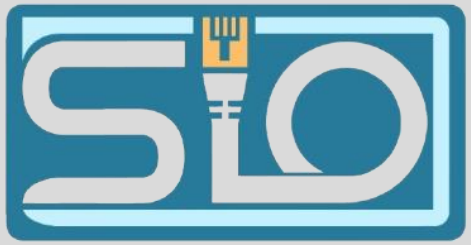
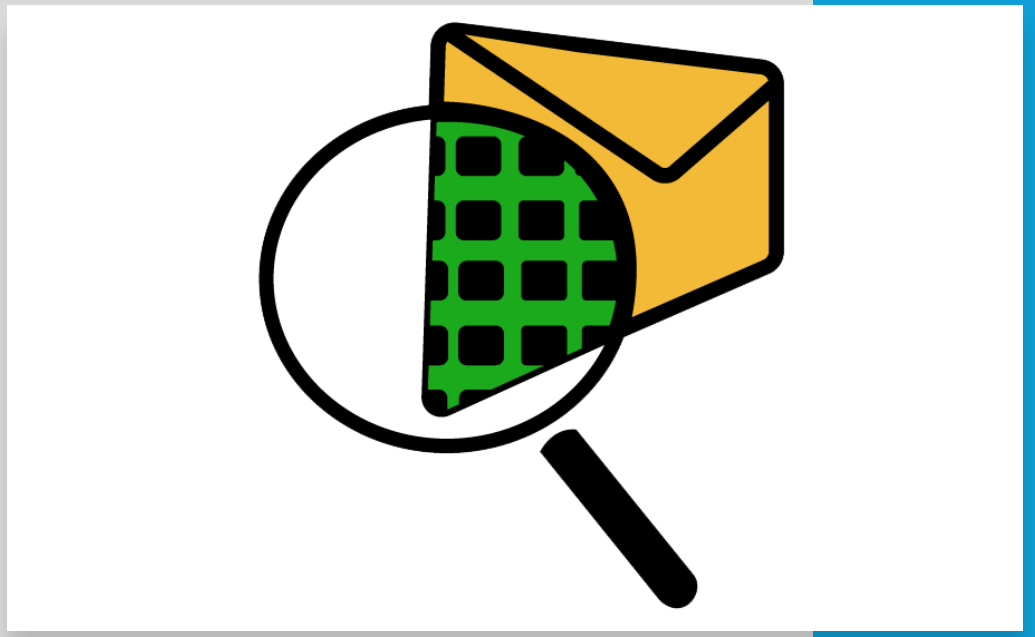
TRIOUX Jimmy – BTS SIO1 SISR

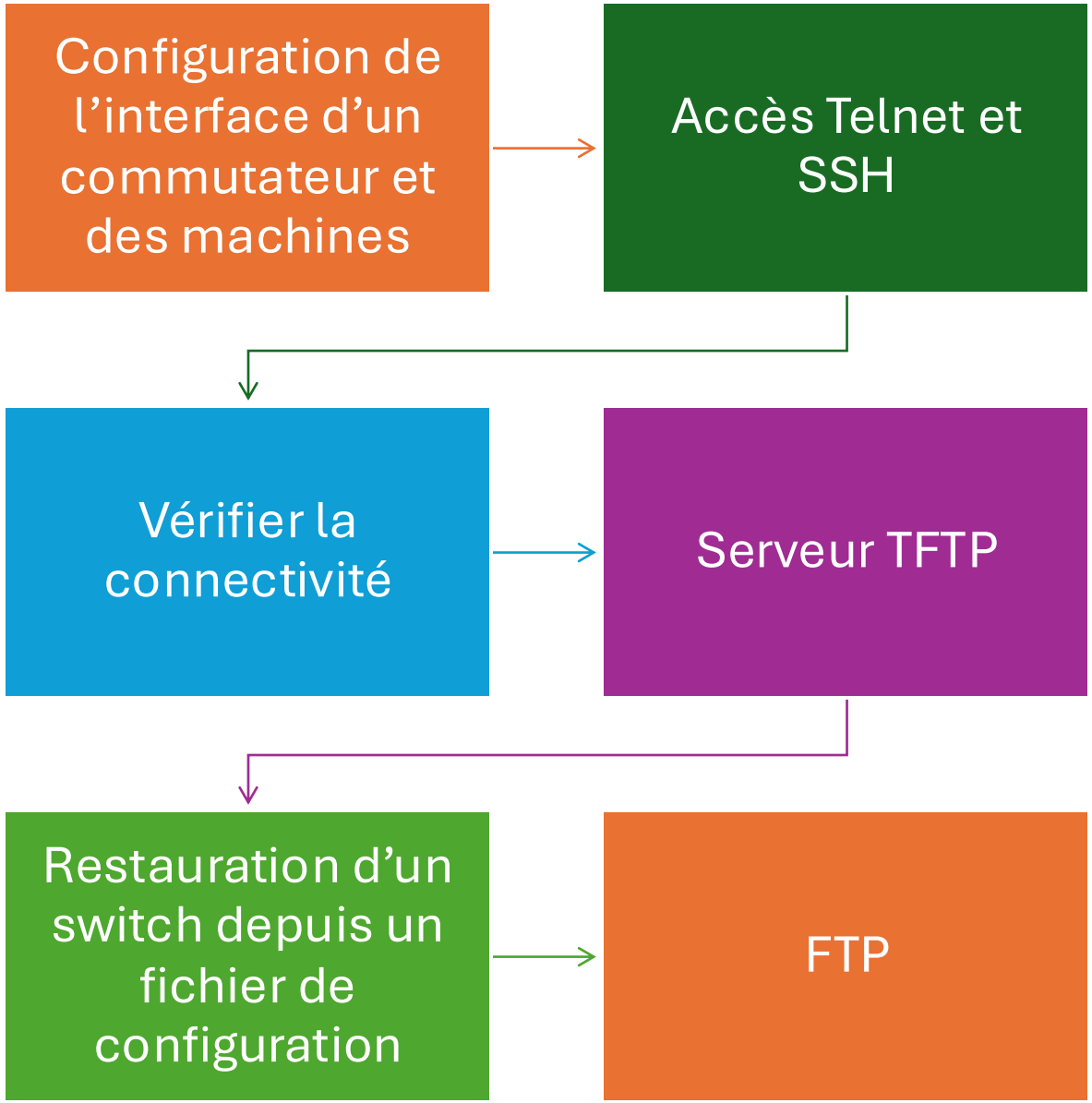
TP – Découverte et preparation d'un switch



