Maxime
LE BRAS
Nilda
BALDA
SIO1
Bloc 2 - SISR

Le 26/01/2024

TP2 - Configuration des switchs et sécurisation des ports

Sommaire

I - Configuration des deux stations

Tout d'abord, on configure deux stations Linux Debian 12.

PC1 Linux Debian 12 : 192.168.1.55 avec un masque de 255.255.255.0
PC2 Linux Debian 12 : 192.168.1.105 avec un masque de 255.255.255.0

```
administrateur@Debian-12-Bookworm:~$ su
Mot de passe :
root@Debian-12-Bookworm:/home/administrateur# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:49:1b:65 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.55/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe49:1b65/64 scope link
       valid_lft forever preferred_lft forever
root@Debian-12-Bookworm:/home/administrateur#
```

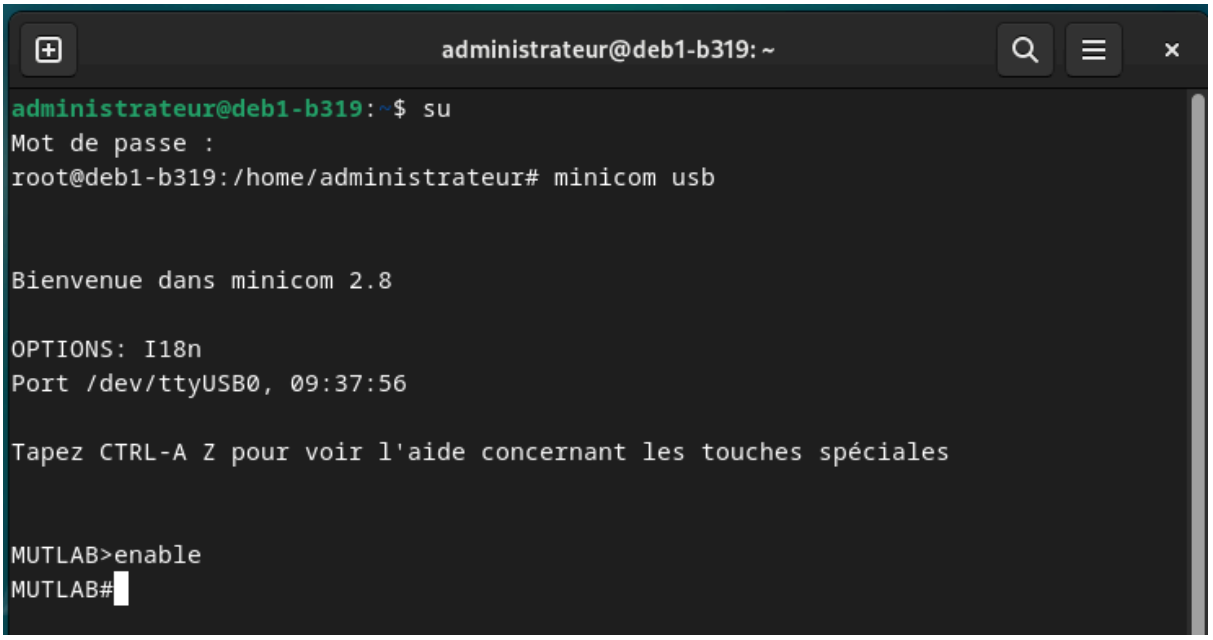
```
administrateur@deb1-b319: ~
    link/ether 08:00:27:af:02:c9 brd ff:ff:ff:ff:ff:ff
    inet 200.100.100.26/24 brd 200.100.100.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feaf:2c9/64 scope link
       valid_lft forever preferred_lft forever
root@deb1-b319:/home/administrateur# sudo ifdown enp0s3
RTNETLINK answers: Cannot assign requested address
root@deb1-b319:/home/administrateur# sudo ifdown enp0s3
ifdown: interface enp0s3 not configured
root@deb1-b319:/home/administrateur# sudo ifup enp0s3
root@deb1-b319:/home/administrateur# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:af:02:c9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.105/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feaf:2c9/64 scope link
       valid_lft forever preferred_lft forever
root@deb1-b319:/home/administrateur#
```

Nous avons testé les interconnexions entre les deux ordinateurs et ça a marché !

Lorsqu'on a fait les branchements au switch, allez dans le terminal, se mettre en su -, faire minicom -s pour configurer le switch, faire les configurations nécessaires (en fixant le débit 9600 bits et le port série à ttyUSB0) et sauvegarder-sous sous le nom d'USB.
Enfin, il faut vérifier que le périphérique Prolific est activé.

II - Configuration du switch

1) Etape 1



Taper enable pour passer en accès privilégié.

2) Etape 2

Il faut taper la commande "show running-config" (ou "show run") afin de voir comment est configuré le switch cisco (voir screens partie III étape 1, ça ressemble à peu près à ça, car sur la configuration de base, il y a des paramètres non définis)

Question 1:

Il y a 24 interfaces Fast Ethernet et 2 interfaces Gigabit Ethernet.

Question 2:

La plage de valeurs affichée pour les lignes VTY est de 0 à 15.

Question 3:

```
MUTLAB#show startup-config
startup-config is not present
MUTLAB#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MUTLAB(config)#hostname ALSwitch
ALSwitch(config)#exit
ALSwitch#
*Jun 18 01:52:23.719: %SYS-5-CONFIG_I: Configured from console by console
ALSwitch#
```

Ça nous affiche “startup-config is not present” donc il y a pas de fichier de configuration présent dans le switch.

