configuration
```

Configuration actuelle

```
Switch# show running-config
```

Configuration actuelle d'une interface particulière

```
Switch# show running-config interface GigabitEthernet1/0/1
```

Ecrire la configuration actuelle en Flash

```
Switch# write
```

Changer le nom d'hôte

```
Switch# configure terminal
Switch(config)# hostname sw-test
sw-test(config)# end
```

Changer le nom de domaine

```
Switch# conf t
Switch(config)# ip domain-name test.com
Switch(config)# end
```

Chiffrer les mots de passe

```
Switch# configure terminal
Switch(config)# service password-encryption
```

Mise en place d'un mot de passe "enable"

Attention : Apparaitra en clair si password-encryption n'est pas activé !

```
Switch# configure terminal
Switch(config)# enable password le_mot_de_passe
Switch(config)# end
```

Note : si besoin de désactiver un ancien mot de passe, il peut être nécessaire de faire no enable secret

Mise en place d'un mot de passe telnet

```
Switch# configure terminal
Switch(config)# line vty 0 4
Switch(config-line)# password le_mot_de_passe
Switch(config-line)# login
Switch(config-line)# end
```

Mise en place d'un mot de passe console

Note : ne fonctionne pas a priori...

```
Switch# configure terminal
Switch(config)# line vty 5 15
Switch(config-line)# password le_mot_de_passe
Switch(config-line)# login
Switch(config-line)# end
```

Synchronisation NTP

```
Switch# ntp server 31.170.8.123
Switch# show ntp status
Switch# show ntp associations
```

Infos/gestion d'une interface

Voir l'état et la vitesse de tous les ports :

```
Switch# show interfaces status
```

Statut d'une interface :

```
Switch# show interfaces GigabitEthernet1/0/48
```

Infos détaillées sur la config d'un port :

```
Switch# show interfaces GigabitEthernet1/0/48 switchport
```

Désactiver/activer une interface :

```
Switch# conf t
```

```
Switch# interface GigabitEthernet1/0/48
Switch# shutdown
Switch# no shutdown
Switch# exit
```

Forcer la vitesse du port :

```
Switch# conf t
Switch# interface GigabitEthernet1/0/48
Switch# speed {10,100,1000,auto}
Switch# exit
```

Affecter un nom / une description à l'interface :

```
Switch# conf t
Switch# interface GigabitEthernet1/0/48
Switch# description Machine XYZ
```

Gestion du MTU pour toutes les interfaces Gigabits :

system mtu jumbo 9000

Gérer les fichiers/répertoires

```
Switch# cd flash:
Switch# cd rep
Switch# dir
Switch# copy foo bar
Switch# delete bar
Switch# mkdir rep
Switch# rm rep
Switch# more info.txt
Switch# verify image.bin
```

Commandes à manipuler avec précaution :

```
Switch# fsck
Switch# erase
Switch# format
```

Reboot complet du switch

```
Switch# reload
```

Reset complet du switch

Avec le bouton MODE

Si l'on appuye plus de 8 secondes sur le bouton MODE, le switch redémarre et sera remis en configuration d'usine !

Autre méthode sans mot de passe

Sur certains modèles, cette méthode ne fonctionne pas. Après être raccorder au switch, il faut le redémarrer en maintenant le bouton MODE enfoncé.

Ensuite, initialiser le file system flash :

```
switch: flash_init
switch: load_helper
```

Si on veut on peut sauvegarder, ou la supprimer l'ancienne configuration :

```
switch: dir_flash:
switch: rename flash:config.text flash:config.old
```

Enfin on boot :

```
switch: boot
```

Sauvegardes

Voir la liste des protocoles disponibles :

```
Switch# show file systems
File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -    opaque     ro   bs:
*   57931776    42733568     flash     rw   flash: flash1:
           -           -    opaque     rw   system:
           -           -    opaque     rw   tmpsys:
      524288      518420     nvram     rw   nvram:
           -           -    opaque     rw   null:
           -           -    opaque     ro   tar:
           -           -   network     rw   tftp:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
           -           -   network     rw   rcp:
           -           -   network     rw   http:
           -           -   network     rw   ftp:
           -           -   network     rw   scp:
           -           -   network     rw   https:
           -           -    opaque     ro   cns:
Switch# show flash

Directory of flash:/

  581  -rwx           5  Mar 21 2012 19:19:25 +01:00  private-config.text
  582  -rwx        3096  Mar 21 2012 19:19:25 +01:00  multiple-fs
  583  -rwx        2739  Mar 21 2012 19:19:25 +01:00  config.text
    2  drwx         512   Mar 1 1993 01:14:39 +01:00  c2960s-universalk9-mz.122-55.SE3

57931776 bytes total (42733568 bytes free)
```

Copier la configuration actuelle dans un fichier nommé sauvegarde :

```
Switch# copy running-config sauvegarde
Destination filename [sauvegarde]?