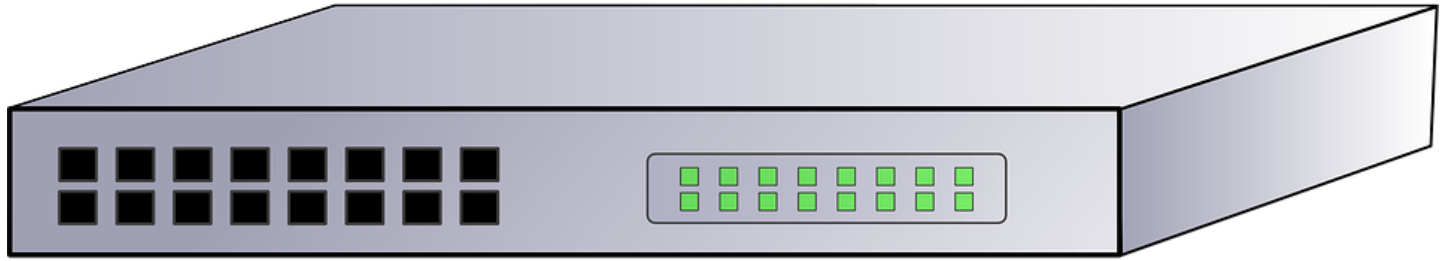


Sommaire

Sur Cisco Packet Tracer en simulation
Et sur un switch Cisco en physique



Configuration de l’interface d’un commutateur



Sur Cisco Packet Tracer

Intérêt des commandes

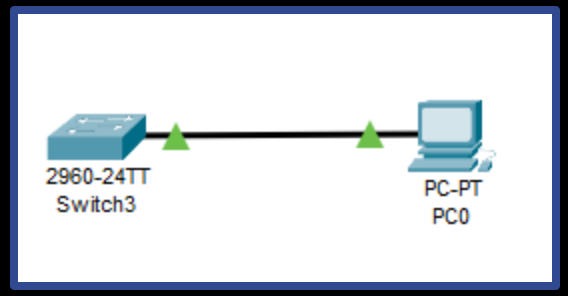
Commandes	Actions
Enable	Mode privilégié
Enable secret « mot-de-passe »	Mode privilégié avec un mot de passe
Configuration terminal	Mode de configuration globale
Interface vlan 1	Mode de configuration de l'interface VLAN native
Hostname « nom »	Modifie le nom du switch
Line vty x x	Configure les lignes pour accéder à Telnet ou au SSH
Ip address 192.168.X.X 255.255.X.X	Affecte une adresse IP et un masque de sous réseau
No sh	Permet d'activer l'interface qui est désactivé par défaut
Exit	Permet de quitter le mode de configuration actuel ou de revenir à un niveau antérieur

Pourquoi définir une passerelle dans le cadre d’un switch ?

La **passerelle par défaut**, ou **default gateway**, est le routeur auquel le switch va être connecté pour envoyer des données à l’extérieur de son LAN.

Définir une passerelle dans le cadre d'un switch apporte une sécurité, et de pouvoir y accéder à distance pour un administrateur qui souhaiterait configurer le switch depuis un autre réseau.

