

# La couche OSI 2

## 1. Introduction

Comme point de départ, nous utilisons un document édité par la NSA concernant la sécurisation des switches dans l'environnement IOS :

Les recommandations sont les suivantes :

- Accès physique aux commutateurs au seul personnel autorisé
- Installer la dernière version stable de l'IOS sur chaque commutateur.
- Mettre des mots de passe sur les interfaces d'administration (par défaut vide !)
- Mettre des timeout pour les sessions d'administration et configurer les niveaux de privilèges.
- Configurer une bannière indiquant que l'accès non autorisé est interdit.
- Désactiver les services réseau inutiles (par exemple : SNMP , HTTP).
- Activer les services réseau nécessaires et configurer ces services en toute sécurité.
- Si possible, gérer les switches hors réseau (par câble console). Sinon, créer un VLAN dédié à l'administration.
- Utiliser SSH au lieu de telnet et définir un mot de passe fort pour SSH.
- Si SNMP est nécessaire, définir une chaîne de communauté forte pour SNMP.
- Mettre en oeuvre la sûreté des ports pour limiter l'accès basé sur l'adresse MAC.
- Désactiver l'auto-agrégation sur les ports.
- Utiliser la capacité du commutateur en miroir des ports pour l'accès IDS.
- Désactiver les ports de commutateur non utilisés et leur attribuer un numéro de VLAN inutilisé.
- Attribuer un numéro de ports trunk VLAN natif qui n'est pas utilisé par tout autre port.
- Limiter les VLAN qui peuvent être transportés sur un tronc à seulement ceux qui sont nécessaires.
- Utiliser la configuration VLAN statiques.
- Si possible, désactiver VTP. Sinon, configurer le domaine de gestion, un mot de passe et le pruning, puis passer VTP en mode transparent.
- Utiliser les listes de contrôle d'accès (ACL) lorsque nécessaire.
- Activer la journalisation et envoyer des journaux à hôte de journalisation dédié et sécurisé.
- Configurer la journalisation pour inclure des informations de temps précis, en utilisant NTP et les horodatages.
- Revue des journaux pour d'éventuels incidents et les archiver conformément à la politique de sécurité.
- Utiliser les fonctionnalités AAA (Radius) pour autoriser l'accès local et distant.
- Gérer l'historique des versions du fichier de configuration des routeurs dans un système sécurisé.

Nous allons essayer d'implémenter une partie de tout cela....

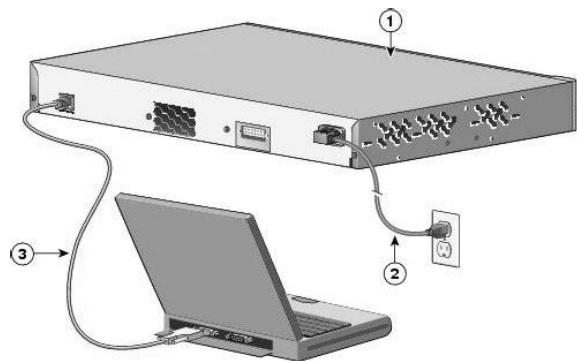
## 2. Le déballage du carton

Nous allons construire notre beau réseau. Voici où nous en sommes : nous avons tout conçu et nous avons tout commandé. Mais que faire lorsque le livreur est reparti et que vous vous retrouvez face à une pile de cartons avec de jolis commutateurs à configurer.

Chez CISCO, les appareils n'ont par défaut aucune configuration réseau. Mais ils sont livrés avec un câble particulier (de couleur bleue) appelé « câble console ». Ce câble est en fait un câble série qui d'un côté dispose d'un port DB9 et de l'autre un port RJ45 (mais ce n'est pas un câble réseau !).



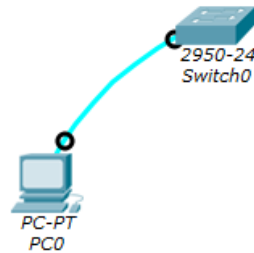
La connexion sera la suivante :



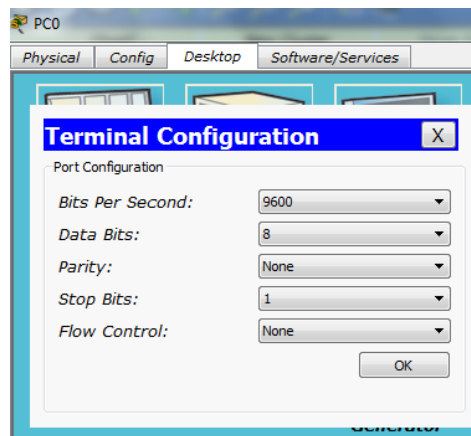
Du côté switch ou routeur, le port est également repéré par une couleur bleue (ce n'est pas un port réseau !) :



Ceci peut être simulé dans Packet Tracer en prenant le câble bleu et en connectant le port RS232 côté PC au port Console côté switch. Réalisez donc cette première configuration avec un switch 2950-24 :



Ensuite, pour prendre la main sur le switch, il faut un logiciel permettant la connexion par port série (par exemple, Hyperterminal sous Windows). Les paramètres à configurer seront les suivants :



### 3. Configuration de base

Cliquez sur le PC puis sur l'onglet « Desktop » puis sur « Terminal ». Les paramètres proposés sont les bons. Vous devez voir apparaître les mêmes choses que dans l'onglet « CLI » du switch : l'interface en ligne de commande IOS (Internetwork Operating System, OS chez CISCO).

**IMPORTANT** : vous devez détailler le sens de chaque commande avec l'aide en ligne IOS ou Internet si besoin (commande ?).

*Switch>*

Passons en mode privilégié :

*Switch>enable*

Allons dans le terminal de configuration :

*Switch#conf t*

*Enter configuration commands, one per line. End with CNTL/Z.*

Dans la vraie vie, pour faciliter l'administration du parc, il est vivement conseillé de définir un nom pour chaque élément actif ayant un sens :

*Switch(config)#hostname sw1*

Désactivons la résolution de nom DNS qui ne marchera pas ici et qui bloque le switch pendant un moment en cas d'erreur de saisie

```
sw1(config)#no ip domain-lookup
```

Définissons un mot de passe chiffré pour le mode enable :

```
sw1(config)#enable secret !Cisco123!
```

Protégeons également le mode Telnet :

```
sw1(config)#line vty 0 15
```

```
sw1(config-line)#password !Cisco123!
```

```
sw1(config-line)#login
```

```
sw1(config-line)#exec-timeout 4
```

```
sw1(config-line)#motd-banner
```

**Important :** dans la vraie vie, vous n'utiliserez PAS telnet mais SSH. Packet Tracer ne le supporte pas pour les switches (mais le supporte pour les routeurs...). Il faudrait ici mettre une commande « transport input ssh » et générer une clé.

```
sw1(config-line)#exit
```

Protégeons le mode console :

```
sw1(config)#line console 0
```

```
sw1(config-line)#password !Cisco123!
```

```
sw1(config-line)#login
```

```
sw1(config-line)#exec-timeout 4
```

```
sw1(config-line)#motd-banner
```

```
sw1(config-line)#exit
```

Définissons une bannière qui préviendra les petits curieux :

```
sw1(config)#banner motd #
```

```
Enter TEXT message. End with the character '#'
```

```
*****
```

```
** Toutes les tentatives d'accès sont enregistrées **
```

```
*****
```

```
#
```

## 4. Le VLAN d'administration

Une fois les premières configurations réalisées par câble console, il est fort probable que vous administrerez ensuite vos switches à distance via SSH. Sinon c'est conseillé mais difficile à mettre en oeuvre car cela veut dire qu'à chaque changement de configuration il faut se déplacer physiquement à proximité du switch.