2739 bytes copied in 2.076 secs (1319 bytes/sec)

Switch# show flash

Directory of flash:/

  580  -rwx        2739  Mar 21 2012 19:29:32 +01:00  sauvegarde
  581  -rwx           5  Mar 21 2012 19:19:25 +01:00  private-config.text
  582  -rwx        3096  Mar 21 2012 19:19:25 +01:00  multiple-fs
  583  -rwx        2739  Mar 21 2012 19:19:25 +01:00  config.text
    2  drwx         512   Mar 1 1993 01:14:39 +01:00  c2960s-universalk9-mz.122-55.SE3
```

```
57931776 bytes total (42729984 bytes free)


Switch# delete sauvegarde
Delete filename [sauvegarde]?
Delete flash:/sauvegarde? [confirm]
```

On peut aussi envoyer la configuration sur un serveur distant :

Switch# copy running-config ftp://<IP>/rep/sauvegarde_29fevrier2012.txt

De même, on peut sauvegarder le firmware du switch sur un serveur distant :

```
Switch# cd flash:/
Switch# cd c2960s-universalk9-mz.122-55.SE3
Switch# dir

Directory of flash:/c2960s-universalk9-mz.122-55.SE3/

    3  drwx        5632   Mar 1 1993 01:08:54 +01:00  html
  578  -rwx    10907578   Mar 1 1993 01:10:24 +01:00  c2960s-universalk9-mz.122-
55.SE3.bin
  579  -rwx         484   Mar 1 1993 01:13:44 +01:00  info

Switch# copy flash:/c2960s-universalk9-mz.122-55.SE3/c2960s-universalk9-mz.122-
55.SE3.bin ftp://<IP>/rep/sauvegarde_firmware.bin
```

Pour sauvegarder la liste des VLANs, c'est le fichier vlan.dat qui nous intéresse :

```
Switch# copy flash:/vlan.dat ftp://<IP>/rep/sauvegarde_vlan.dat
```

Mettre à jour IOS

Si il y a assez de place sur la mémoire flash (dir flash:), copier le nouveau firmware dessus (copy ftp://<IP>/fichier.bin flash:), sinon effacer le contenu de la flash (erase flash:), puis placer le nouveau firmware. Ensuite, il suffit de spécifier de charger le nouveau firmware.

```
enable
conf t
system boot flash:new_firmware.bin
reload
```

Gestion des VLANs

Affecter une adresse IP à un VLAN

```
configure terminal
interface Vlan 1
ip address 192.168.0.10 255.255.255.0
```

Créer un VLAN

Dans cet exemple, ce sera le VLAN d'ID 2 nommé "bob".

```
Switch# configure terminal
Switch(config)# vlan 2
Switch(config-vlan)# name bob
Switch(config-vlan)# end
Supprimer un VLAN
Switch# configure terminal
```

```
Switch(config)# no vlan 2
Switch(config)# end
```

Affecter des interfaces (ports) à un VLAN

Dans cet exemple on affecte l'interface GigabitEthernet 0/13 au VLAN 2

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet0/13
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

On peut affecter un range de ports à un VLAN :

```
Switch# conf t
Switch(config)#interface range GigabitEthernet1/0/1-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 13
Switch(config-if-range)#exit
```

Voir la configuration des VLAN

D'un VLAN en particulier

```
Switch# show vlan <ID>
Switch# show interfaces vlan <ID>
```

De tous les VLAN

Voir un résumé de la configuration :

```
Switch# show vlan brief
```

Voir la configuration de tous les VLAN :

```
Switch# show vlan
```

Faire un port trunk

Dans cet exemple l'interface trunké est l'interface GigabitEthernet0/24