Configurer un switch sur Cisco Packet Tracer



2

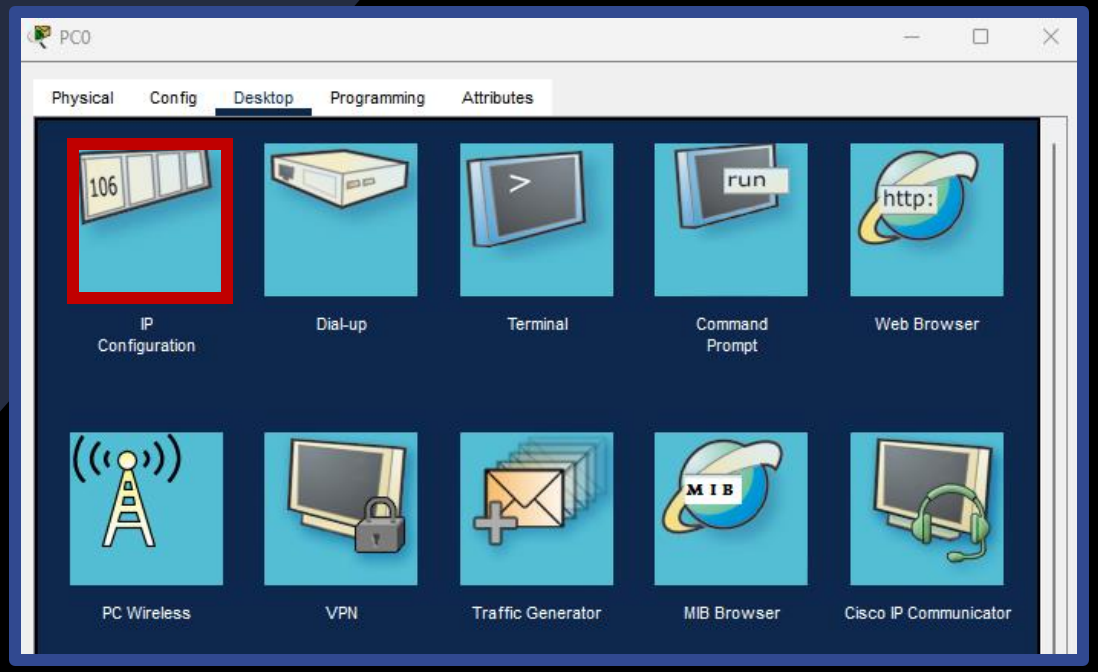
```
Switch>enable
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#interface vlan 1
Switch(config-if)#
Switch(config-if)#ip address 192.168.1.100 255.255.255.0
Switch(config-if)#
Switch(config-if)#no sh
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#
Switch(config)#ip default-gateway 192.168.1.1
Switch(config)#
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

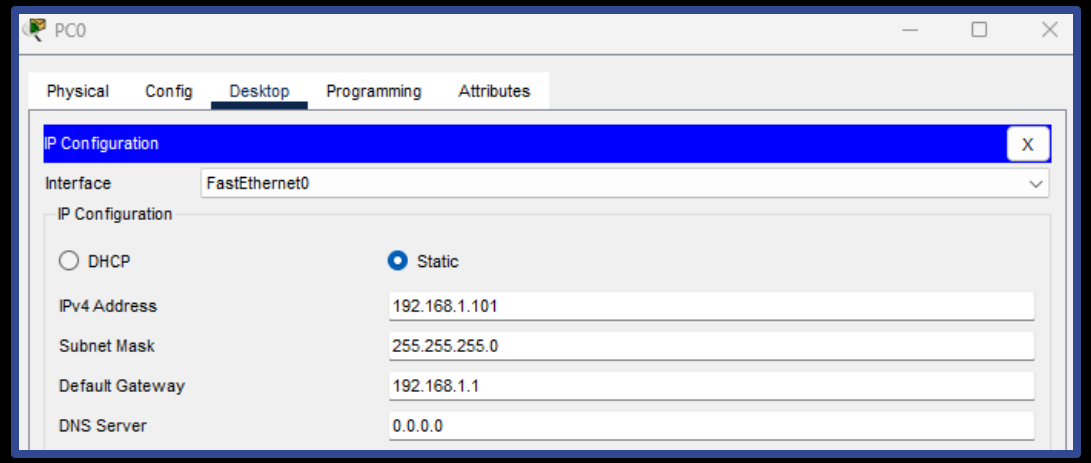
Nous allons configurer un réseau afin de pouvoir s'y connecter à distance avec **Telnet.**

- Placer un switch **2960** et un poste de PC avec un câble **Copper Straight-Through** ;
- Double cliquer sur votre switch et accédez à l'onglet « **CLI** » ;
- Et suivez les étapes comme sur l'image 2 avec vos propres adresses.

Réitérez-vous au slide d'explication des commandes CLI pour paramétrer le VLAN.

Relier le poste de PC au switch





Tout d'abord, contrairement au switch, le poste de PC se configure depuis l'onglet « **Desktop** » dans le menu « **IP Configuration** ».

Désormais, vous accédez à la page de paramétrage des interfaces réseaux de votre poste.

Afin de faire communiquer le poste de PC avec le switch préalablement configuré, il sera important de renseigner une passerelle par défaut pour que les deux puissent communiquer ensemble.

Config du PC :

Adresse IP : 192.168.1.101
Masque : 255.255.255.0
Passerelle : 192.168.1.1

Test de connectivité

