

Premiers pas chez Cisco

1 Exercice

Le but de ce TP est de se familiariser avec un matériel de réseau en utilisant quelques commandes de configuration basiques. La sécurité du matériel et du réseau n'est pas abordée dans ce TP.

Vous venez d'acquérir un switch Cisco, vous allez le découvrir et effectuer la première configuration en ligne de commande (CLI).

Déroulement du TP :

- Découverte du matériel
- Connectique et configuration du terminal windows
- Découverte de la console
- Donner un nom au matériel
- Affecter une adresse IP d'administration au matériel
- Configurer la route par défaut
- Sauvegarder la configuration
- Mettre le matériel à l'heure
- Comprendre les mots de passe
- Chiffrer les mots de passe
- Découvrir le serveur HTTP
 - Désactiver une interface, visualiser des statistiques
- Télécharger une configuration à partir d'un serveur TFTP
- Reboot du matériel

Le TP s'arrêtera à ce stade, il resterait à faire :

- Sécuriser les accès VTY, HTTP et SNMP
- Mettre en place un serveur de log et loguer le matériel
- Configurer des VLANs
- Mettre en place des listes de contrôles,
- Mettre en place des listes de MAC adresses autorisées
- ...

2 Le matériel

- 2 Catalyst 2940, 8 ports 10/100 cuivre, 1 port 1000 cuivre
- 1 Catalyst 2950, 24 ports 10/100 cuivre
- 1 Routeur 1700, 2 ports 10 cuivre, 1 port 100 cuivre

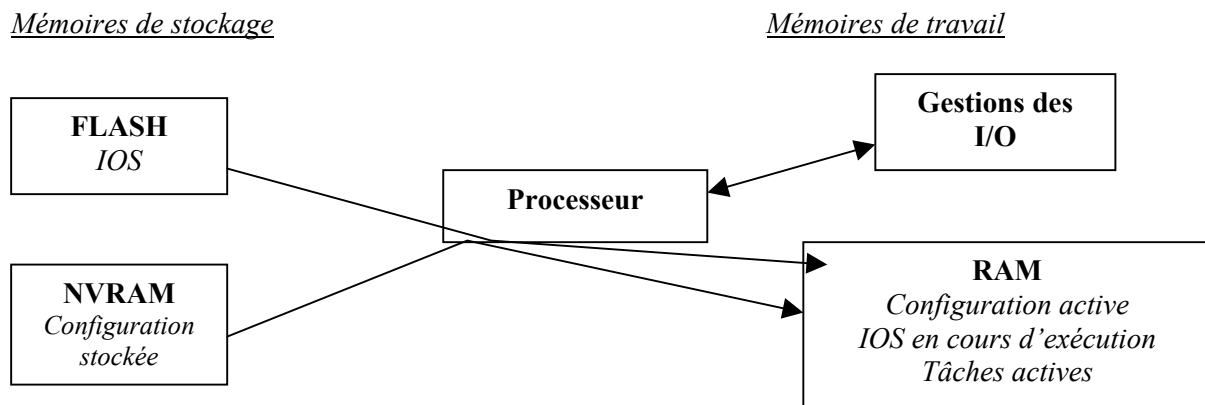
3 Le système d'exploitation Cisco

- Les routeurs, switchs et catalysts Cisco sont classés par gamme comprenant chacune plusieurs modèles.
- L'IOS, le système d'exploitation de Cisco, est le même sur l'ensemble des matériels.
- L'IOS se décline selon plusieurs gamme appelées packages dont les fonctionnalités varient en fonction des capacités du matériel. Les quatre principaux packages :
 - IP Routing
 - IP/IPX Routing and IBM
 - Desktop and IBM
 - Enterprise
- Les routeurs travaillent aux niveaux 1,2 et 3 du modèle OSI

- Les switches : 1 et 2
- Les catalysts sont des switches de niveau 2 ayant des fonctions de routage du niveau 3 plus ou moins réduites selon les gammes.
- Modèle OSI :
 7. Application
 6. Présentation
 5. Session
 4. Transport
 3. Réseau
 2. Protocole
 1. Physique

4 Architecture matérielle

Schéma 1 :



5 Configuration système

- La première configuration du système s'effectue via une console en ligne de commande, CLI (Command Line Interface).
- Lorsque le matériel possède une adresse IP, il est possible de modifier sa configuration
 - en ligne de commande (CLI) via la console ou par connexion à distance via les protocoles telnet ou SSH,
 - par le réseau via le protocole TFTP
 - par l'interface web CMS (Cluster Management Suite)
 - ou par SNMP au travers d'une plate-forme de supervision de réseau SNMP

