Collection Formation Réseau Cisco CCNA

LAN SWITCHING

Prise en main d'un commutateur Cisco©

François-Emmanuel Goffinet
Formateur IT
Version 16.01

Objectifs ICND1

2. Technologies de commutation LAN

2.3. Configurer et vérifier la configuration initiale du commutateur, y compris la gestion de l'accès à distance.

- 2.3.a hostname
- 2.3.b mgmt ip address
- 2.3.c Ip default-gateway
- 2.3.d local user and password
- 2.3.e enable secret password
- 2.3.f console and VTY logins
- 2.3.g exec-timeout
- 2.3.h service password encryption
- 2.3.i copy run start

2.4. Vérifier l'état du réseau et le fonctionnement du commutateur en utilisant les outils de base telles que ping, telnet et ssh.

Objectifs ICND1

6. Sécurité des périphériques du réseau

6.1. Configurer et vérifier les caractéristiques de sécurité des périphériques réseau tels que :

- 6.1.a. Sécurité par mot de passe du périphérique
- 6.1.b. Enable secret vs enable
- 6.1.c. Transport : désactiver telnet, SSH
- 6.1.d. Lignes VTYs
- 6.1.e. La sécurité physique
- 6.1.f. mot de passe de service
- *6.1.g. Décrire les méthodes externes d'authentification*

Objectifs ICND1

6. Sécurité des périphériques du réseau

6.2. Configurer et vérifier dans un commutateur les fonctions de sécurité sur les ports telles que

- 6.2.a. Sticky MAC
- 6.2.b. Limitation d'adresse MAC
- 6.2.c. Static / dynamic
- 6.2.d. Violation modes : Err disable, Shutdown, Protect restrict
- 6.2.e. Shutdown unused ports
- 6.2.f. Err disable recovery
- *6.2.g. Assigner les ports inutilisés à un VLAN inutilisé*
- *6.2.h. Placer le VLAN natif dans un autre que le VLAN par défaut*

Opérations

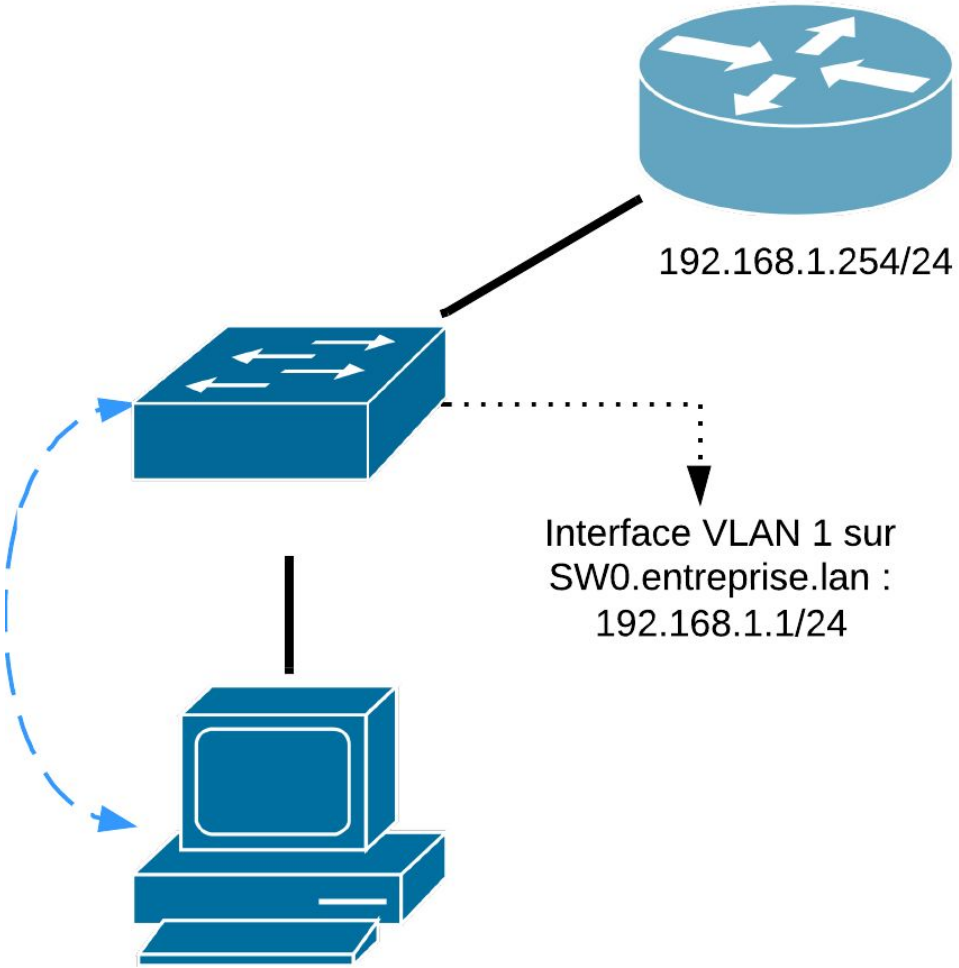
Pour un commutateur Cisco :