Pour rappel, il faut dissocier les flux de données des flux d'administration, règle de sécurité élémentaire. Sur ce VLAN, seuls les informaticiens seront habilités à se connecter pour faire une seule tâche : administrer les éléments actifs du réseau.

Nous créons un nouveau VLAN :

```
sw1(config)#vlan 1000
```

```
sw1(config-vlan)#name admin
```

```
sw1(config-vlan)#exit
```

Nous affectons une adresse IP d'administration (le VLAN est vu comme une « interface ») :

```
sw1(config)#int vlan 1000
```

```
sw1(config-if)#
```

```
%LINK-5-CHANGED: Interface Vlan1000, changed state to up
```

```
sw1(config-if)#ip address 172.16.254.1 255.255.0.0
```

```
sw1(config-if)#no shut
```

```
sw1(config-if)#
```

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

```
sw1(config-if)#exit
```

Nous décidons de connecter notre PC d'administration sur le port Fa0/1 du switch, nous le passons donc dans le bon VLAN :

```
sw1(config)#int fa0/1
```

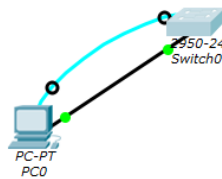
```
sw1(config-if)#switchport mode access
```

```
sw1(config-if)#switchport access vlan 1000
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1000, changed state to up
```

```
sw1(config-if)#
```

Il ne reste plus qu'à relier un PC sur le bon port :



On configurera le PC avec une adresse IP dans la plage 172.16.x.x. On peut à ce stade débrancher le câble console, l'administration pourra se poursuivre avec un telnet 172.16.254.1 lancé depuis le PC. Vous devez donc obtenir ceci :

```
Command Prompt
Packet Tracer PC Command Line 1.0
PC>telnet 172.16.254.1
Trying 172.16.254.1 ...
% Connection timed out; remote host not responding
PC>telnet 172.16.254.1
Trying 172.16.254.1 ... Open
*****
**      Toutes les tentatives d'accès sont enregistrées      **
*****

User Access Verification

Password:
```

Remarque : il faut au préalable, modifier le vlan associé au port du switch où est relié le PC.

## 5. Mise à jour de l'IOS

Nous abordons ici une des principales missions de l'administrateur réseau : tenir à jour ses systèmes.

### 5A. Préambule

La prochaine étape consiste à vérifier la version du système installée sur les appareils et à vérifier si une mise à jour n'existe pas. Ne foncez pas sur la rubrique « download » du site cisco.com, les mises à jour sont payantes et sont en général accessibles via votre revendeur et dans le cadre d'un contrat de maintenance.

Cette opération est délicate car elle peut rendre inutilisable l'appareil en cas de problème pendant le processus (coupure de courant par exemple...). Il faut donc prendre quelques précautions. Il faut bien sûr garder une copie de la configuration du switch mais il est également conseillé de faire une sauvegarde de l'image d'IOS actuellement utilisée au cas où il faudrait revenir en arrière.

Vérifions la version d'IOS installée sur notre switch 2950 :

```
sw1#show ver
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE
SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
[...coupé...]
```

Dans le flot d'informations, la version est affichée dès le départ.

Sauvegardons la configuration de la mémoire vive du switch vers la nvram (mémoire non volatile) :

```
sw1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
sw1#dir nvram:
Directory of nvram:/
 238 -rw- 996 <no date> startup-config
 996 bytes total (237588 bytes free)
sw1#
```

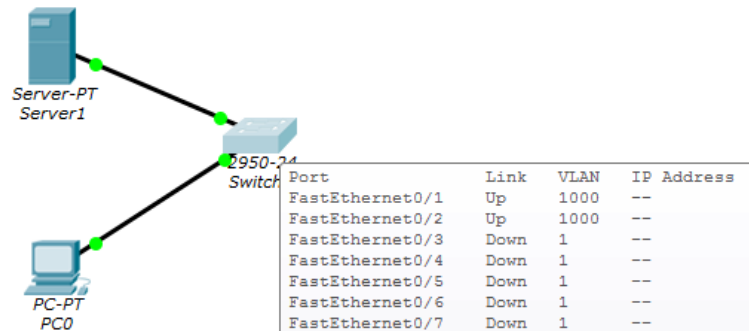
Par mesure de précautions, nous exporterons tout à l'heure cette configuration vers un serveur TFTP (Trivial File Transfert Protocol, un protocole simplifié de transfert de fichier qui fonctionne en UDP sur le port 69, transfert vers routeur, switch)

### 5B. Mise en place de la source

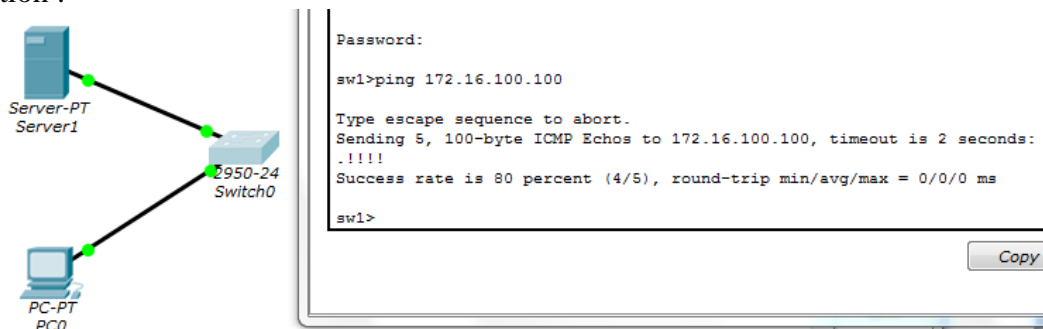
Il faut bien que la nouvelle image de l'IOS soit stockée quelque part. Historiquement, il fallait disposer d'un serveur TFTP, ce que nous allons faire. Sachez néanmoins, que maintenant ce processus est beaucoup plus simple car il se fait via une simple clé USB.

Travail à faire : installez un serveur, affectez-lui une adresse IP 172.16.x.x, connectez-le sur le port fa0/2 du switch, mettez ce port dans le VLAN 1000, un ping lancé vers cette machine depuis le switch doit fonctionner correctement (bien attendre que les ports du switch redeviennent verts).