5.1 Utilisation d'une console

5.1.1 Utilisation d'un terminal Windows

- Ouvrir un terminal :
Menu **Démarrer-Accessoires-Communications-HyperTerminal**
 - Donnez un nom au terminal, choisir une icône : Cisco
 - Sélectionner le port de communication : **COM1**
- Configurer le port :
Bits par seconde : **9600**
Bits de données : **8**
Parité : **Aucun**
Bit d'arrêt : **1**
Contrôle de flux : **Matériel**

- Activer la console côté matériel Cisco :
Tapez sur la touche **Entrée**
Vous entrez en mode CLI sur le matériel Cisco, vous devez obtenir le prompt :

Switch>

5.2 Commandes de visualisation

- Affichage des paramètres hardware et software :

Switch> show version

Cisco Internetwork Operating System Software
IOS (tm) C2940 Software (C2940-I6Q4L2-M), Version 12.1(13)AY, RELEASE SOFTWARE (fc3)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Thu 26-Jun-03 18:33 by antonino
Image text-base: 0x80010000, data-base: 0x805BA000

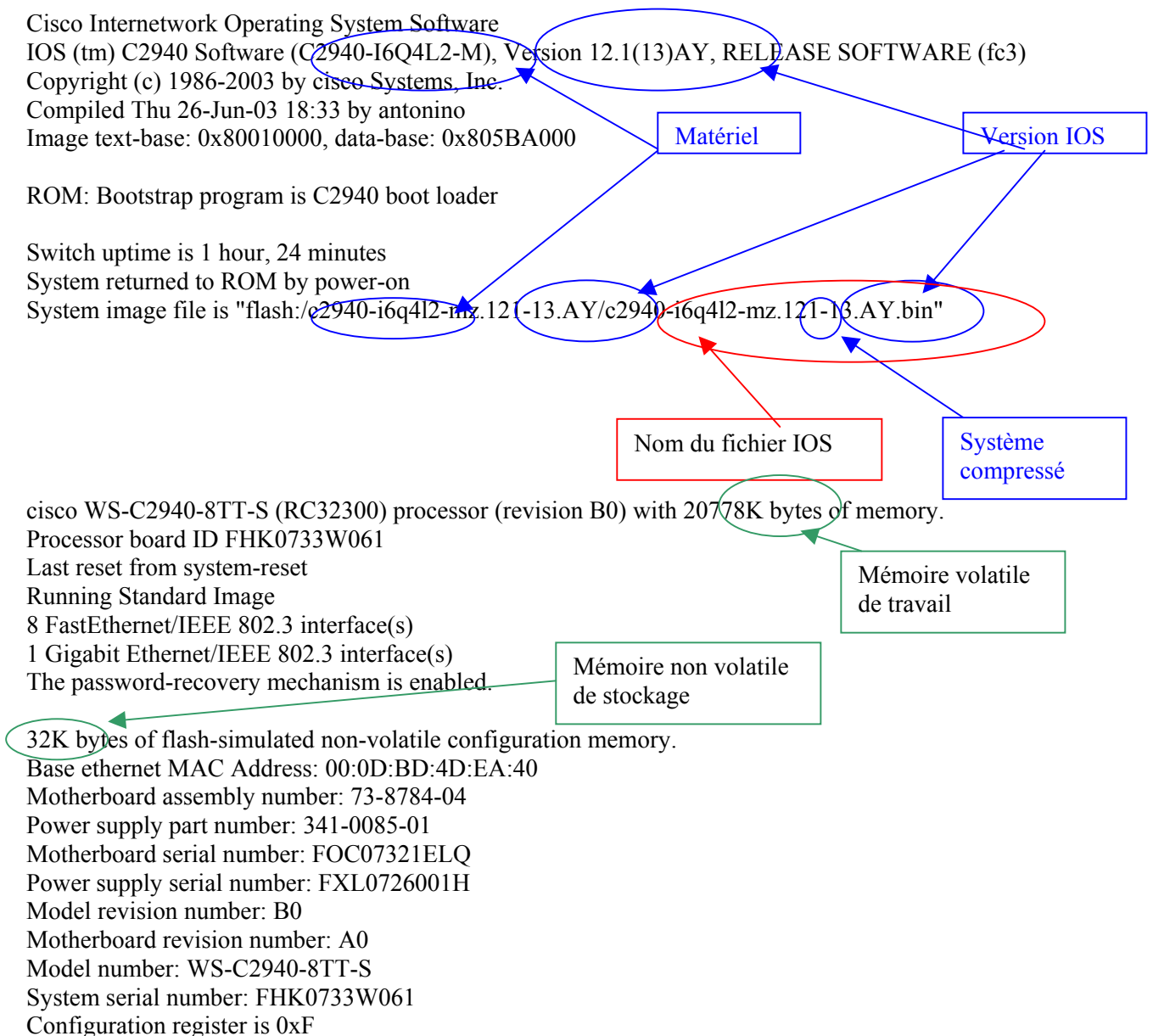
ROM: Bootstrap program is C2940 boot loader