- Configuration globale
- Configuration de l'interface de gestion
- Activation de la console distante SSH
- Sécurisation de base
- Sécurisation des ports
- Diagnostic de base

Scénario

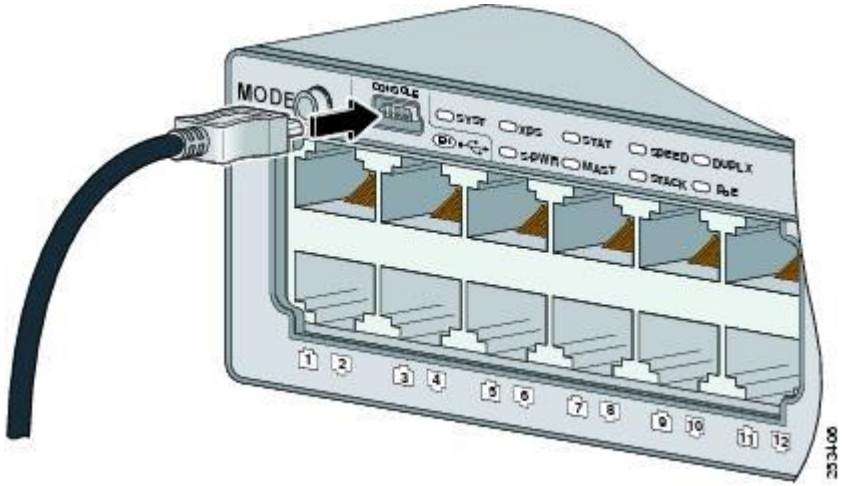
- Un commutateur connecte une ou deux stations de travail dans un LAN (192.168.1.0 /24).
- On suppose l'existence d'une passerelle dont on ne soucie pas.
- La configuration est réalisée via la console physique.
- **A des fins de gestion seulement**, une adresse IP est fixée sur le commutateur.

Topologie


192.168.1.254/24
Interface VLAN 1 sur
SW0.entreprise.lan :
192.168.1.1/24

Connexion à la console physique

- Câble inversé (roll-over) COM1/RJ ou du port USB du PC au commutateur sur le port console.
- Lancer un logiciel d'émulation de terminal (putty/hyperterminal) 9600 bauds