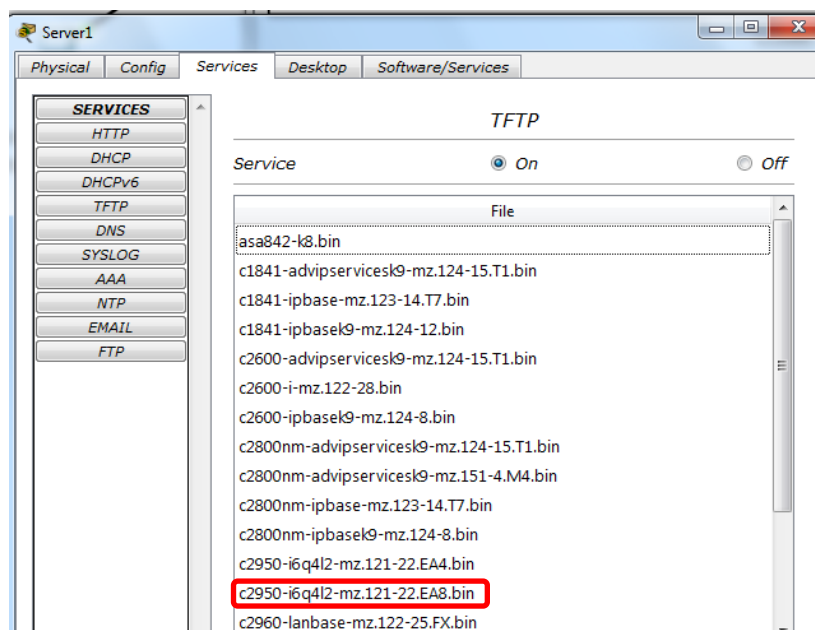
Réseau :



Validation :



Ouvrons maintenant le serveur et allons dans « Services/TFTP » vérifier si une image plus récente de l’IOS de notre switch 2950 est disponible :



Nous avons une image plus récente (version EA8) alors que la version installée est en EA4. Dans la vraie vie, il vous appartiendra bien sûr de placer la bonne image sur un serveur TFTP que vous aurez monté pour l’occasion.

## 5C. Sauvegardes

Envoyons une copie de notre configuration sur le serveur TFTP :

```
sw1#copy running-config tftp:
Address or name of remote host []? 172.16.100.100
Destination filename [sw1-config]?
Writing running-config...!!
[OK - 1104 bytes]
1104 bytes copied in 0.031 secs (35000 bytes/sec)
```

Faisons une sauvegarde de l'image actuelle de l'IOS (même si elle est déjà dans le serveur TFTP, un exercice...). Celle-ci se trouve dans la mémoire flash :

```
sw1#dir flash
Directory of flash:/

 1 -rw-     3058048      <no date>  c2950-i6q4l2-mz.121-22.EA4.bin
 4 -rw-         1482      <no date>  config.text
 2 -rw-         616      <no date>  vlan.dat

64016384 bytes total (60956238 bytes free)
```

Puis :

```
sw1#copy flash: tftp
Source filename []? c2950-i6q4l2-mz.121-22.EA4.bin
Address or name of remote host []? 172.16.100.100
Destination filename [c2950-i6q4l2-mz.121-22.EA4.bin]? monIos_2950.bin

Writing c2950-i6q4l2-
mz.121-22.EA4.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 3058048 bytes]

3058048 bytes copied in 0.055 secs (55600872 bytes/sec)
sw1#
```

Copy Paste

Remarque : utilisez éventuellement Copy/Paste pour le nom du fichier .bin

Constatons que ces deux fichiers sont maintenant bien présents sur TFTP :

```
c2950-i6q4l2-mz.121-22.EA4.bin
c3560-advipservicesk9-mz.122-37.SE1.bin
monIos_2950.bin
pt1000-i-mz.122-28.bin
pt3000-i6q4l2-mz.121-22.EA4.bin
sw1-config
```

Remove File



## 5D. Migrer

On vous rappelle que chaque switch dépasse les 1000 € alors si vous ne voulez pas avoir des saisies sur salaire pendant quelque temps, il vaut mieux faire très attention et bien copier la bonne image...

D'abord, vérifions que notre mémoire flash dispose de suffisamment d'espace :

```
sw1#dir flash
Directory of flash:/

   1  -rw-     3058048      <no date>  c2950-i6q412-mz.121-22.EA4.bin
   4  -rw-         1482      <no date>  config.text
   2  -rw-         616      <no date>  vlan.dat

64016384 bytes total (60956238 bytes free)
sw1#
```

---

Nous pourrions avoir les deux images en parallèle, ce qui pourra nous sauver en cas de problème : le switch pourra basculer sur l'ancienne image.

Récupérons la nouvelle image :

```
sw1#copy tftp flash:
Address or name of remote host []? 172.16.100.100
Source filename []? c2950-i6q412-mz.121-22.EA8.bin
Destination filename [c2950-i6q412-mz.121-22.EA8.bin]?

Accessing tftp://172.16.100.100/c2950-i6q412-mz.121-22.EA8.bin....
Loading c2950-i6q412-mz.121-22.EA8.bin from 172.16.100.100:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 3117390 bytes]

3117390 bytes copied in 3.062 secs (1018089 bytes/sec)
```

Changeons l'image de boot, puis redémarrons :

```
sw1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
sw1(config)#boot system flash:/c2950-i6q412-mz.121-22.EA8.bin
sw1(config)#exit
sw1#
%SYS-5-CONFIG_I: Configured from console by console

sw1#reload
Proceed with reload? [confirm]
```

Après le redémarrage, vérifions :

```
sw1#show ver
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA8 RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 12-May-06 17:19 by pt_team
```

Tout a l'air OK. Lorsque le bon fonctionnement sera validé, nous pourrions effacer l'ancienne image de l'IOS.

## 6. Journalisation

Une des difficultés est que nous avons de nombreux serveurs, de nombreux éléments actifs à gérer et qu'il faut suivre leur activité. Un sujet important sera de centraliser sur une machine les différents événements générés par ces appareils. Il s'agit des « logs » et un des protocoles faisant ce travail s'appelle « syslog ». Dans ce domaine, un élément important est le Temps et il faut à tout prix que toutes les machines soient synchronisées sinon il est impossible de faire une analyse rigoureuse d'un incident.

Le protocole internet NTP (Network Time Protocol) permet de synchroniser les machines en fonction d'une horloge de référence. Hélas, Packet Tracer ne permet pas de faire cette configuration sur les switches (mais on peut la faire sur les routeurs, Cisco n'aime pas les switches ?).