Switch uptime is 1 hour, 24 minutes
System returned to ROM by power-on
System image file is "flash:c2940-i6q4l2-mz.121-13.AY/c2940-i6q4l2-mz.121-13.AY.bin"

cisco WS-C2940-8TT-S (RC32300) processor (revision B0) with 20778K bytes of memory.
Processor board ID FHK0733W061
Last reset from system-reset
Running Standard Image
8 FastEthernet/IEEE 802.3 interface(s)
1 Gigabit Ethernet/IEEE 802.3 interface(s)
The password-recovery mechanism is enabled.

32K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address: 00:0D:BD:4D:EA:40
Motherboard assembly number: 73-8784-04
Power supply part number: 341-0085-01
Motherboard serial number: FOC07321ELQ
Power supply serial number: FXL0726001H
Model revision number: B0
Motherboard revision number: A0
Model number: WS-C2940-8TT-S
System serial number: FHK0733W061
Configuration register is 0xF



- Afficher les commandes disponibles :

Switch> ?

5.3 Le mode privilege

C'est le mode super utilisateur, il permet d'accéder aux commandes de configuration et d'administration du système.

Mdp : otot04

- Passer en mode privilège :

Switch> enable

Password:

Switch#

- Afficher les commandes disponibles :

Switch> ?

- Sortir du mode privilège :

Switch# disable

Switch>

5.4 Commandes de configuration

Il y a trois types de commandes :

- Les **commandes globales** : Elles affectent une fonction générale pour tout le switch ou routeur.
- Les **commandes majeures** : Elles indiquent une tâche ou une interface particulière que l'on va configurer, elles doivent être suivies d'au moins une sous-commandes.
- Les **sous-commandes** : Elles sont utilisées après une commandes majeure et permettent de configurer une tâche ou une interface.

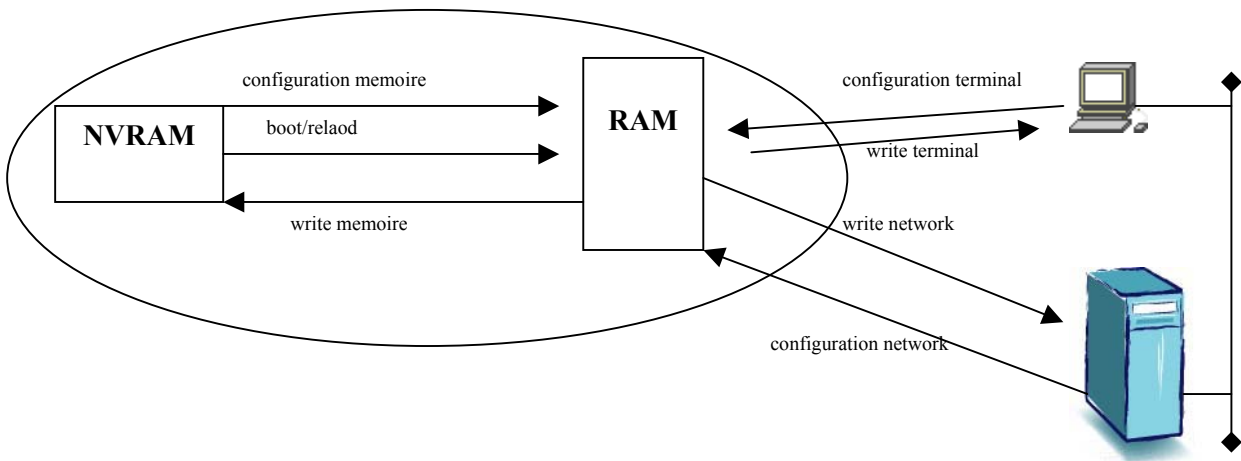
Il y a toujours deux configurations :

- Une **configuration stockée** en mémoire non-volatile NVRAM (sauvegardée)
- Une **configuration active** utilisée par l'IOS lors de son exécution en mémoire volatile RAM (non sauvegardée)

Lorsque le matériel est démarré ou ré-initialisé, la configuration stockée dans le mémoire non-volatile NVRAM est copiée comme configuration active dans la mémoire volatile RAM.