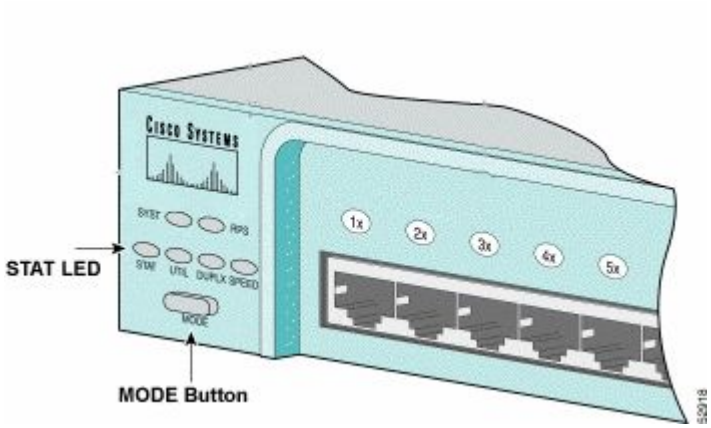
Démarrage d'un commutateur

```
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of
memory.
2960-24TT starting...
Base ethernet MAC Address: 0009.7C8D.80C5
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
############################################################################
[OK]
```

Password Recovery

On peut reprendre la main sur un commutateur déjà configuré en interrompant son démarrage et en renommant le fichier de configuration initiale.
La procédure est bien documentée : http://www.cisco.com/c/en/us/support/docs/switches/catalyst-2950-series-switches/12040-pswdrec-2900xl.html



Navigation CLI

Passage en mode privilège

```
>enable
#
```

Passage en mode de configuration globale

```
#configure terminal
(config)#
```

Configuration d'une interface

```
(config)#interface FastEthernet 0/1
(config-if)#
```

Passage aux modes inférieurs

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

Aide au CLI

- Une aide est accessible via le point d'interrogation.
- Les commandes s'auto-complètent avec la touche de tabulation.
- L'environnement indique l'endroit d'une erreur.
- Les commandes s'abrègent si il n'y pas d'ambiguïté.
- En cas d'ambiguïté, l'environnement propose les choix.
- Par défaut les logs apparaissent dans la console, pas en terminal distant.
- raccourcis clavier : on peut faire défiler l'historique des commandes avec les flèches du haut et du bas, on peut revenir au mode privilège directement (CTRL-Z), etc.
- La commande do permet d'exécuter une commande du mode privilège dans un autre mode.

Navigation CLI

Toutes les commandes d'administration s' exécutent en mode privilège :

Commande IOS	Signification
`#show running-config`	Visualise la configuration courante (RAM)
`#show flash:`	Visualise le contenu de la mémoire Flash
`#show ip interface brief`	Visualise l'état des interfaces (IPv4)
`#show vlan`	Visualise la DB des VLANs
`#copy running-config startup-config`	Enregistre la configuration courante
`#write memory`	Enregistre la configuration courante

Configuration globale

Accès au mode de configuration globale	>**en** #**configure terminal** (config)#
Nom d'hôte	**hostname *SW0***
Nom du domaine	**ip domain-name entreprise.lan**
Accès au mode privilège	**enable secret *cisco***

Configuration du service SSH (1/2)

Création d'un compte d' administration	**username *admin* secret *cisco***
Création d'une clé RSA de 1024 bits	**crypto key generate rsa** *The name for the keys will be: SW0. entreprise.lan* *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]*

Configuration du service SSH (2/2)

Activation SSHv2	`(config)#`**`ip ssh version 2`**
Configuration des lignes virtuelles et activation de SSH	`(config)#`**`line vty 0 15`** `(config-line)#`
Authentification dans la base de données locale	**`login local`**
Activation de SSH comme console TCP/IP	**`transport input ssh`**
Sortir de la configuration des lignes virtuelles	`(config)line#`**`exit`** `(config)#`

Configuration statique de l'interface de gestion

L'interface de gestion du commutateur est attribuée au VLAN 1 par défaut	`(config)#`**`interface vlan`** ***`1`*** `(config-if)#`
Configuration de l'adresse IP	**`ip address`** ***`192.168.1.1`*** ***`255.255.255.0`***
On prend garde de monter l' interface	**`no shutdown`**
Sortir de la configuration d' interface VLAN 1	`(config-if)#`**`exit`** `(config)#`
Configuration de la passerelle soit l'adresse IP de l'interface du routeur qui est dans le VLAN 30.	**`ip default-gateway`** ***`192.168.1.254`***
Configuration d'un serveur de nom (à condition d'en disposer en laboratoire)	**`ip name-server`** ***`8.8.8.8`***