Question 4:

Il n'y a pas d’adresse IP définie sur le commutateur.

Questions 5-6-7:

```
ALSwitch#show interface VLAN 1
Vlan1 is up, line protocol is down
  Hardware is EtherSVI, address is 0025.8440.ac40 (bia 0025.8440.ac40)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 10w4d, output 10w6d, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     17980 packets input, 4152439 bytes, 0 no buffer
     Received 0 broadcasts (130 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     2219 packets output, 174124 bytes, 0 underruns
```

L’adresse MAC de cette interface de commutateur virtuelle est 0025.8440.AC40.

La taille maximale des paquets (MTU = Maximum Transfert Unit) est fixée à 1500. Le MTU est exprimé en bytes.

L’interface fonctionne parfaitement !

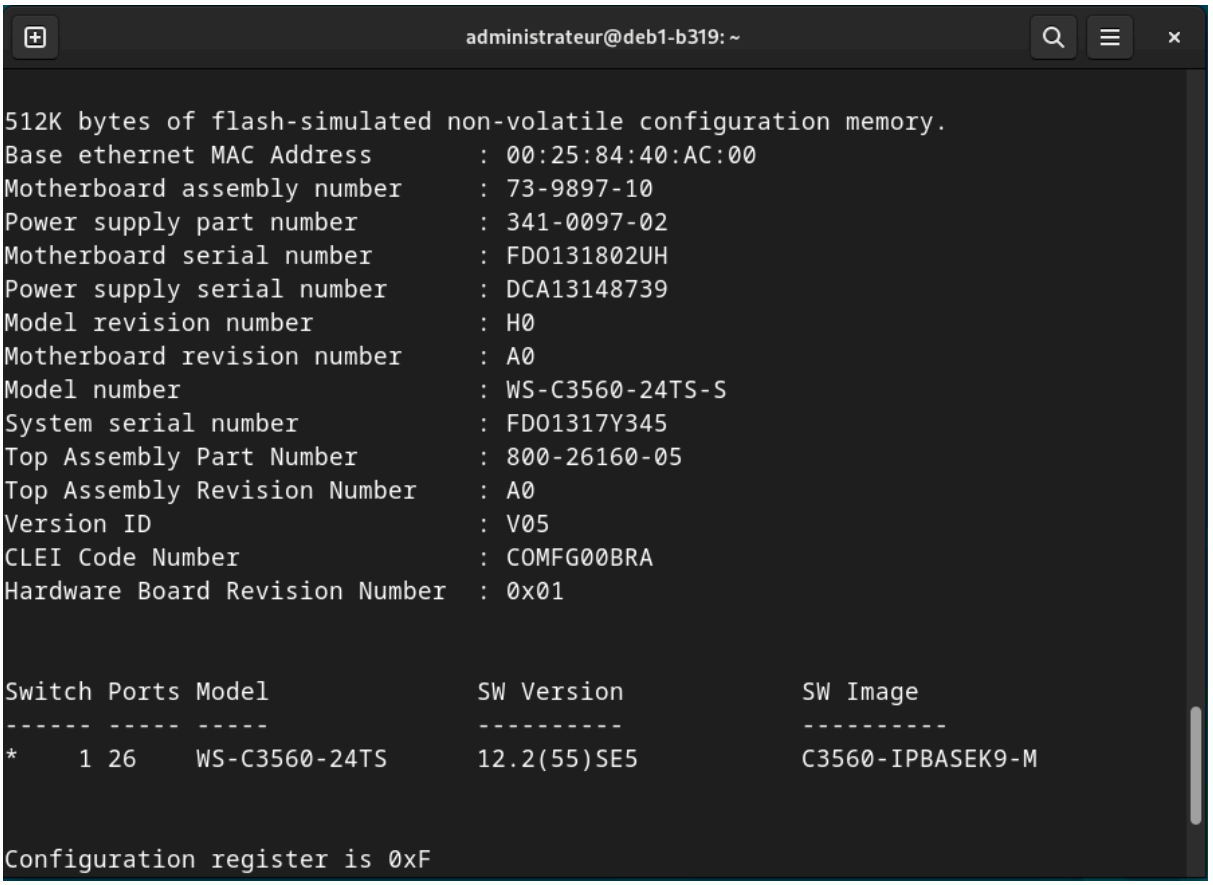
3) Etape 3

Question 1:

L'acronyme IOS de Cisco signifie "InternetWork Operating System" ce qui veut dire en français "système d'exploitation pour la connexion des réseaux".

On tape "show version" afin d'avoir les informations de version du switch.

Questions 2-3-4-5:



Le commutateur exécute la version 12.2 de l'IOS Cisco.