Dans l'immédiat, nous allons voir comment fixer l'horloge et envoyer les événements dans un serveur spécialisé. Il faut configurer notre fuseau horaire (GMT+1) puis l'heure doit être fixée en mode UTC (Universal Time Clock) :

```
sw1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
sw1(config)#clock timezone gmt 1
sw1(config)#exit
sw1#
%SYS-5-CONFIG_I: Configured from console by console
```

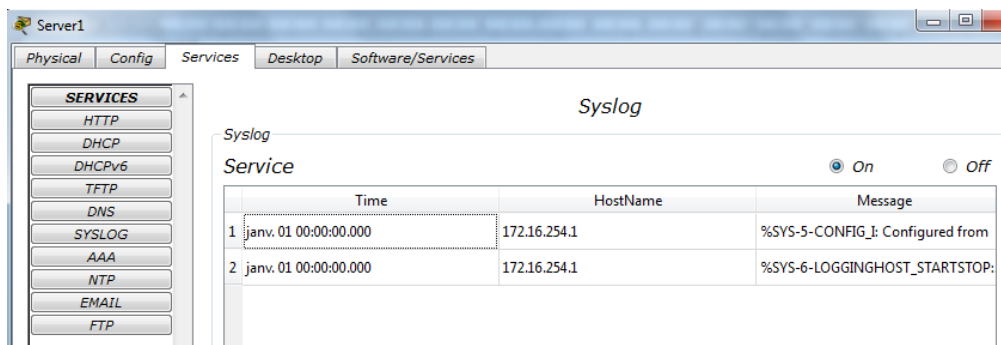
Réglage de l'heure :

```
sw1#clock set 21:38:00 22 nov 2017
sw1#show clock
22:38:8.200 gmt Wed Nov 22 2017
```

Enfin, il faut envoyer les logs sur le serveur syslog. Nous réutilisons ici notre serveur (tftp) de tout à l'heure (172.16.100.100 ici) :

```
sw1(config)#logging 172.16.100.100
sw1(config)#
```

Ce qui donnera dans le serveur (au bout d'un certain temps) :



Ainsi, tout événement sera enregistré. Il sera plus facile d'en faire le suivi.

## 7. Sécurisation par adresse MAC

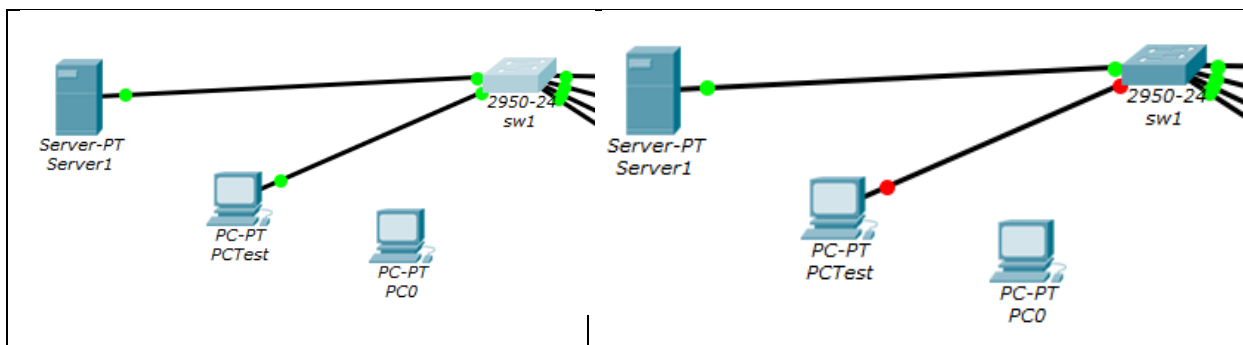
Dans le cours, pour éviter l’empoisonnement des tables de localisation nous avons vu qu’il était conseillé de forcer sur chaque port du switch l’adresse MAC de la machine connectée dessus. Cela empêche également que n’importe qui ne débranche un PC pour se connecter à la place.

Relevez l’adresse MAC du PC puis réalisez cette configuration :

```
sw1(config)#interface fastEthernet 0/1
sw1(config-if)#switchport port-security
sw1(config-if)#switchport port-security mac-address aaaa.bbbb.cccc
sw1(config-if)#switchport port-security violation shutdown
```

Bien sûr, vous remplacez aaaa.bbbb.cccc par l’adresse MAC du PC.

Faites un ping avec le switch, il ne doit pas y avoir de problème. Installez un nouveau PC, configurez une adresse IP 172.16.x.x. Débranchez l’ancien PC, connectez le nouveau, attendez que le port du switch soit redevenu vert et refaites un ping.



Vous devez constater que les deux ports sont devenus rouge. Pour réactiver le port du switch, il faudra faire un shutdown suivi d’un no shutdown, sur l’interface concernée.

D’autres politiques peuvent être mises en place : limiter simplement le nombre d’adresses derrière un port, n’autoriser que la première adresse MAC que verra passer le port, journaliser le problème sans bloquer le port, etc.

La commande show mac-address-table permet de suivre les adresses MAC découvertes ainsi que leur localisation.

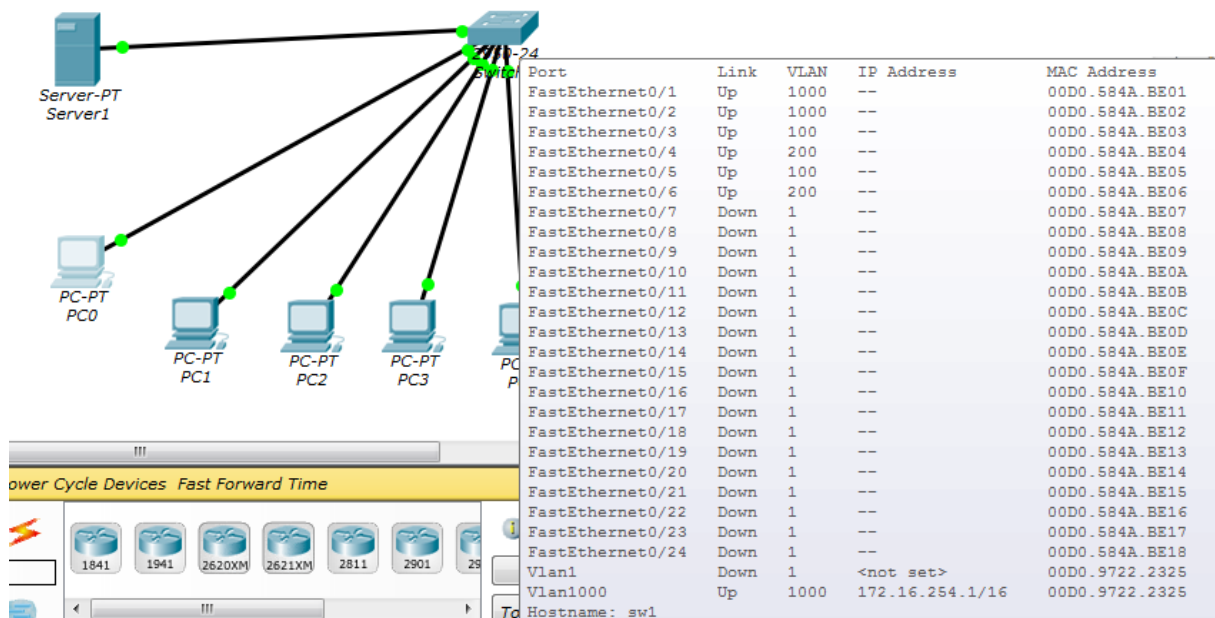
```
sw1#show mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
1000    0001.4289.0b58   DYNAMIC    Fa0/1
1000    0040.0b6c.0557   DYNAMIC    Fa0/2
sw1#
```

## 8. Ajout de machines

Bien sûr, l'objectif n'est pas « moi et mon switch », cela serait trop beau... Il faut ouvrir ce switch à des utilisateurs. Nous réalisons donc les configurations suivantes :

PC	Port	IP	VLAN
PC1	Fa0/3	172.17.0.1	100
PC2	Fa0/4	172.18.0.1	200
PC3	Fa0/5	172.17.0.2	100
PC4	Fa0/6	172.18.0.2	200

Vous obtenez donc :



Ensuite, comme vu dans le cours, il faut stopper complètement les ports inutilisés (personne ne pourra alors s'y connecter) et bien mettre les autres ports en mode switchport access afin d'éviter les problèmes liés à DTP et au VLAN hopping.