```
Switch>ping 192.168.1.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.101, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Pour vérifier la connectivité avec le poste de PC depuis le VLAN1, faites un ping, toujours dans le **CLI** du switch.

```
C:\>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.100: bytes=32 time<1ms TTL=255
Reply from 192.168.1.100: bytes=32 time<1ms TTL=255
Reply from 192.168.1.100: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Pour pinger votre VLAN1, retourner dans « **Desktop** », « **Command Prompt** » et faites un ping vers l'adresse IP de votre VLAN.

Vérifier si l'interface virtuelle est bien configurée

```
interface Vlan1
 ip address 192.168.1.100 255.255.255.0
!
ip default-gateway 192.168.1.1
```

```
Switch#show interface vlan 1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 0060.70ab.e410 (bia 0060.70ab.e410)
  Internet address is 192.168.1.100/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, 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
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Pour vérifier que l'interface VLAN 1 est bien configurée, nous irons dans le **CLI** du switch, et nous taperons la commande « **sh ru** » qui sert à afficher la configuration active du dispositif réseau.

Pour vérifier que l'interface VLAN 1 est bien configurée, nous irons dans le **CLI** du switch, et nous taperons la commande « **sh ru** » qui sert à afficher la configuration active du dispositif réseau.

Combien y a-t-il de lignes VTY possibles ?

```
line vty 0 4
 password sio2024
 login
line vty 5 15
 password sio2024
 login
```

Il existe 16 lignes VTY au total, numérotées de 0 à 15, elles renseignent sur le nombre de connexions simultanées possibles sur le switch.

Vous pouvez les retrouver en tapant la commande « **sh ru** ».

Vérifier si l'interface virtuelle est bien configurée

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line vty 0 4
Switch(config-line)#password sio2024
Switch(config-line)#login
Switch(config-line)#
Switch(config-line)#
Switch(config-line)#transport input telnet
Switch(config-line)#
Switch(config-line)#exit
Switch(config)#
Switch(config)#write memory
                ^
% Invalid input detected at '^' marker.

Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#write memory
Building configuration...
[OK]
Switch#
```

Maintenant, nous allons configurer Telnet afin de pouvoir accéder à distance au switch. Pour activer Telnet, il faut configurer les lignes VTY qui s'occupent des connexions à distance :

1. Enable
2. Conf t
3. Line vty 0 4
4. Password « votremotdepasse »
5. Login
6. Transport input telnet (très important puisque la ligne spécifie que Telnet est autorisé sur les lignes VTY de 0 à 4)
7. Exit
8. Exit
9. Write memory (pour sauvegarder la configuration)

```
C:\>telnet 192.168.1.100
Trying 192.168.1.100 ...Open


User Access Verification

Password:
Switch>
```

Depuis le poste de PC, dans « **Desktop** », « **Command Prompt** » vous pouvez vérifier si cela fonctionne avec la commande « **telnet votreip** ».

A quoi correspond la commande « sh run » ?

La commande « **sh ru** », ou abréviation de « **show running-config** », dans l'environnement Cisco, permet d'afficher l'intégralité de la configuration en cours d'un périphérique réseau comme un switch ou un routeur par exemple.
On y retrouve les interfaces réseau configurées, les VLAN/routeur/switch, les paramètres de sécurités, les configurations des lignes de terminal (y compris les lignes VTY pour Telnet ou SSH)

Où voit-on que la ligne Telnet est ouverte ?

```
line vty 0 4
 password sio2024
 login
 transport input telnet
line vty 5 15
 password sio2024
 login
```

Descendez tout en bas de votre configuration, vous trouverez « **line vty** », si la mention « **transport input telnet** » est présente alors le Telnet est actif.

Configuration du protocole SSH