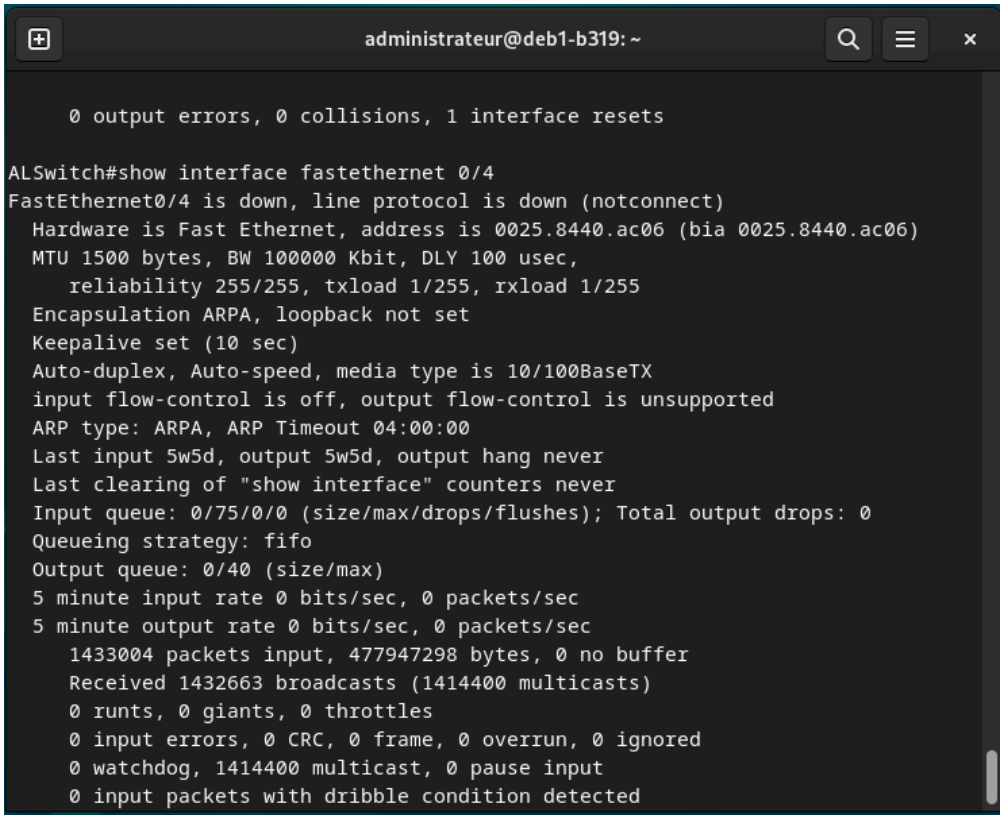
Le nom de fichier de l'image système est C3560-IPBASEK9-M.

L'adresse MAC de base de ce commutateur est 00:25:84:40:AC:00.

Le modèle exact du switch est WS-C3560-24TS-S.

4) Etape 4

Faire la commande “show interface fastethernet 0/4” pour examiner les propriétés de la quatrième interface FastEthernet.



Question 1:

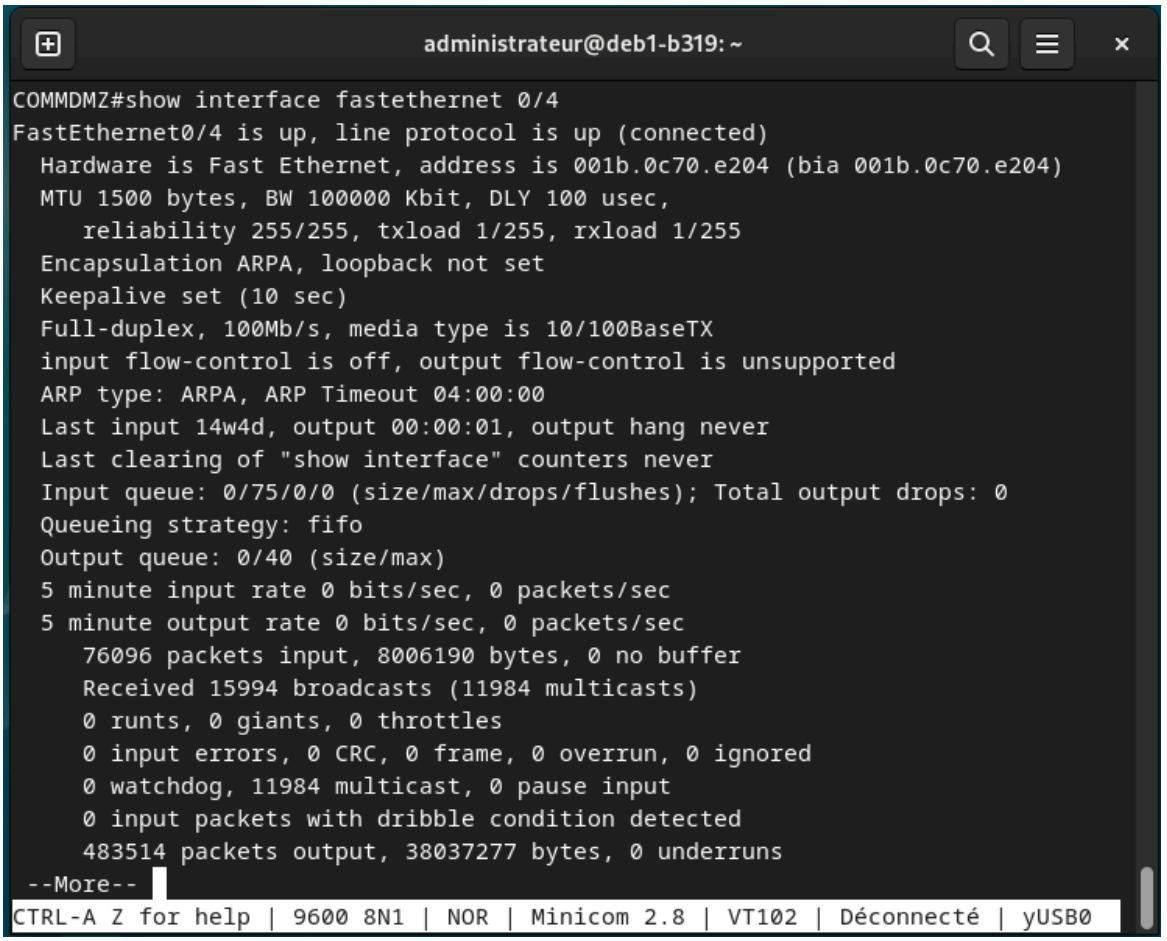
L’interface FastEthernet 0/4 est en mode down.