Mettre les ports de 3 à 24 en mode access :

```
sw1(config)#int range fastEthernet 0/3-24
sw1(config-if-range)#switchport mode access
sw1(config-if-range)#exit
```

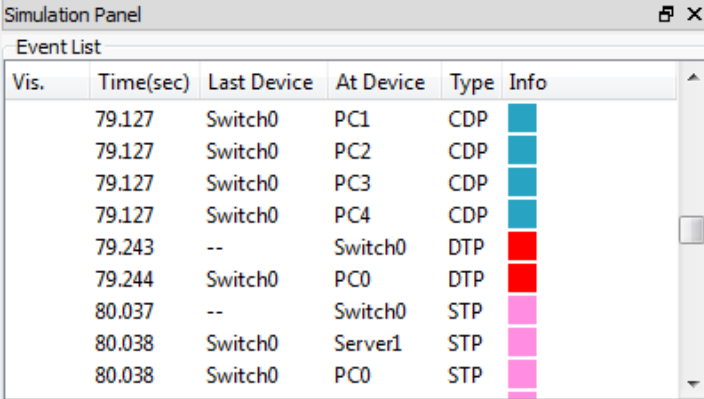
Arrêter les ports de 7 à 24 (en supposant qu'ils étaient up contrairement à la figure au-dessus) :

```
sw1(config)#int range fastEthernet 0/7-24
sw1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
```

## 9. Interconnexion

Basculez en mode « simulation » et lancez une capture « Auto capture / play ». Observez le résultat. Votre switch est plutôt bavard ! Vous devez observer de très nombreux paquets STP et de temps en temps, des paquets CDP et DTP. Notez bien que ces paquets arrivent aux PC en bout de chaîne alors que cela ne les concerne en aucun cas.



The screenshot shows a window titled "Simulation Panel" with a sub-window "Event List". The table below represents the data shown in the event list:

Vis.	Time(sec)	Last Device	At Device	Type	Info
	79.127	Switch0	PC1	CDP	
	79.127	Switch0	PC2	CDP	
	79.127	Switch0	PC3	CDP	
	79.127	Switch0	PC4	CDP	
	79.243	--	Switch0	DTP	
	79.244	Switch0	PC0	DTP	
	80.037	--	Switch0	STP	
	80.038	Switch0	Server1	STP	
	80.038	Switch0	PC0	STP	

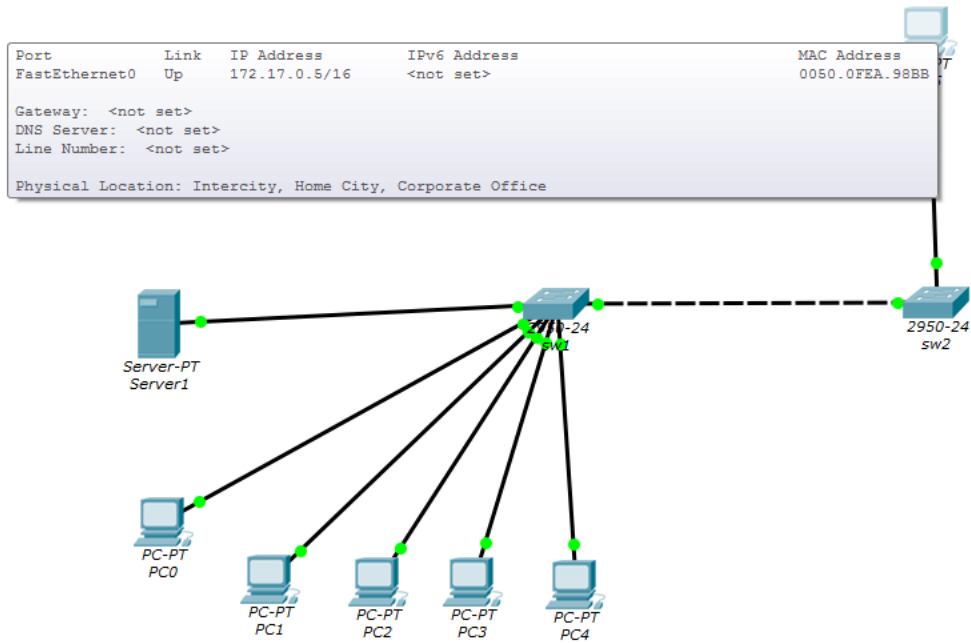
En tant qu'administrateur, il faudra faire des choix... Pas facile... Tout automatique et on est à la merci des machines... Tout manuel et on se tape des tâches fastidieuses et répétitives...

L'objet de cette partie est de mettre l'accent sur la configuration « usine » des appareils dont il faut se méfier. Nous voyons ici comment désactiver ces protocoles, dans la vraie vie, cela sera à l'administrateur de voir et juger, en pleine responsabilité...

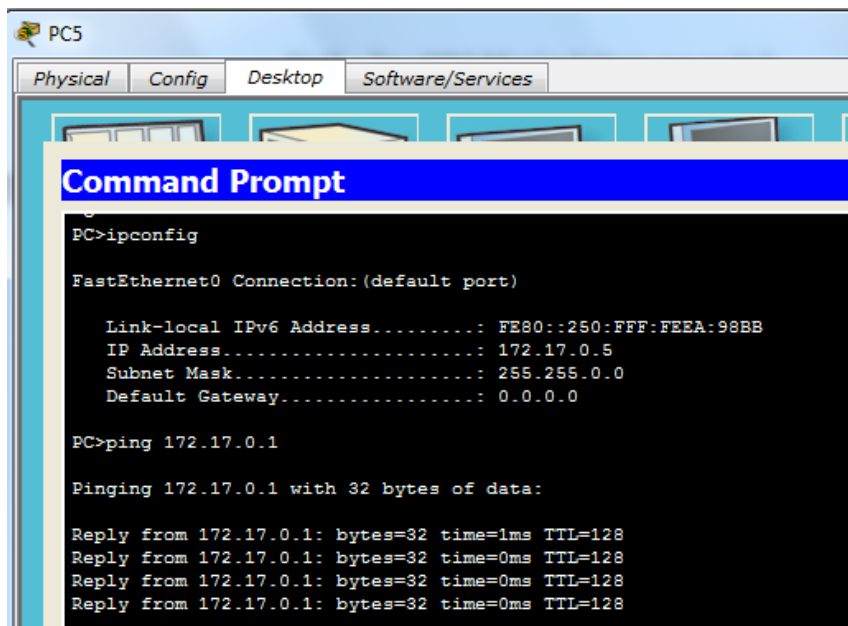
Supposons que nous soyons dans un bâtiment à deux étages et qu'un autre switch (sw2) soit mis en oeuvre dans un SR (Sous Répartiteur). Il faut le relier à sw1 et configurer l'interconnexion du port Fa0/24 de sw1 vers le port Fa0/24 de sw2 et configurer le mode trunk sur les deux switches. Nous supposons que seuls les VLAN 100, 200 et 1000 seront utilisés. Il n'est pas nécessaire de transmettre le VLAN1 natif sur le trunk. Vous utilisez VTP (sw1 en serveur et sw2 en client) pour propager les informations sur les VLAN uniquement sur le trunk.