```
Switch#sh ver
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen
```

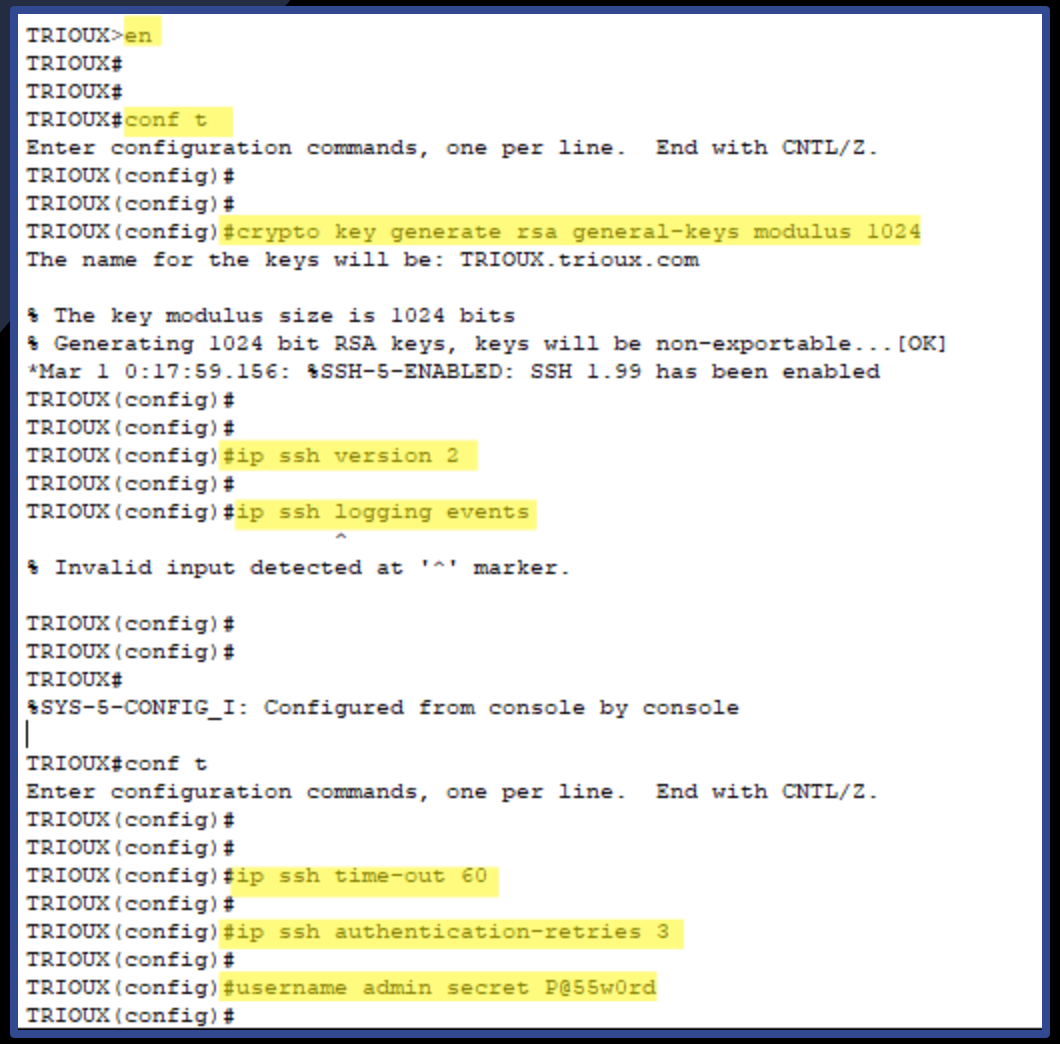
Afin de vérifier si votre switch peut recevoir le protocole SSH, il faut d'abord vérifier sa version avec la commande « **sh ver** » (**show version**). Dans le cas des switch Cisco, la mention « **K9** » ou « **crypto** » doit être présente et indique que les fonctionnalités sont disponibles.

```
Switch>en
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#hostname TRIOUX
TRIOUX(config)#
TRIOUX(config)#ip domain-name trioux.com
TRIOUX(config)#
TRIOUX(config)#exit
TRIOUX#
%SYS-5-CONFIG_I: Configured from console by console

TRIOUX#sh ru
Building configuration...

Current configuration : 1214 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname TRIOUX
!
!
!
ip domain-name trioux.com
!
```

Ensuite, nous irons dans le **CLI** du switch afin d'y configurer un nom d'hôte et un nom de domaine.

en → conf t → hostname votrenomdhote → ip domain-name nomdomaine.com

Quittez le mode config et refaites un « **sh ru** », si cela a fonctionné, les lignes « **hostname** » et « **ip domain-name** » apparaîtront.



```
TRIOUX>en
TRIOUX#
TRIOUX#
TRIOUX#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TRIOUX(config)#
TRIOUX(config)#
TRIOUX(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: TRIOUX.trioux.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:17:59.156: %SSH-5-ENABLED: SSH 1.99 has been enabled
TRIOUX(config)#
TRIOUX(config)#
TRIOUX(config)#ip ssh version 2
TRIOUX(config)#
TRIOUX(config)#ip ssh logging events
                  ^
% Invalid input detected at '^' marker.

TRIOUX(config)#
TRIOUX(config)#
TRIOUX#
%SYS-5-CONFIG_I: Configured from console by console

TRIOUX#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TRIOUX(config)#
TRIOUX(config)#
TRIOUX(config)#ip ssh time-out 60
TRIOUX(config)#
TRIOUX(config)#ip ssh authentication-retries 3
TRIOUX(config)#
TRIOUX(config)#username admin secret P@55w0rd
TRIOUX(config)#
```

Suivez les étapes comme indiquer sur l'image.
La commande « **ip ssh logging events** » ne fonctionne pas ici, probablement dû à la version de l'IOS. Cette commande peut-être remplacé par « **logging buffered 4096** » suivit d'un « **logging console** » et « **show logging** » pour avoir le journal d'événement après avoir quitté le mode de configuration terminal.

Définitions des commandes :

- **crypto key generate rsa general-keys modulus 1024** : permet de générer une clé RSA en 1024 bits afin de chiffrer l'accès en SSH ;
- **ip ssh version 2** : commande qui force le switch à utiliser la version 2 du SSH ;
- **ip ssh logging events** : active la journalisation des événements SSH. Il permet de surveiller les activités et de détecter les anomalies ou les tentatives non autorisées ;
- **ip ssh time-out 60** : commande qui définit un délai de 60 secondes pour attendre qu'une connexion SSH soit authentifiée ;
- **ip ssh authenticate-retries 3** : Limite le nombre d'essais pour entrer un mot de passe correct lors de l'authentification SSH.

Désactiver le telnet pour l'accès au switch