Question 2:

On doit brancher l’ordinateur à la 4ème interface FastEthernet du switch Cisco et faire les étapes suivantes :

- passer en mode privilégié (enable)
- conf t
- interface fastethernet 0/4
- no shutdown
- exit *2
- show interface fastethernet 0/4

Normalement, l’interface est up après cette procédure.



Question 3:

L'adresse MAC de cette interface est 001B.0C70.E204

Question 4:

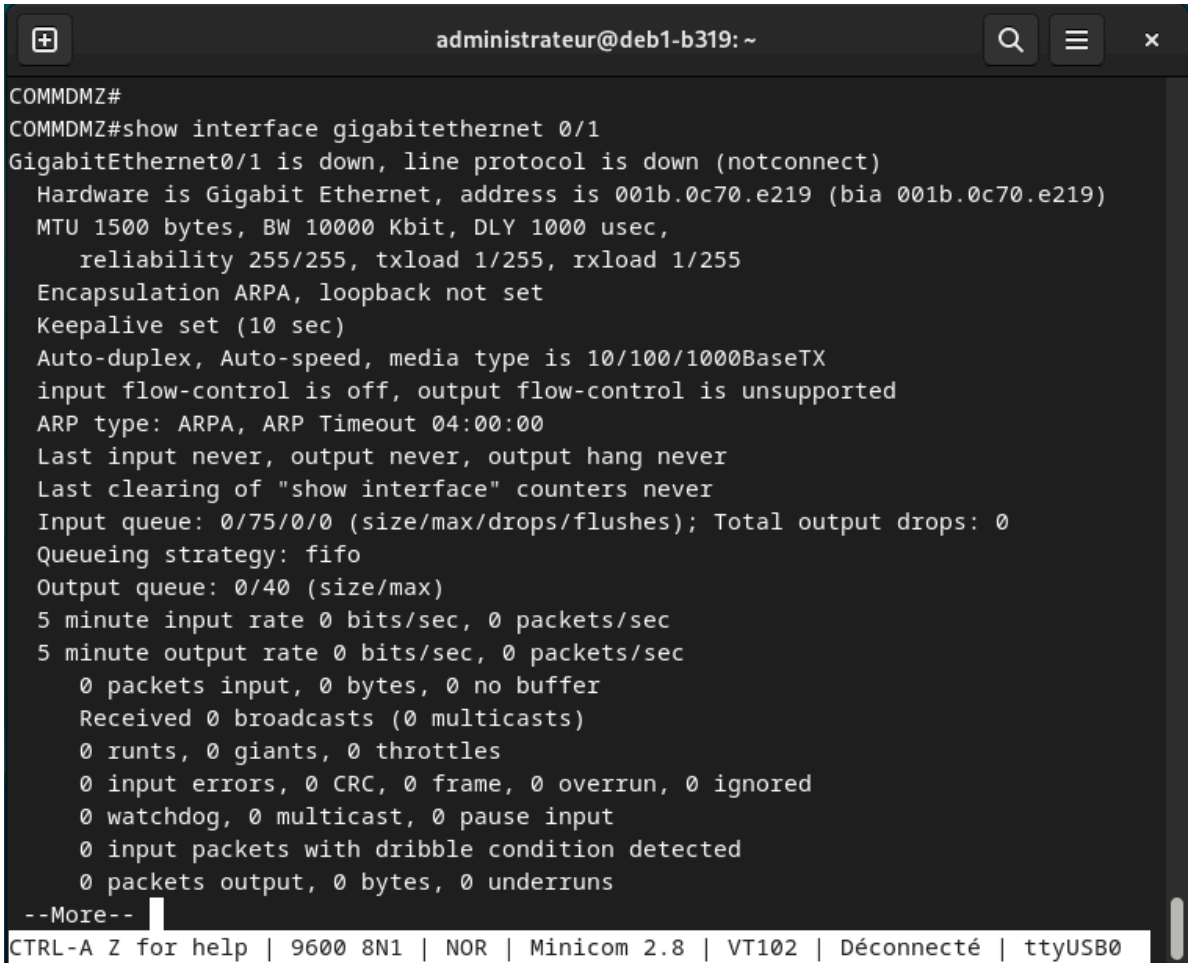
J'ai remarqué que les deux adresses MAC (celles de l'interface et du contrôleur réseau du switch) sont quasiment les mêmes sauf que le dernier chiffre de l'adresse MAC de l'interface est un identifiant numérique de l'interface afin de différencier les interfaces du switch.