Vous autorisez CDP uniquement sur le trunk. Et bien sûr, vous appliquerez les configurations de sécurité faites sur sw1 à sw2 !

Sur l'autre switch, des configurations symétriques devront être réalisées. Les VLAN 100, 200 et 1000 seront alors propagés de sw1 vers sw2. Ce qui permettra ensuite de finaliser la configuration.



Le poste PC5 connecté à sw2 doit pouvoir communiquer avec PC1 ou PC3.



Lorsque vous aurez fait les manipulations sur sw1, vous devriez obtenir quelque chose comme ceci :

**sw1#sh run**

Building configuration...

Current configuration : 2774 bytes

!

version 12.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

```

hostname sw1
!
enable secret 5 $1$mERr$yGPvrcRq4jgNmgP7jLRm.1
!
clock timezone gmt 1
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport access vlan 1000
switchport mode access
no cdp enable
!
interface FastEthernet0/2
switchport access vlan 1000
switchport mode access
no cdp enable
!
interface FastEthernet0/3
switchport access vlan 100
switchport mode access
no cdp enable
!
interface FastEthernet0/4
switchport access vlan 200
switchport mode access
no cdp enable
!
interface FastEthernet0/5
switchport access vlan 100
switchport mode access
no cdp enable
!
interface FastEthernet0/6
switchport access vlan 200
switchport mode access
no cdp enable
!
interface FastEthernet0/7
switchport mode access
no cdp enable
shutdown
!
[ coupure ..... ]
!
interface FastEthernet0/23
switchport mode access

```

```

no cdp enable
shutdown
!
interface FastEthernet0/24
switchport trunk allowed vlan 100,200,1000
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan1000
ip address 172.16.254.1 255.255.0.0
!
logging 172.16.100.100
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
end

```

Pour sw2 :

```

switchport access vlan 100
switchport mode access
!
interface FastEthernet0/2
!
sw2>enable
sw2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
sw2(config)#interface range fastEthernet 0/1
sw2(config-if)#switchport access vlan 100
sw2(config)#interface range fastEthernet 0/1-23
sw2(config-if-range)#switch mode access
sw2(config-if-range)#no cdp enable
sw2(config-if-range)#exit
sw2(config)# interface range fastEthernet 0/2-23
sw2(config-if-range)#shutdown
sw2(config-if-range)#exit
sw2(config)#exit
sw2#
%SYS-5-CONFIG_I: Configured from console by console

```



**sw2#sh run**

Building configuration...

Current configuration : 2186 bytes

```
!  
version 12.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname sw2  
!  
!  
spanning-tree mode pvst  
!  
interface FastEthernet0/1  
switchport access vlan 100  
switchport mode access  
no cdp enable  
!  
interface FastEthernet0/2  
switchport mode access  
no cdp enable  
shutdown  
!  
[ coupure ..... ]  
!  
interface FastEthernet0/23  
switchport mode access  
no cdp enable  
shutdown  
!  
interface FastEthernet0/24  
switchport trunk allowed vlan 100,200,1000  
switchport mode trunk  
!  
interface Vlan1  
no ip address  
shutdown  
!  
line con 0  
!  
line vty 0 4  
login  
line vty 5 15  
login  
!  
end
```

Concernant le protocole VTP, ceci n'est pas stocké dans le fichier de configuration. Pour configurer VTP, il faudra spécifier :

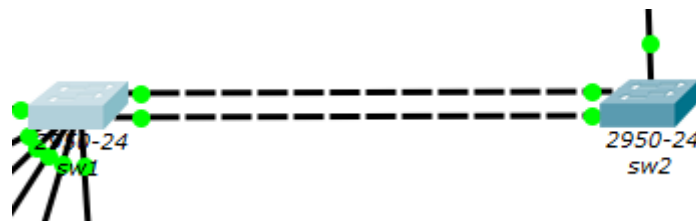
```
sw1(config)#vtp domain monreso
sw1(config)#vtp password !Cisco123!
sw1(config)#vtp mode server
```

Ce qui donnera :

```
sw1#show vtp status
VTP Version           : 2
Configuration Revision : 5
Maximum VLANs supported locally : 255
Number of existing VLANs : 8
VTP Operating Mode    : Server
VTP Domain Name       : monreso
VTP Pruning Mode      : Disabled
VTP V2 Mode           : Disabled
VTP Traps Generation  : Disabled
MDS digest            : 0xF3 0x6E 0xA0 0xE7 0x7B 0xDA 0x1F 0x1F
Configuration last modified by 172.16.254.1 at 3-1-93 00:02:38
Local updater ID is 172.16.254.1 on interface Vl1000 (lowest numbered VLAN
interface found)
```

## 10. Agrégation de liens

Pour des raisons de débits insuffisants, nous décidons de doubler le débit entre les deux switches. Pour ce faire, tirez un deuxième lien entre les ports Fa0/23 des deux switches :



Il nous faut créer un groupe de liens sur chaque interface :

```
sw1#conf t
sw1(confi g)#int fastEthernet 0/23
sw1(confi g-if)#channel-group 1 mode auto
sw1(confi g-if)#exit
sw1(confi g)#int fastEthernet 0/24
sw1(confi g-if)#channel-group 1 mode auto
sw1(confi g-if)#exit
```

Ensuite, il faut configurer le groupe de liens comme une interface normale de type trunk :

```
sw2(confi g)#int port-channel 1
sw2(confi g-if)#switchport trunk native vlan 666
sw2(confi g-if)#switchport trunk allowed vlan 100, 200, 1000
sw2(confi g-if)#switchport mode trunk
```

Enfin, pour valider le tout, un ping depuis le PC1 vers PC5 doit fonctionner.

On devrait avoir ces configurations suivantes pour sw2 et sw1 :

**sw2#sh run**

Building configuration...