```
TRIOUX>en
TRIOUX#
TRIOUX#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TRIOUX(config)#
TRIOUX(config)#line vty 0 15
TRIOUX(config-line)#
TRIOUX(config-line)#login local
TRIOUX(config-line)#
TRIOUX(config-line)#transport input ssh
TRIOUX(config-line)#
TRIOUX(config-line)#exit
TRIOUX(config)#
TRIOUX(config)#exit
TRIOUX#
%SYS-5-CONFIG_I: Configured from console by console

TRIOUX#
TRIOUX#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 3
TRIOUX#
```

```
C:\>ssh -l admin 192.168.1.100

Password:



TRIOUX>
```

Pour désactiver l'accès au switch par **Telnet** et donc de passer en **SSH**, suivez les étapes indiquées sur les images.

- **login local** : indique que l'authentification des utilisateurs se fera via des comptes locaux configurés sur l'appareil ;
- **transport input ssh** : spécifie que les connexions SSH sont autorisées sur les lignes VTY.
- **show ip ssh** : montre les informations de l'état actuel de la configuration SSH sur le switch (version, nombre d'essais, délai d'attente, si activé)

Pour tester si cela fonctionne, aller dans « **Command Prompt** » et taper la commande « **ssh –l admin ip-du-switch** » sur le PC.
Après avoir rentré votre mot de passe, si votre nom d'hôte s'affiche alors tout est bon.

Supprimer la clé SSH

```
TRIOUX#
TRIOUX#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TRIOUX(config)#
TRIOUX(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
TRIOUX(config)#
*Mar 1 0:47:16.611: %SSH-5-DISABLED: SSH 1.5 has been disabled
TRIOUX(config)#
TRIOUX(config)#exit
TRIOUX#
%SYS-5-CONFIG_I: Configured from console by console

TRIOUX#
TRIOUX#sh ip ssh
SSH Disabled - version 2
%Please create RSA keys (of atleast 768 bits size) to enable SSH v2.
Authentication timeout: 60 secs; Authentication retries: 3
TRIOUX#
```

Pour supprimer la clé SSH, retourner en configuration terminal, puis rentrer simplement la commande « **crypto key zeroize rsa** » qui va effacer toutes les clés disponibles.

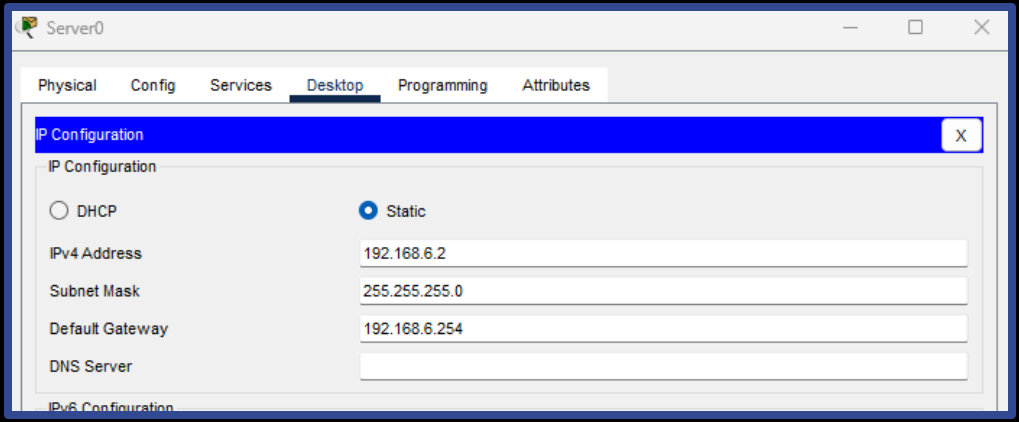
TP – Sauvegarde de la configuration d'un switch

Configuration du switch