Attention Toutes les commandes de configuration soumises sont immédiatement prises en compte. Ceci, car nous travaillons dans la RAM.

Schéma 2 :



- Afficher la configuration active :

```
Switch# write terminal
```

- Afficher la configuration stockée :

```
Switch# show configuration
```

```
Using 919 out of 32768 bytes
```

```
!
```

```
version 12.1
```

```
no service pad
```

```
service timestamps debug uptime
```

```
service timestamps log datetime
```

```
no service password-encryption
```

```
!
```

```
hostname Switch
```

```
!
```

```
enable secret 5 $1$QBdh$HjEPJ5O1EOxQF.mCzXzxH0
```

```
enable password otot05
```

```
!
```

```
ip subnet-zero
```

```
!
```

```
!
```

```
spanning-tree mode pvst
```

```
no spanning-tree optimize bpdu transmission
```

```
spanning-tree extend system-id
```

```
!
```

```
!
```

```
interface FastEthernet0/1
```

```
no ip address
```

```
!
```

```
interface FastEthernet0/2
```

```
no ip address
```

```
!
```

```
././ Configuration tronquée
```

```
!
```

```
interface GigabitEthernet0/1
```

```

no ip address
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
ip http server
!
!
line con 0
exec-timeout 0 0
line vty 0 4
password otot04
login
line vty 5 15
password otot04
login
!
end

```

Pour les switches, par défaut toutes les interfaces sont dans le vlan 1, ils ne supportent que UNE @ IP sur un vlan.

Pour les routeurs, ils sont de niveau 3, il faut affecter une @ IP et le réseau accessible par interface. Les catalyts, de niveau 2 et 3, acceptent des vlans et des @ IP sur chaque interfaces.

- Configurer via la console :

```

Switch# configure terminal
Switch(config)#
Switch(config)# exit
Switch#

```

- Messages de la console :

Vous êtes en mode console, donc les messages de la console s'affichent au milieu du texte que vous frappez ☺

Ils sont de la forme :

```
hh:mm:ss: %TYPE DU MESSAGE: message
```

- Changer le nom du matériel :

```
Switch(config)# hostname sugiton
```

- Affecter une adresse IP d'administration au matériel :

Pour les switches :

Cette adresse IP sera utiliser pour administrer à distance le matériel. On utilise le vlan1 à cet effet. Le vlan1 est un vlan standard créé par défaut à cet effet. Les switches n'acceptent qu'un VLAN avec une adresse IP.

```
sugiton(config)# interface vlan 1
```

```
sugiton(config-if)# ip address 10.0.0.2 255.0.0.0
```

Pour le routeur :

L'on doit configurer une @ IP et un réseau accessible par interface. Pour le TP, l'on va configurer l'interface FastEthernet 0 avec l'@ 10.0.0.2 derrière laquelle il y aura le réseau 10.0.0.0

```
sugiton(config)# interface fastethernet 0
```

```
sugiton(config-if)# ip address 10.0.0.2 255.0.0.0
```

- Activer le VLAN :

```
sugiton(config-if)# no shutdown
```

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

```
sugiton(config)#
```

- Configurer la route par défaut :

```
sugiton(config)# ip default-gateway 10.0.0.1
```

- Configurer le serveur DNS :

```
sugiton(config)# ip name-server 10.0.0.10
```

```
sugiton(config)# exit
```

- Afficher la configuration active :

```
sugiton# write terminal
```

- Afficher la configuration sauvegardée :

```
sugiton# show configuration
```

- Sauvegarder en NVRAM la configuration active :

```
sugiton# copy system:running-config nvram:startup-config  
ou
```

```
sugiton# write memory
```

- Sauvegarder sur un serveur TFTP la configuration active :

```
sugiton# copy system:running-config tftp://10.0.0.3/Config-X  
ou
```

```
sugiton# write network
```

- Afficher l'heure :

```
Sugiton> show clock
```

```
*00:15:52.531 UTC Mon Mar 1 1993
```

L'étoile signifie que l'heure n'a pas été configurée ou est fausse

- Mettre le matériel à l'heure :

Par défaut la timezone utilisée est UTC (GMT=UTC). L'on peut, **simplement pour l'affichage**, modifier la timezone du matériel.