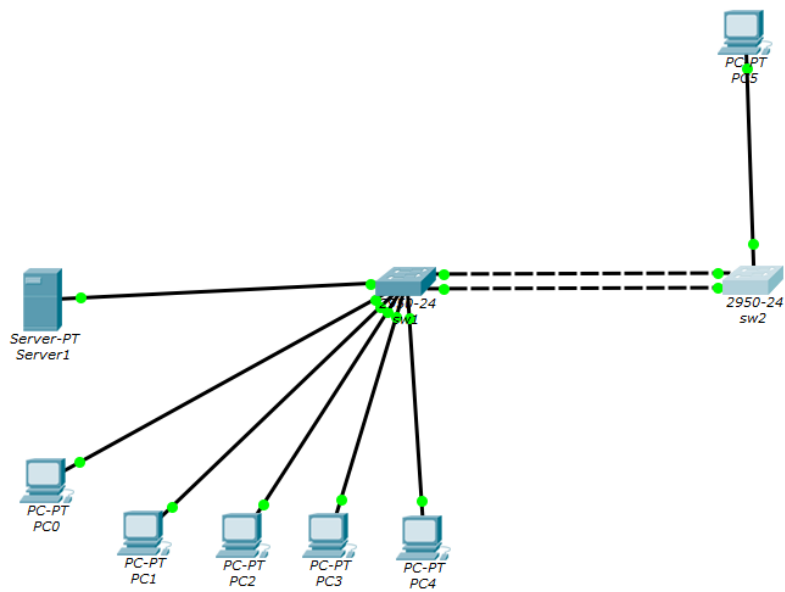
Current configuration : 2367 bytes

```
!  
version 12.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname sw2  
!  
spanning-tree mode pvst  
!  
interface FastEthernet0/1  
switchport access vlan 100  
switchport mode access  
no cdp enable  
!  
interface FastEthernet0/2  
switchport mode access  
no cdp enable  
shutdown  
!  
[ coupure ..... ]  
!  
interface FastEthernet0/22  
switchport mode access  
no cdp enable  
shutdown  
!  
interface FastEthernet0/23  
switchport trunk allowed vlan 100,200,1000  
channel-group 1 mode auto  
switchport mode trunk  
no cdp enable  
!  
interface FastEthernet0/24  
switchport trunk allowed vlan 100,200,1000  
channel-group 1 mode auto  
switchport mode trunk  
!  
interface Port-channel 1  
switchport trunk allowed vlan 100,200,1000  
switchport mode trunk  
!  
interface Vlan1  
no ip address
```

```

shutdown
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
end

```



```

sw1#sh run
Building configuration...

Current configuration : 2955 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname sw1
!
enable secret 5 $1$mERr$yGPvrcRq4jgNmgP7jLRm.1
!
clock timezone gmt 1
!
no ip domain-lookup
!
!
spanning-tree mode pvst

```

```

!
interface FastEthernet0/1
switchport access vlan 1000
switchport mode access
no cdp enable
!
interface FastEthernet0/2
switchport access vlan 1000
switchport mode access
no cdp enable
!
interface FastEthernet0/3
switchport access vlan 100
switchport mode access
no cdp enable
!
interface FastEthernet0/4
switchport access vlan 200
switchport mode access
no cdp enable
!
interface FastEthernet0/5
switchport access vlan 100
switchport mode access
no cdp enable
!
interface FastEthernet0/6
switchport access vlan 200
switchport mode access
no cdp enable
!
interface FastEthernet0/7
switchport mode access
no cdp enable
shutdown
!
[ coupure ..... ]
!
interface FastEthernet0/22
switchport mode access
no cdp enable
shutdown
!
interface FastEthernet0/23
switchport trunk allowed vlan 100,200,1000
channel-group 1 mode auto
switchport mode trunk
no cdp enable
!
interface FastEthernet0/24

```

```

switchport trunk allowed vlan 100,200,1000
channel-group 1 mode auto
switchport mode trunk
!
interface Port-channel 1
switchport trunk allowed vlan 100,200,1000
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan1000
ip address 172.16.254.1 255.255.0.0
!
logging 172.16.100.100
!
line con 0
login
!
line vty 0 4
login
line vty 5 15
login
!
end

```

## 11. Désactivation des protocoles inutiles (facultatif)

Finalement, aucun protocole n'est à désactiver. STP est utile pour l'agrégation de liens. CDP, VTP et DTP ont été cantonnés au trunk, donc aucun élément extérieur ne peut intervenir (si le trunk ne peut être physiquement compromis bien sûr).

Sur certains switches, un serveur HTTP est actif pour proposer une interface de configuration en mode web. Il est préférable de le désactiver avec un `no ip http server` (sinon attention à la sécurisation de l'authentification : quel mot de passe ? Https?).

Si SNMP n'est pas utilisé, il faut également le désactiver :

```

Switch(config)# no snmp-server community
Switch(config)# no snmp-server enable traps
Switch(config)# no snmp-server system-shutdown
Switch(config)# no snmp-server

```

## 12. Activer Radius pour les connexions Wi-Fi

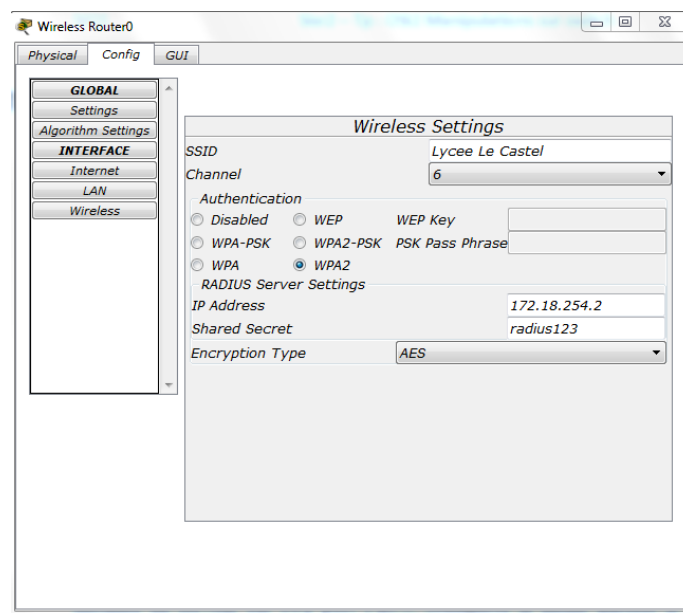
Nous décidons qu'un point d'accès Wi-Fi sera relié à sw2 permettant ainsi la connexion d'un ordinateur portable. Les machines associées à ce point d'accès seront affectées au VLAN 200. Un serveur AAA (Authentication Authorization Accounting) sera également installé sur ce VLAN 200 afin d'autoriser (ou non) les machines à se connecter.

Installez un point d'accès (borne) Wi-Fi Linksys-WRT300N.

Connectez son port LAN (Ethernet 1) sur le port Fa0/2 de sw2, puis affectez-lui une adresse IP en 172.18.x.x. (172.18.254.1 par exemple).

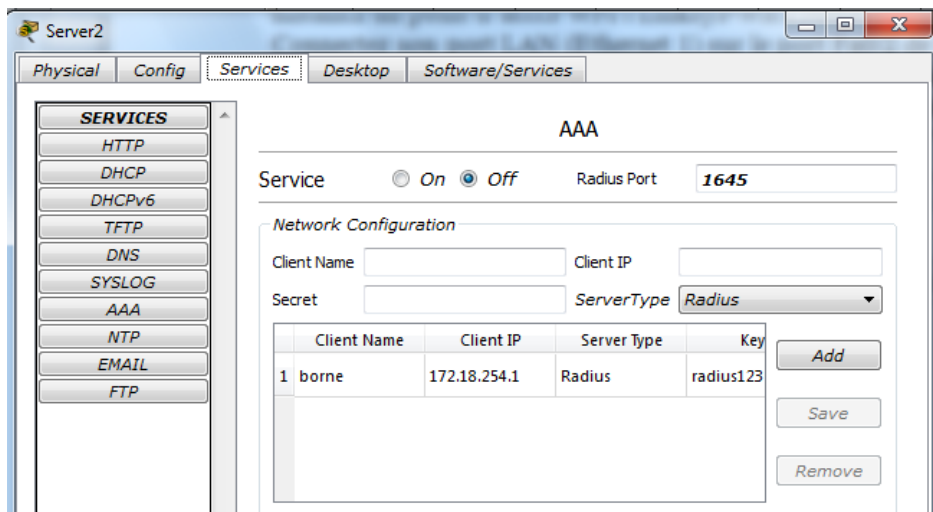
Configurez le VLAN 200 sur cette interface du switch.