```
Switch>
Switch>
Switch>en
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.6.1 255.255.255.0
Switch(config-if)#
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#
Switch(config-if)#ip default-gateway 192.168.6.254
Switch(config)#
Switch(config)#hostname Jimmy
Jimmy(config)#
Jimmy(config)#enable password sio2024
Jimmy(config)#
```

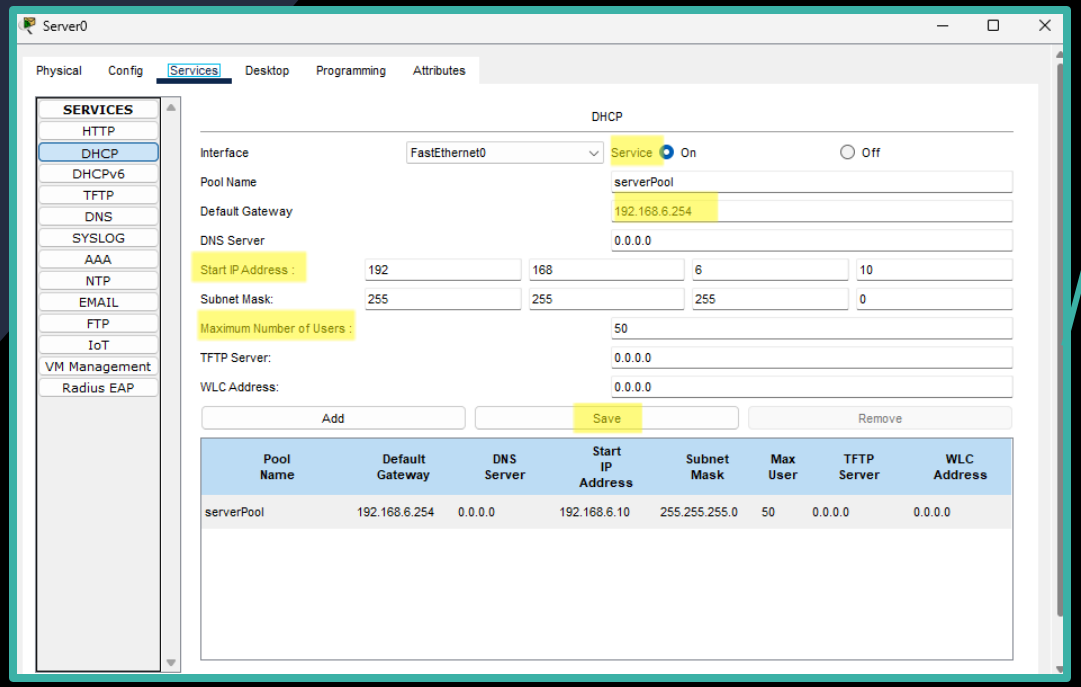
Comme dans la première partie, il est nécessaire de configurer l'interface vlan 1, d'y insérer une passerelle par défaut (**default-gateway**), de changer le nom d'hôte et d'établir un mot de passe pour se connecter au switch.

Configuration du serveur



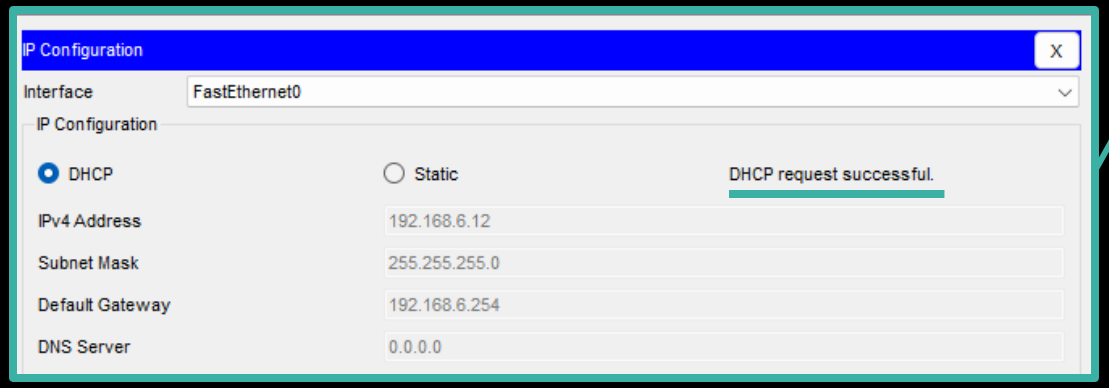
Pour le serveur, aller dans « **Desktop** », « **IP Configuration** ». On y adresse son IP, son masque de sous-réseau ainsi que sa passerelle par défaut (ici, l'interface vlan 1).

Mettre en place le DHCP



Sur le serveur :

Commencer par définir le DHCP sur le serveur avant de toucher aux postes de PC.
Pensez à cocher DHCP Service « **ON** », de définir la passerelle par défaut, une adresse IP de départ, ainsi que le nombre maximal d'utilisateur pouvant s'adresser sur la pool.



Pour les postes de PC :

Cliquer sur le poste de PC, aller dans « **Desktop** » et sélectionner « **IP Configuration** » puis cocher la case DHCP.
Si vous voyez le message « **DHCP request successful.** », tout est OK.
Refaites cette étape pour chaque poste de PC.

Vérifier si les paramètres sont actifs

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0090.217D.7B8A
   Link-local IPv6 Address.........: FE80::290:21FF:FE7D:7B8A
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.6.12
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.6.254
   DHCP Servers....................: 192.168.6.2
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-E9-AA-69-43-00-90-21-7D-7B-8A
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address.................: 0002.173A.480E
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-E9-AA-69-43-00-90-21-7D-7B-8A
   DNS Servers.....................: ::
                                     0.0.0.0
```

Aller dans « **Command Prompt** » sur l'un de vos poste PC, et taper « **ipconfig /all** » afin de vérifier si le service DHCP est bien actif.

Le poste de PC est bien relié au serveur DHCP (**192.168.6.2**), son adresse IPv4 est bien au dessus de **192.168.6.10** comme exigeait dans l'adressage de pool DHCP et la passerelle par défaut apparaît également.