Question 5:

Les paramètres de vitesse et de mode duplex de l'interface sont:

- 100 Mb/s (ce qui correspond au maximum de débit par rapport à la carte réseau)
- Full-duplex (transmission de données dans les deux sens et simultanément)

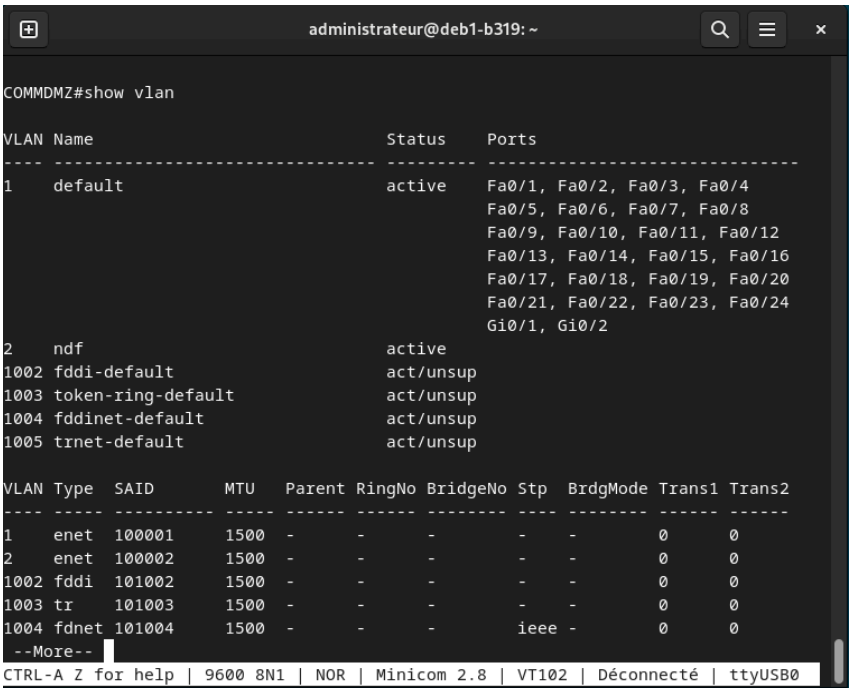
Question 6:



L'interface GigabitEthernet 0/1 est down.
L'utilité d'une interface GigabitEthernet est d'équilibrer le trafic et d'augmenter la capacité de la bande passante des liaisons montantes.

5) Etape 5

Avec l'aide de la commande "show vlan", on peut voir les paramètres VLAN du switch.



Question 1:

Le nom du VLAN 1 est : default

Question 2:

Les ports qui se trouvent dans le VLAN 1 sont :

- Fa0/1 à Fa0/24
- Gi0/1, Gi0/2

Question 3:

Le VLAN 1 est actif, car c'est le VLAN par défaut où il y a toutes les interfaces du switch.

Question 4:

Le type du VLAN 1 est enet. Le type de VLAN enet se réfère à un VLAN Ethernet Standard, cela signifie que le VLAN est basé sur les adresses MAC des dispositifs connectés au switch (aux interfaces). Les adresses MAC permettent d'assigner les ports à des VLANS spécifiques.

6) Etape 6

```
COMMDMZ# show flash

Directory of flash:/

    2  -rwx         736   Mar 1 1993 00:41:38 +00:00  vlan.dat.renamed
    3  -rwx        1384   Mar 9 1993 20:46:16 +00:00  config.text
    4  -rwx     9813681   Mar 1 1993 00:07:13 +00:00  c2960-lanbasek9-mz.122-55.SE5.bin
    5  -rwx        1387   Mar 1 1993 00:44:51 +00:00  config.text.renamed
    6  -rwx         616   Mar 2 1993 18:11:13 +00:00  vlan.dat
    8  -rwx           5   Mar 1 1993 00:44:51 +00:00  private-config.text.renamed
    9  -rwx           5   Mar 9 1993 20:46:16 +00:00  private-config.text
   10  -rwx        2072   Mar 9 1993 20:46:16 +00:00  multiple-fs

32514048 bytes total (22689792 bytes free)
COMMDMZ#
```

La mémoire Flash est comme une mémoire ROM sauf que c'est sur un switch et elle stocke l'image de l'OS (décompressée et lancée au démarrage).

Question 1:

On a comme fichiers :

- vlan.dat.renamed
- config.text
- c2960-lanbasek9-mz.122-55.SE5.bin
- config.text.renamed
- vlan.dat
- private-config.text.renamed
- private-config.text
- multiple-fs

Ils permettent le bon fonctionnement du switch.

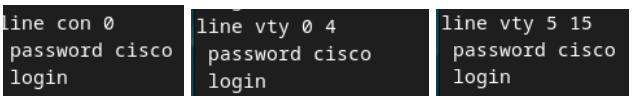
7) Etape 7

```
32514048 bytes total (22689792 bytes free)
COMMDMZ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COMMDMZ(config)#hostname ALSwitch
ALSwitch(config)#exit
ALSwitch#
*Jun 27 01:33:37.454: %SYS-5-CONFIG_I: Configured from console by console
ALSwitch#
```

Pour attribuer un nom au switch, il faut faire “conf t”, ensuite “hostname (nom de la machine)” et on quitte le mode config avec “exit”.