```
Switch# configure terminal
Enter configuration commandsss, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet0/24
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
```

Sur les 2960, le switch ne supporte que le dot1q. On aura juste à basculer le port en mode trunk :

```
# switchport mode trunk
```

Il est possible de spécifier le ou les vlans transportés par le trunk :

```
# switchport trunk allowed vlan 11,13
```

Astuce : pour ajouter un VLAN sur un trunk sans reprendre toute la liste de ceux déjà autorisés on peut utiliser la syntaxe :

```
# switchport trunk allowed vlan add 42
```

Une façon de contrôler si le trunk est bien mis en place des 2 côté est de consulter la sortie de la commande "show vlan brief". Si le port est toujours dans le vlan 1, c'est que le trunk n'est pas opérationnel (interface non montée, ou port distant non configuré en trunk). Si tout fonctionne bien, on ne doit le voir dans aucun vlan, mais on le verra en trunk dans un "show interfaces status".

Pour afficher les VLAN autorisés sur un trunk :

```
# show interfaces Gi1/0/50 trunk
```

ATTENTION : si l'on configure un port trunk, il est indispensable de créer le VLAN sur le switch, sinon cela ne marche pas !

Administration à distance

Par HTTP/HTTPS

"Les interfaces web, c'est pour les lusers" :

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no ip http secure-server
Switch(config)# no ip http server
```

Par SSH

Activation et ajout d'un utilisateur local :

```
configure terminal
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa authorization network default local
#username name privilege 15 password 7 le_mot_de_passe #password 0 le_mot_de_passe ==>
en clair
username root privilege 15 secret 0 mot_de_passe
end
```

Important : Mettre en place le nom d'hôte et le nom de domaine.

Activation de SSH :

```
configure terminal
crypto key generate rsa
```

Activer SNMP

Afin de permettre des requêtes SNMP :

```
Switch# conf t
(config)# snmp-server community public RO
```

On pourra ainsi faire des requêtes du type :

```
$ snmpwalk -v2c -c public <IP switch> .1
```

Configuration IP

Configuration IP de base :

```
Switch# conf t
(config)# interface Vlan1
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# no shutdown
```

La configuration IP de base permet un accès au switch via telnet

Désactiver services web

```
Switch(config)#no ip http server
Switch(config)#no ip http secure-server
```

Gestion des adresses MAC

Lister toutes les adresses MAC connues :

```
Switch#show mac address-table
Switch#show mac address-table int Gi0/11
```

Gestion des adresses MAC dynamiques, notamment forcer la suppression

```
Switch#clear mac address-table dynamic
Switch#clear mac address-table dynamic address <mac>
Switch#clear mac address-table dynamic interface <if>
Switch#clear mac address-table dynamic vlan <id>
```

Configurer des alertes lors de modifications :

```
snmp-server enable traps mac-notification change
snmp-server enable traps mac-notification move
```

Forcer des adresses MAC de façon statique :

```
mac address-table static <mac> vlan <id> interface <if>
```

STP : Spanning Tree Protocol

http://en.wikipedia.org/wiki/Spanning_Tree_Protocol

Le STP est un protocole permettant de détecter et désactiver automatiquement des boucles sur un segment Ethernet. Cela permet donc d'éviter une boucle faite par erreur (ce qui en découle sur un Packet Storm et un réseau très dégradé) ...ou de créer des boucles volontairement pour assurer de la redondance !

Le principe de fonctionnement est qu'un des switchs est élu ROOT (racine de l'arbre STP), et qu'un coût est associé à chaque lien vers le ROOT. Ce coût est calculé automatiquement à partir du nombre de connexions et du type de ces connexions (un lien 10Mb/s coûte 100, un lien 100Mb/s coûte 19, un lien 1Gb/s coûte 4, etc.). Ce coût peut aussi être forcé manuellement si l'on veut influencer le calcul du STP. Ensuite, grâce à ces coûts, si une boucle est détectée certains ports peuvent être bloqués. Des vérifications sont réalisées régulièrement pour détecter un changement et adapter les blocages si nécessaire.