Enregistrement et vérification

Enregistrement de la configuration courante

```
(config)# ^Z
#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]? ↵
Building configuration...
[OK]
#
```

Vérification de la Configuration courante

```
#show running-config
...
```

Faiblesse des mots de passe

La plupart des mots de passe sont visibles dans le fichier de configuration :

```
no service password-encryption
!
hostname SW1
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
username admin privilege 1 password 0 cisco
```

Chiffrement automatique des mots de passe

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

activera le chiffrement type 7 sur les mots de passe. Dans le fichier de configuration :

```
service password-encryption
hostname SW1
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
username admin privilege 1 password 7 0822455D0A16
```

On préférera toujours le paramètre "secret" au lieu de password fournissant un chiffrement de type 5 (MD5) :

```
(config)#username admin secret cisco
```

Déchiffrement type 7

- http://www.ibeast.com/content/tools/CiscoPassword/

Configuration des messages d'accueil

```
(config)#banner motd #Message#
(config)#banner login #Message#
```

Configurer une plage d'interfaces

```
(config)#interface range f0/1-24
(config-if-range)#duplex auto
(config-if-range)#speed auto
(config-if-range)#mdix auto
(config-if-range)#switchport mode access
(config-if-range)#switchport access vlan 1
(config-if-range)#spanning-tree portfast
(config-if-range)#exit
```

Diagnostic sur un commutateur

Table de commutation :

```
#show mac-address-table
```

Interfaces :

```
#show interface f0/1
```

Interface de gestion VLAN 1 :

```
#show vlan
#show interface vlan 1
#show ip interface vlan 1
```

Passerelle de l'interface de gestion :

```
#show ip route
```

Sécurité sur les ports

```
(config)#interface f0/1
(config-if)#switchport mode access
(config-if)#switchport port-security
```

Cette fonction permet de contrôler les adresses MAC autorisées sur un port. En cas de violation, une action est prise. Par défaut,

- Cette fonction est désactivée
- Une seule adresse MAC apprise dynamiquement
- En cas de violation, le port tombe en mode shutdown

Définition des adresses MAC autorisées

On peut fixer le nombre d'adresses MAC autorisées :

```
(config-if)#switchport port-security maximum 10
```

Les adresses MAC apprises peuvent être inscrites dynamiquement dans la configuration :

```
(config-if)#switchport port-security mac-address sticky
```

Les adresses MAC autorisées peuvent être fixées :

```
(config-if)#switchport port-security mac-address 0000.0000.0003
```

Mode de violation

```
(config-if)#switchport port-security
violation {protect | restrict | shutdown}
```

- **Mode protect :** dès que la violation est constatée, le port arrête de transférer le trafic des adresses non autorisées sans envoyer de message de log.
- **Mode restrict :** dès que la violation est constatée, le port arrête de transférer le trafic des adresses non autorisées et transmet un message de log.
- **Mode shutdown :** dès que la violation est constatée, le port passe en état *err-disabled* (shutdown) et un message de log est envoyé.

Diagnostic sécurité sur les ports

Désactivation d'un port err-disabled selon la plateforme (`shut/no shut`) :

```
(config)#errdisable recovery cause psecure-violation
```

Diagnostic :

```
#show port-security
#show port-security interface f0/1
#show running-config
#clear port-security {all | configured | dynamic | sticky}
```

Références

- http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/configuration/guide/scg_2960.html

Présentations ICND1/ICND2 sur la commutation LAN

- Technologie Ethernet et commutation
- Prise en main d'un commutateur Cisco©
- Technologies VLANs
- Lab VLANs
- Spanning-Tree et Etherchannel
- *Lab VLANs+STP+Etherchannel*
- *Diagnostic sur le LAN*
- *Sécurités sur le LAN*

Droits