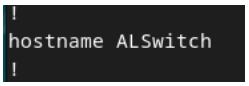
8) Etape 8

Question 1:



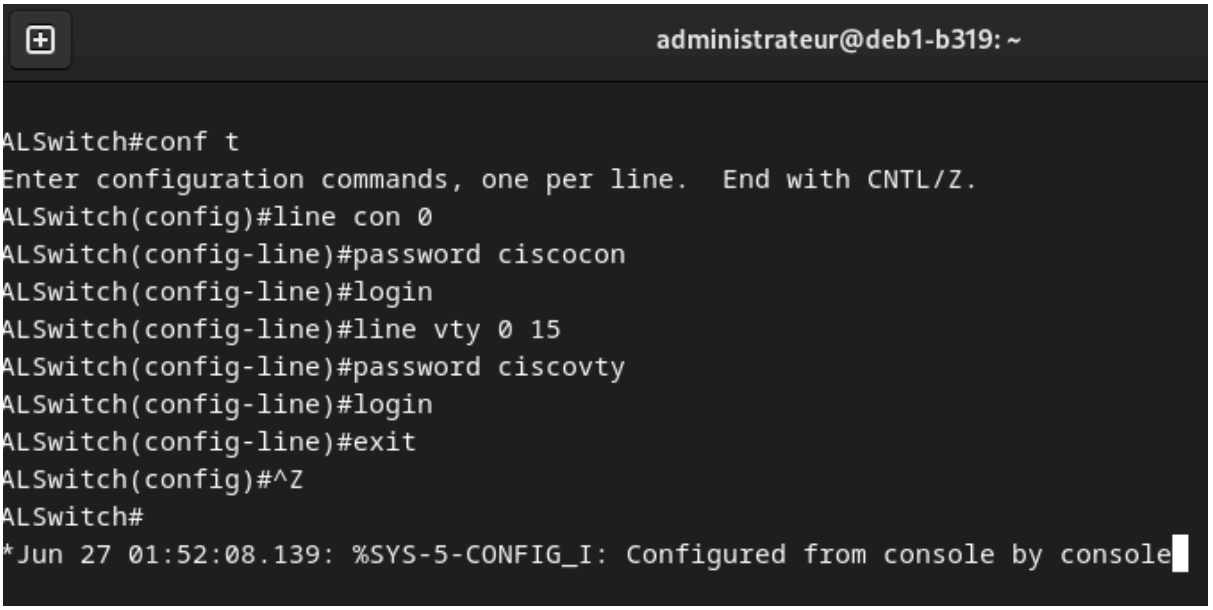
Ces screens permettent d’illustrer les lignes VTY et CON où on a défini manuellement les mots de passe (cisco) de la console et de l’accès par telnet (voir étape suivante), cependant sur la configuration de base, il y a aucun mot de passe défini pour les lignes VTY et CON.

Question 2:



En ce qui concerne le nom d’hôte du switch, la configuration indique “hostname ALSwitch” donc ça représente la commande que j’ai saisie précédemment pour modifier le nom de machine.

9) Etape 9



```
Bienvenue dans minicom 2.8

OPTIONS: I18n
Port /dev/ttyUSB0, 16:39:46

Tapez CTRL-A Z pour voir l'aide concernant les touches spéciales



User Access Verification

Password:
ALSwitch>
```

Ces commandes permettent de configurer les mots de passe d'accès à la console du switch et par Telnet.

10) Etape 10

```
enable secret 5 $1$BEaN$H3t2./Tda3VFRAPROMUG//
```

```
User Access Verification

Password:
ALSwitch>enable
Password:
ALSwitch#
```

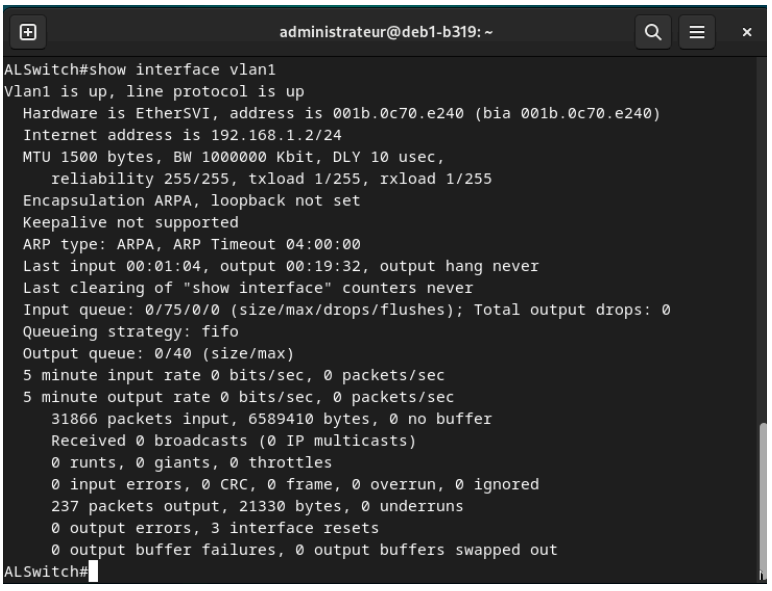
Afin de sécuriser quand on veut passer en mode privilégié, il faut faire "conf t" et "enable secret class", dans la configuration ("show running-config"), le mot de passe sera crypté.

11) Etape 11

```
ALSwitch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ALSwitch(config)#interface vlan1
ALSwitch(config-if)#ip address 192.168.1.2 255.255.255.0
ALSwitch(config-if)#no shutdown
ALSwitch(config-if)#exit
ALSwitch(config)#ip default-gateway 192.168.1.1*
                                              ^
% Invalid input detected at '^' marker.

ALSwitch(config)#ip default-gateway 192.168.1.1
ALSwitch(config)#exit
ALSwitch#
*Jun 27 02:16:29.141: %SYS-5-CONFIG_I: Configured from console be
```

```
ALSwitch#telnet 192.168.1.2
Trying 192.168.1.2 ... Open


User Access Verification

Password:
ALSwitch>
```

12) Etape 12



Question 1:

La bande passante définie sur cette interface est 1000000 Kbit.
La bande passante d'une interface est la capacité maximale de transmission des données à travers elle.