/!\ Le keepalive - élement essentiel pour STP - n'est pas activé par défaut sur les ports **SFP** d'un switch Cisco : il faut absolument l'activer si vos segments Ethernet sont propagés sur les ports SFP !

```
Switch#conf t
```

```
(config)# int Gi0/49
(config-if)# keepalive
```

Sur les Cisco 2960-2970, le STP est géré par VLAN on parle de « per-VLAN spanning-tree plus (PVST+) » et si le mode « Rapid » est activé de « rapid per-VLAN spanning-tree plus (rapid-PVST+) ».

La valeur par défaut de la priorité du root switch est 3276.

Le root ID est calculé avec cette priorité + une dérivation de l'adresse MAC.

C'est le plus petit ID qui l'emporte. Il peut être intéressant de changer la priorité pour choisir le switch root.

On peut aussi changer la priorité des ports (128 par défaut + coût du lien [10MBps = 100, 100Mbps = 19, 1Gbps = 4]) pour influencer le calcul SPT et les connexions à désactiver.

La configuration par défaut des timers respecte les recommandations de la norme 802.1d.

```
Hello time: 2 seconds.
Forward-delay time: 15 seconds.
Maximum-aging time: 20 seconds.
Transmit hold count: 6 BPDUs
```

Il faut avoir les mêmes valeurs si d'autres équipements interviennent sur le réseau, comme des machines OpenBSD ou Linux.

Voir les informations du STP sur le switch :

```
#show spanning-tree summary
#show spanning-tree
#show spanning-tree detail
```

Activer le mode rapid STP 802.1w.

```
#conf t
(config)#spanning-tree mode rapid-pvst
```

Forcer un switch en root (la priorité sera calculée automatiquement).

```
#conf t
(config)#spanning-tree vlan 1-4096 root primary
```

Changer le coût d'un port :

```
Switch# conf t
(config)# interface gigabitEthernet 0/50
(config-if)# spanning-tree cost 65536
```

Changer le coût uniquement pour un ou plusieurs VLANs :

```
# spanning-tree vlan 1-4096 cost 1
rate-limiting
```

On peut forcer un port à rate-limiter à 10, 20, 30.... ou 90% de sa capacité.

Par exemple pour rate-limiter à du 8 Mb/s :

```
int Gi0/1
speed 10
```

```
srr-queue bandwidth limit 80
```

Infos sur le rate-limiting :

```
show mls qos interface GigabitEthernet0/1 queueing
GigabitEthernet0/1
QoS is disabled. When QoS is enabled, following settings will be applied
Egress Priority Queue : disabled
Shaped queue weights (absolute) :  25 0 0 0
Shared queue weights  :  25 25 25 25
The port bandwidth limit : 10  (Operational Bandwidth:11.12)
The port is mapped to qset : 1
```

Cisco L3

DHCP relay sur plusieurs VLANs

Exemple de mise en oeuvre de DHCP Relay sur 2 VLANs

Serveur DHCP

Côté serveur DHCP (serveur linux), configurer un subnet par VLAN. Penser aux routes permettant d'accéder à chaque réseau de chaque VLAN. Le serveur DHCP pourra être dans un VLAN dédié.

Cisco 3750

Pour activer le DHCP Relay, sur chaque interface VLAN, rajouter la directive ip address helper <ip-server-dhcp>.

Voici un exemple de création d'un VLAN avec l'adresse 192.168.200.1/24, faisant office de DHCP relay pour le serveur 10.0.1.2 :

```
(config)#interface vlan 200
(config-if)#ip address 192.168.200.1 255.255.255.0
(config-if)#ip helper-address 10.0.1.2
(config-if)#end
```

On répètera cette manipulation pour chaque VLANs et chaque subnet déclaré sur le serveur DHCP que l'on souhaite activer.

Routage Inter-VLANs

L'activation du routage inter-VLANs se fait de la manière suivante :

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

Tous les VLANs seront routés entre eux. Il sera possible si besoin de limiter le routage inter-VLANs grâce aux ACLs.