Dans l'onglet « Wireless », donnez un SSID puis les références du serveur Radius installé après :

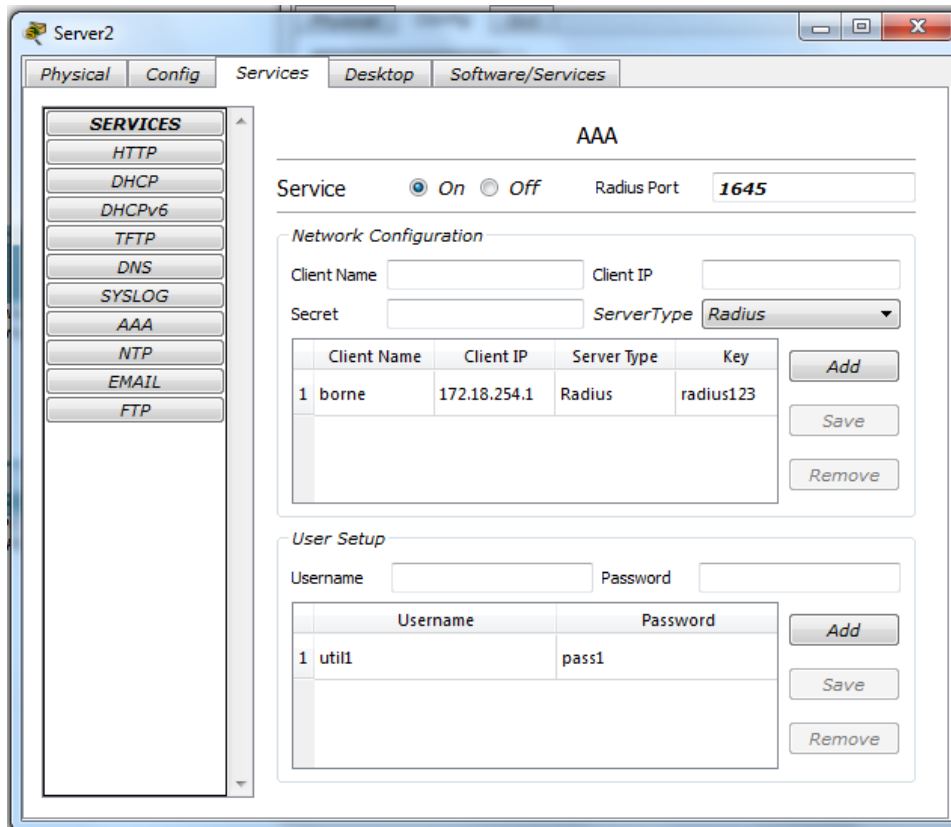


Installez un serveur sur sw2 port Fa0/3, configurez la même adresse IP que celle indiquée dans Wireless (figure ci-dessus), configurez le VLAN 200 sur cette interface du switch.

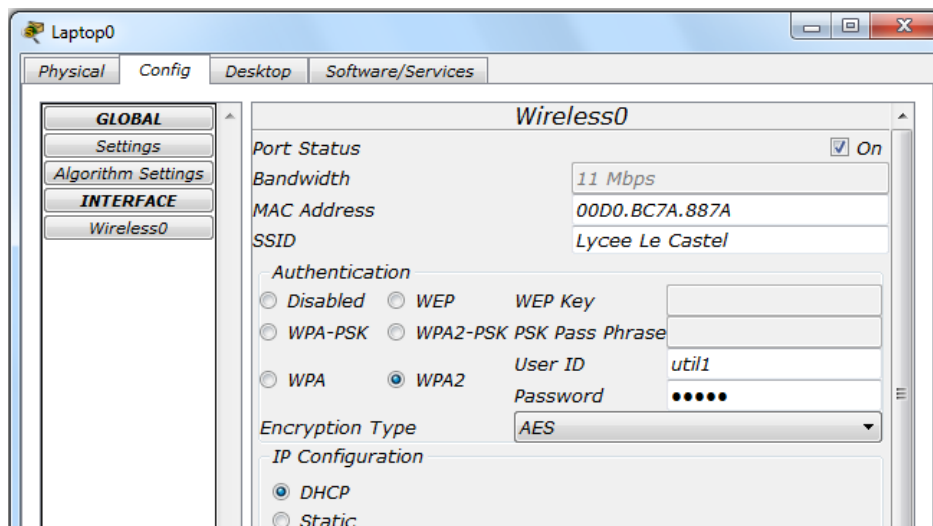
Allez dans l'onglet « Config/Services/AAA ». Mettez l'adresse IP de la borne et la zone Secret (le nom n'est pas obligatoire) :



Créez un utilisateur avec un mot de passe :

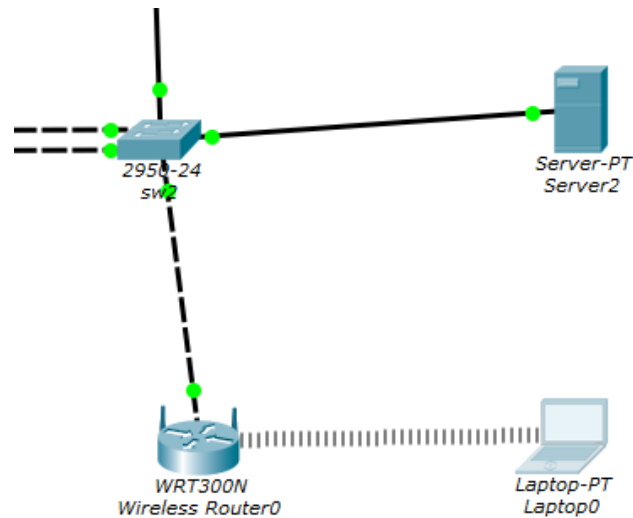


Prenez un portable, remplacez la carte filaire par une carte sans-fil PT-LAPTOP-NM-1W. Configurez le SSID de la borne, mettez WPA2 avec le nom d'utilisateur et le mot de passe saisis dans le serveur AAA. Laissez DHCP, la borne attribuera une adresse :





Le portable doit pouvoir s'associer à la borne :



Un ping lancé depuis le portable vers une machine du VLAN 200 doit fonctionner. Vous pouvez passer en mode simulation et redémarrer le portable pour voir ce qu'il se passe et comment se mettent en place les échanges RADIUS.