Question 2:

L'état du VLAN 1 est up (câble relié entre l'ordinateur et le switch) et le protocole de ligne est up. Le protocole de ligne utilisé est le STP (Spanning-Tree Protocol) qui est mis par défaut. Le STP est un protocole réseau de niveau 2 permettant de déterminer une topologie réseau sans boucles dans les LAN avec ponts.

Question 3:

La stratégie de file d'attente est le FIFO (First In First Out).

III - Contrôle des tables de mac-adresses d'un switch et sécurité de port

1) Etape 1

Avec l'aide des commandes de la partie précédente, nous avons réussi à configurer une deuxième fois le switch.

Nous pouvons voir la configuration du switch avec la commande "show running-config":

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

Current configuration : 1514 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ALSwitch
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$bXh5$ABEnbh2zWarSviyHzq59a1
```

```
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
```

```
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
```

2) Etape 2-3

Avant de faire un ping, vérifiez si on est bien sur la bonne interface réseau (voir dans l'onglet réseau de la machine virtuelle).

```
root@Debian-12-Bookworm:/home/administrateur# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=1.47 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=2.32 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=2.04 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=255 time=1.58 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=255 time=2.35 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=255 time=3.13 ms
64 bytes from 192.168.1.2: icmp_seq=8 ttl=255 time=3.28 ms
64 bytes from 192.168.1.2: icmp_seq=9 ttl=255 time=1.43 ms
64 bytes from 192.168.1.2: icmp_seq=10 ttl=255 time=2.35 ms
64 bytes from 192.168.1.2: icmp_seq=11 ttl=255 time=1.95 ms
64 bytes from 192.168.1.2: icmp_seq=12 ttl=255 time=1.54 ms
64 bytes from 192.168.1.2: icmp_seq=13 ttl=255 time=2.54 ms
64 bytes from 192.168.1.2: icmp_seq=14 ttl=255 time=1.33 ms
64 bytes from 192.168.1.2: icmp_seq=15 ttl=255 time=2.33 ms
64 bytes from 192.168.1.2: icmp_seq=16 ttl=255 time=4.15 ms
64 bytes from 192.168.1.2: icmp_seq=17 ttl=255 time=17.9 ms
```

Ping du PC2 (192.168.1.7) au switch (192.168.1.2)

```
root@deb1-b319:/home/administrateur# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=1.19 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=2.26 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=1.96 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=1.19 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=255 time=2.64 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=255 time=1.68 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=255 time=2.01 ms
64 bytes from 192.168.1.2: icmp_seq=8 ttl=255 time=3.14 ms
64 bytes from 192.168.1.2: icmp_seq=9 ttl=255 time=2.77 ms
64 bytes from 192.168.1.2: icmp_seq=10 ttl=255 time=3.15 ms
64 bytes from 192.168.1.2: icmp_seq=11 ttl=255 time=2.29 ms
64 bytes from 192.168.1.2: icmp_seq=12 ttl=255 time=2.87 ms
64 bytes from 192.168.1.2: icmp_seq=13 ttl=255 time=2.46 ms
64 bytes from 192.168.1.2: icmp_seq=14 ttl=255 time=1.76 ms
64 bytes from 192.168.1.2: icmp_seq=15 ttl=255 time=2.44 ms
64 bytes from 192.168.1.2: icmp_seq=16 ttl=255 time=1.39 ms
64 bytes from 192.168.1.2: icmp_seq=17 ttl=255 time=2.19 ms
```

Ping du PC1 (192.168.1.6) au switch (192.168.1.2)

Tous les pings sont fonctionnels donc c'est bon !

3) Etape 4

PC1:


```
    link/ether 08:00:27:af:02:c9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.6/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feaf:2c9/64 scope link
       valid_lft forever preferred_lft forever
```

PC2:


```
link/ether 08:00:27:49:1b:65 brd ff:ff:ff:ff:ff:ff
```

4) Etape 5

Pour voir les adresses MAC apprises par le commutateur, il faut taper la commande “show mac address-table” en mode “enable” (accès privilégié) :

```
ALSwitch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
```

Il n'y a pas d’adresses dynamiques.
Il y a 20 adresses MAC au total.
Il n’y a pas d’adresses statiques définies par l’utilisateur.
Les adresses MAC ne correspondent pas aux adresses MAC des hôtes.

5) Etape 6

La commande “show mac address-table” avec l’option “?” permet de voir les différentes options de celle-ci :

```
ALSwitch#show mac address-table ?
  address       Address to lookup in the table
  aging-time    MAC address table aging parameters
  count         Number of MAC addresses in the table
  dynamic       List dynamic MAC addresses
  interface     List MAC adresses on a specific interface
  learning      Display learning on VLAN or interface
  move          MAC Move information
  multicast     List multicast MAC addresses
  notification  MAC notification parameters and history table
  secure        List secure MAC addresses
  static        List static MAC addresses
  vlan          List MAC addresses on a specific vlan
  |             Output modifiers
  <cr>
```

Il y a 13 options disponibles pour la commande “show mac address-table”

Le nombre d’adresses MAC de la table qui ont été apprises dynamiquement est de 1.

6) Etape 7

Dans le mode “enable”, la commande “clear mac address-table dynamic” permet de supprimer toutes les adresses MAC dynamiques de la table.

```
ALSwitch#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    1860.2489.50e2    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 1
ALSwitch#clear mac address-table dynamic
ALSwitch#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

Lorsqu'on tape "show mac address-table" et "show mac address-table dynamic", on a plus d'adresses MAC dynamiques.