Définir une route par défaut

```
(config)# ip default-gateway IP_routeur
```

ou

(config)# ip route 0.0.0.0 0.0.0.0 IP_routeur

Divers

Cron / tâches planifiées

Voir http://www.tmartin.io/articles/2010/sauvegarder-la-configuration-de-cisco-ios-vers-un-serveur-distant-avec-kron/

Désactiver la vérification des modules GBIC

Par défaut, CISCO n'autorise pas les modules GBIC non agréés, il faut donc désactiver la vérification des checksum des modules GBIC pour pouvoir les connecter :

```
#conf t
#service unsupported-transceiver
On peut ensuite les lister via :
#show inventory
```

Remettre un port désactivé par errdisable

Un port est désactivé dans divers cas, tel que la non-autorisation des modules GBIC tiers.

```
#conf t
#interface GigabitEthernet0/28
#shutdown
#no shutdown
```

Consulter les informations DOM d'un SFP

Pour surveiller la température, ou le voltage :

```
Switch# show interface transceiver
```

Passer un port SFP en "speed nonegotiate"

On ne peut pas forcer la vitesse d'un port SFP... mais il faut parfois passer en "speed nonegotiate" :

```
(config-if)# speed nonegotiate
(config-if)# shutdown
(config-if)# no shutdown
```

Lire http://herdingpackets.net/2013/03/21/disabling-gigabit-link-negotiation-on-fiber-interfaces/

Synchro immédiate : Spanning Tree Portfast

Lorsque l'on se branche sur un port, il faut 50s pour qu'il soit utilisable à cause du Spanning Tree. Le Spanning Tree Portfast permet de passer un port dans l'état forwarding de façon immédiate, en lui faisant sauter les états listening et learning. On utilisera cette commande uniquement si l'on est sûr de ne pas avoir besoin du Spanning Tree (serveur non virtuel connecté directement au port, etc.).

Activer

```
(config)#interface GigabitEthernet0/28
(config-if)#spanning-tree portfast
```

Désactiver

```
(config)#interface GigabitEthernet0/28
```

(config-if)#no spanning-tree portfast

Exemple sur packet tracer en version rapide.

```
switch

3650 24ps
une fois le boot lancé

on change le hostname
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#host
Switch(config)#hostname 3650G
3650G(config)#

on renseigne le domaine
3650G(config)#ip domain-name mondomaine.moi

on active le chiffrement des mots de passe.
3650G(config)#service password-encryption

Activation de ssh
3560G(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
3650G(config)#
3650G#
%SYS-5-CONFIG_I: Configured from console by console

on cree la clef RSA pour SSH
3650G(config)#crypto key generate rsa
The name for the keys will be: 3650G.mondomaine.moi
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


Un mot de passe doit etre créé pour se loguer aux différentes lignes.
3560G(config)#enable secret erty
3560G(config)#line con 0
3560G(config-line)#password erty
3560G(config-line)#login
3560G(config-line)#exit
3560G(config)#line vty 0 15
3560G(config-line)#password erty
```

```
3560G(config-line)#login
3560G(config-line)#end

on cree un utilisateur et on active  password et secret

3560G(config)#aaa new-model
3560G(config)#aaa authentication login default local
3560G(config)#username admin secret erty

Désactivation de telnet pour l'accès au switch
3560G(config)#line vty 0 15
3560G(config-line)#transport input ssh
3650G(config-line)#end

on cree les vlans

rappel
1 blackhole
1 gestion
1 salle 1, 2 , 3 et 4
1 trunked
1 natif

(config)#vlan 2, 10, 20, 30, 40, 99, 100, 101

3650G#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, 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
                                                 Gig0/1, Gig0/2
2    native                            active
10   salle_1                           active
20   salle_2                           active
30   salle_3                           active
40   salle_4                           active
99   gestion                           active
100  trunk                             active
101  blackhole                         active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

je place toutes les interfaces dans le vlan 101

```
3650G#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1, Gig0/2
2    native                            active
10   salle_1                           active
20   salle_2                           active
30   salle_3                           active
40   salle_4                           active
99   gestion                           active
100  trunk                             active
101  blackhole                         active    Fa0/1, Fa0/2, 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
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

et les 2 interfaces qui serviront de trunk dans un vlan du nom trunk
juste pour que cela soit ordonné. on reviendra sur le trunk apres la configuration des vlans

```
3650G(config)#int range gig0/1-2
3650G(config-if-range)#switchport access vlan 100
3650G(config-if-range)#no shut
3650G(config-if-range)#end
```