Nous sommes, en hiver : dans la timezone CET = UTC + 1 ;
en été : dans la timezone CEST = UTC + 2

Par directive du parlement Européen,

<http://www.industrie.gouv.fr/energie/developp/econo/pdf/directive-heurete.pdf> à compter de 2002 et pour 5 ans :

Art 2 : À compter de l'année 2002, la période de l'heure d'été commence, dans chaque État membre, à 1 heure du matin, temps universel, le dernier dimanche de mars.

Art 3 : À compter de l'année 2002, la période de l'heure d'été se termine, dans chaque État membre, à 1 heure du matin, temps universel, le dernier dimanche d'octobre.

```
sugiton(config)# clock timezone CET +1
```

```
sugiton(config)# clock summer-time CEST recurring last Sunday March 02:00
last Sunday October 03:00
```

```
sugiton(config)# exit
```

```
sugiton# clock set 22:38:00 29 December 2004
```

```
Sugiton# show clock
```

```
22:38:01.483 CET Thu Dec 30 2004
```

```
sugiton# show clock detail
```

```
22:52:14.231 CET Thu Dec 30 2004
```

```
Time source is user configuration
```

```
Summer time starts 02:00:00 CET Sun Mar 27 2005
```

```
Summer time ends 03:00:00 CEST Sun Oct 30 2005
```

- Comprendre les mots de passe :

Le mot de passe n'est pas la sécurité absolue mais une étape dans la sécurité. Ne jamais laisser un équipement réseau sans mot de passe ou avec un mot de passe constructeur.

Sur les routeurs et switches Cisco, il est possible d'utiliser un mot de passe sur les terminaux virtuels (VTY) c-a-d les connexions à distances, la console, le mode privilège, les comptes utilisateurs, les auxiliaires...

Si l'équipement est dans une pièce sécurisée, il n'est pas recommandé de mettre un mot de passe pour la console. Par contre, il est **impératif** de mettre un mot de passe pour le mode privilège et les connexions à distance.

- Mot de passe du mode privilège :

Il existe deux commandes pour configurer le mot de passe du mode privilège :

enable password et **enable secret**, ces deux commandes ont le même effet mais la commande enable password est obsolète et dangereuse.

La plupart des nouveaux matériels fonctionnent avec enable secret. enable secret chiffre le mot de passe du mode privilège avec l'algorithme MD5.

- Supprimer le enable password :

```
sugiton(config)# no enable password
```

- Changer ou créer le enable secret :

!! Attention, ne pas faire !!

```
sugiton(config)# enable secret mot-de-passe
```

- Mot de passe des terminaux virtuels :

Il est **impératif** de mettre un mot de passe pour les connexions à distance qui sont représentées par les **line vty**

Visualisez la configuration active pour repérer les line vty auxquelles vous appliquerez un mot de passe.

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

```
sugiton(config-line)# password esil
```

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

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

```
sugiton(config)# exit
```

```
sugiton#
```

- Chiffrer les mots de passe :

Les mots de passe apparaissent en clair lorsque l'on visualise la configuration du matériel. Il est possible de les chiffrer.

```
sugiton(config)# service password-encryption
```

- Sauvegarder en NVRAM la configuration active :
- Sauvegarder sur un serveur TFTP la configuration active :
- Utiliser le serveur HTTP :

- Configurer succinctement la carte réseau de votre PC :

```
@IP : 10.0.0.3
```

```
masque : 255.0.0.0
```

```
gateway : 10.0.0.1
```

- Ouvrir un navigateur et aller à l'adresses : 10.0.0.2
- Saisir le mot de passe enable 2 fois
- Cluster Management Suite-> désactiver les ports, visualiser des statistiques

- Charger une configuration en NVRAM à partir d'un serveur TFTP :

```
sugiton# copy tftp://10.0.0.3/switch-config nvram:startup-config
```

- Réinitialisation du matériel :

Switch# reload

Proceed with reload? [confirm]

04:12:43: %SYS-5-RELOAD: Reload requested

/../

Press RETURN to get started!