7) Etape 8

Afin de configurer une adresse MAC statique dans une interface quelconque, on fait "conf t", ensuite, on fait "mac address-table static (adresse MAC du PC2) vlan 1 interface (nom de l'interface voulue). Enfin, on vérifie avec "show mac address-table".

```
ALSwitch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    0800.2749.1b65    STATIC      Fa0/4
Total Mac Addresses for this criterion: 21
```

8) Etape 9

Afin de supprimer une adresse MAC statique, faire "enable", ensuite "conf t" et taper la commande ""no mac address-table static (adresse MAC du PC2) vlan 1 interface (nom de l'interface voulue)

Enfin, on vérifie avec "show mac address-table".

```
ALSwitch#show mac address-table
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
```

9) Etape 10

Nous avons regardé les différentes options de la commande “switchport port-security” en faisant ceci “switchport port-security ?”

On peut utiliser les commandes “mac-address” (adresse autorisée sur le port) et “violation” (options de sécurité en cas de violation) afin de sécuriser le port qu’on veut.

Ensuite, pour que le port de commutation fastethernet 0/4 soit sécurisé, tout d’abord, nous avons tapé (en mode config-if donc dans cette interface), “switchport mode access”, “switchport port-security” (pour se mettre en mode sécurité) et enfin “switchport port-security mac-address sticky” (ce qui permet de sauvegarder les adresses MAC connectées au switch dans la table d’adresses MAC).

```
ALSwitch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ALSwitch(config)#interface fastethernet 0/4
ALSwitch(config-if)#switchport port-security ?
  aging        Port-security aging commands
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
  <cr>
```

10) Etape 11

Les pings sont bien fonctionnels entre le PC1 et le PC2 !

```
All    0100.0ccc.cccd    STATIC      CPU
All    0180.c200.0000    STATIC      CPU
All    0180.c200.0001    STATIC      CPU
All    0180.c200.0002    STATIC      CPU
All    0180.c200.0003    STATIC      CPU
All    0180.c200.0004    STATIC      CPU
All    0180.c200.0005    STATIC      CPU
All    0180.c200.0006    STATIC      CPU
All    0180.c200.0007    STATIC      CPU
All    0180.c200.0008    STATIC      CPU
All    0180.c200.0009    STATIC      CPU
All    0180.c200.000a    STATIC      CPU
All    0180.c200.000b    STATIC      CPU
All    0180.c200.000c    STATIC      CPU
All    0180.c200.000d    STATIC      CPU
All    0180.c200.000e    STATIC      CPU
All    0180.c200.000f    STATIC      CPU
All    0180.c200.0010    STATIC      CPU
All    ffff.ffff.ffff    STATIC      CPU
  1    0800.2749.1b65    DYNAMIC     Fa0/1
  1    0800.27af.02c9    DYNAMIC     Fa0/2
  1    1860.2489.50e2    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 23
```

Ces adresses sont listées en fonction du type d'adressage (statique et dynamique) et de son port.

```
ALSwitch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
      Fa0/4              1            0                  0         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

En première colonne, on a les ports sécurisés.
En deuxième colonne, on a le maximum d'adresses sécurisées dans le port (qui doit être 1).
En troisième colonne, on a le nombre d'adresses actuelles dans le port.
En quatrième colonne, on a le nombre de fois où la sécurité a été non respectée.
En cinquième colonne, on voit l'état de la sécurité dans le port.

11) Etape 12

Pour afficher le fichier de la configuration courante du switch, il faut mettre “show running-config”.

```
interface FastEthernet0/4
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
```

On voit directement la mise en œuvre de la sécurité dans le port fastethernet 0/4 avec les commandes saisies.

12) Etape 13

On a tapé la commande “switchport port-security maximum 1” dans l’interface fastethernet 0/4 afin de définir le nombre maximum d’adresses MAC à 1 pour ce port.

Le port fastethernet 0/4 est down et le protocole de ligne est down.

```
ALSwitch#show interface fastethernet 0/4
FastEthernet0/4 is down, line protocol is down (err-disabled)
```

```
ALSwitch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
      Fa0/4             1            1                  1         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

```
ALSwitch#show port-security interface fastethernet 0/4
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0800.27af.02c9:1
Security Violation Count   : 1
```

13) Etape 14

```
ALSwitch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ALSwitch(config)#interface fastethernet 0/4
ALSwitch(config-if)#shutdown
ALSwitch(config-if)#no shutd
*Jul  6 01:26:17.772: %LINK-5-CHANGED: Interface FastEthernet0/4, changed staten
ALSwitch(config-if)#
*Jul  6 01:26:24.248: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state p
*Jul  6 01:26:25.255: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEth  o
ALSwitch(config-if)#no shutdown
ALSwitch(config-if)#
*Jul  6 01:26:56.746: %PM-4-ERR_DISABLE: psecure-violation error detected on Fae
*Jul  6 01:26:56.746: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation oc.
*Jul  6 01:26:57.752: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
*Jul  6 01:26:58.751: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state
```

Nous avons eu une violation de la sécurité du port fastethernet 0/4 et le port était désactivé (voir étape 13).
On a tapé les commandes “shutdown” pour désactiver le port et “no shutdown" pour le réactiver.
On remarque que le port se déconnecte, car il y a du trafic réseau (voir screen).

IV - Conclusion

Dans ce TP, nous avons appris à configurer un switch, à contrôler les tables d’adresses mac d’un switch et à sécuriser les ports de celui-ci.