je place les ports dans les vlans

```
3650G(config)#int fa0/1
3650G(config-if)#swi
3650G(config-if)#switchport acces
3650G(config-if)#switchport access
3650G(config-if)#switchport access vlan 10
3650G(config-if)#no shut
3650G(config-if)#swi
3650G(config-if)#switchport mode acc
3650G(config-if)#switchport mode access
3650G(config-if)#ex

3650G#sh vlan brief
```

```
VLAN Name                       Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                    active
2    native                     active
10   salle_1                    active    Fa0/1
20   salle_2                    active    Fa0/2
30   salle_3                    active    Fa0/3
40   salle_4                    active    Fa0/4
99   gestion                    active    Fa0/24
100  trunk                      active    Gig0/1, Gig0/2
101  blackhole                  active    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
1002 fddi-default               active
1003 token-ring-default         active
1004 fddinet-default            active
1005 trnet-default              active
3650G#
```

je donne a mes vlans une ip en restant logique avec les reseaux

```
3650G(config)#int vlan 10
3650G(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

3650G(config-if)#ip address 192.168.10.1 255.255.255.0
3650G(config-if)#ex

3650G(config)#int vlan 20
3650G(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

3650G(config-if)#ip address 192.168.20.1 255.255.255.0
3650G(config-if)#ex

3650G(config)#int vlan 30
3650G(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

ip address 192.168.30.1 255.255.255.0
3650G(config-if)#ex

3650G(config)#int vlan 40
3650G(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up
ip address 192.168.40.1 255.255.255.0
```

```
3650G(config-if)#ex

3650G(config)#int vlan 99
3650G(config-if)#ip address 192.168.1.1 255.255.255.0
3650G(config-if)#no shut
3650G(config-if)#end



a ce stade je sauvegarde et je reload

copy ru st
puis reload

Press RETURN to get started!



User Access Verification

Username: admin
Password:
3650G>en
Password:
3650G#

je renseigne une passerelle par defaut dans le meme reseau que le poste admin

3560G(config)#ip default-gateway
3650G(config)#ip default-gateway 192.168.1.254
3650G(config)

maintenant je connecte 4 pc sur chaque port
avec une ip un masque et une passerelle par defaut

etant donnée que j'ai choisi une ip en .1 pour le vlan , je choisi la .254 comme passerelle

a ce stade , le PC10 en salle 1 , ne ping pas le PC20 en salle 2
Packet Tracer PC Command Line 1.0
PC>ping 192.168.20.20

Pinging 192.168.20.20 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

sur le switch
J'active le routage
3650G(config)#ip routing

je parametre mon lien trunk sur gig0/1

3650G(config)#int gig0/1
no shut
3650G(config-if)#switchport trunk encapsulation dot1q
3650G(config-if)#switchport mode trunk

3650G(config-if)#switchport trunk allowed vlan 2,10,20,30,40,99

3650G(config-if)#switchport trunk allowed vlan add 10
3650G(config-if)#switchport trunk allowed vlan add 20
3650G(config-if)#switchport trunk allowed vlan add 30
3650G(config-if)#switchport trunk allowed vlan add 40

3650G(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 GigabitEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
3650G(config-if)#no cdp enable
3650G(config-if)#ex
3650G(config-if)#end

on desactive Le protocole DTP (Dynamic Trunking Protocol)
3650G(config)#int range fa0/1-24
3650G(config-if-range)#swi
3650G(config-if-range)#switchport none
3650G(config-if-range)#switchport nonegotiate
3650G(config-if-range)#end

on active spanning-tree
3560G(config)#spanning-tree mode rapid-pvst

On autorise seulement un poste a se connecte sur la Vty 10 , par exemple,seul l'ip du pc adminstrateur.
3650G(config)#access-list 10 permit 192.168.1.10 0.0.0.255

On autorise la connexion exclusive de ce réseau sur les terminaux virtuel avec la commande access-class
3650G(config)#line vty 0 15
3650G(config-line)#access-class 10 in
3650G(config-line)#exit

```
3650G(config)#
3650G(config)#line vty 0 15
3650G(config-line)#no login local
3650G(config-line)#transport input ssh
3650G(config-line)#end
```

a ce stade on ajoute un routeur 2911
et on cree des interface virtuel qui auront pour ip la passerelle par defaut de chaque reseau

```
Router(config)#int gig0/0.1
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int gig0/0.2
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.3
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.4
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#ex
```

on relie avec un cable et on teste avec ping et ssh .