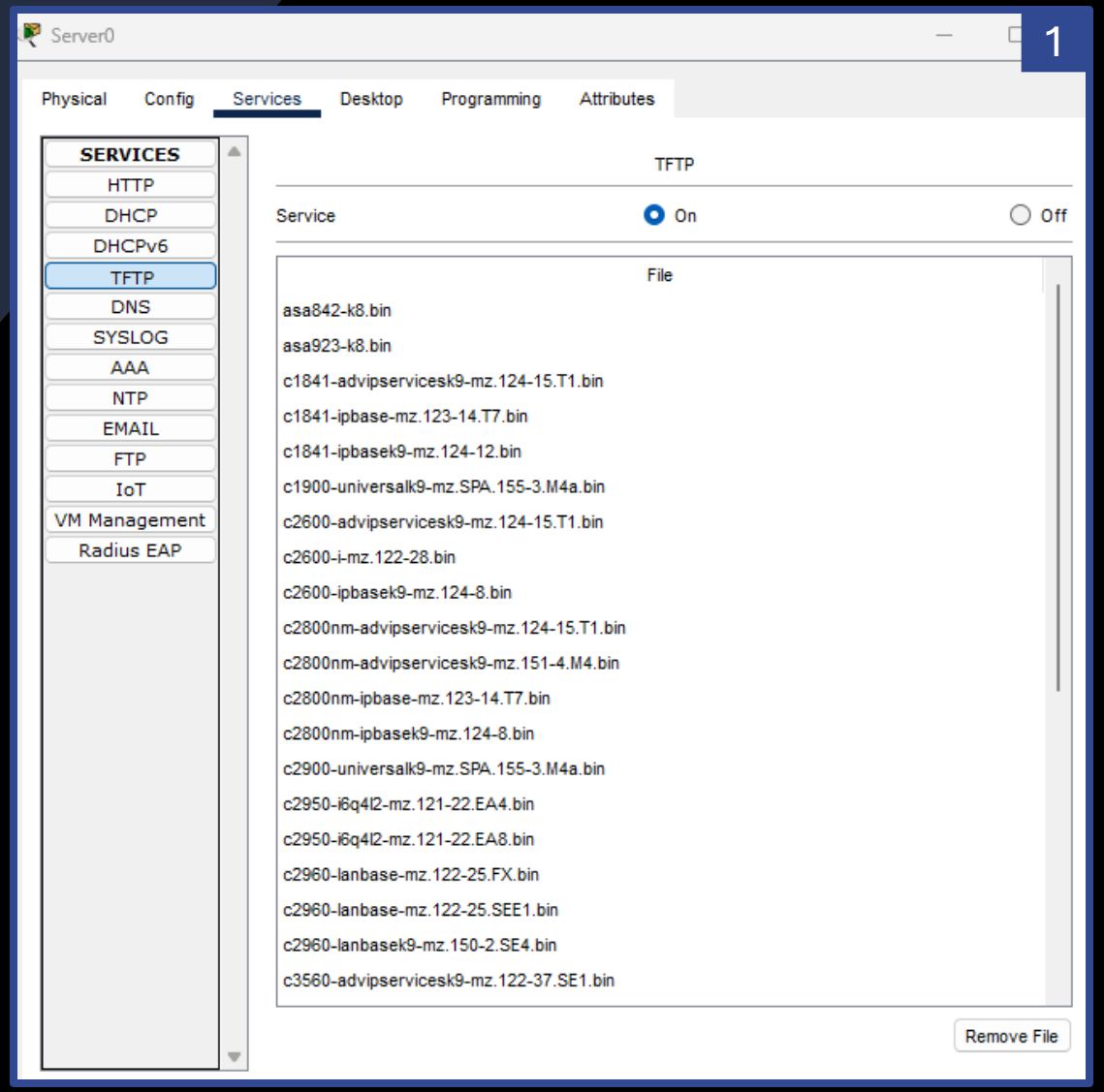
Test de connectivité

```
C:\>ping 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:

Reply from 192.168.6.2: bytes=32 time<1ms TTL=128
Reply from 192.168.6.2: bytes=32 time=1ms TTL=128
Reply from 192.168.6.2: bytes=32 time<1ms TTL=128
Reply from 192.168.6.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.6.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.6.1

Pinging 192.168.6.1 with 32 bytes of data:

Reply from 192.168.6.1: bytes=32 time<1ms TTL=255
Reply from 192.168.6.1: bytes=32 time=25ms TTL=255
Reply from 192.168.6.1: bytes=32 time<1ms TTL=255
Reply from 192.168.6.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.6.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 25ms, Average = 6ms
```

Après avoir configuré vos postes de PC et votre serveur, aller dans « **Command Prompt** » sur l'un des PC puis faites un ping vers votre serveur et vers votre commutateur.

192.168.6.1 = VLAN 1 du switch TRIOUX
192.168.6.2 = Serveur

Configuration du serveur TFTP



1: Depuis le serveur

Aller dans « **Services** » puis l'onglet « **TFTP** » et assurez-vous que la case ON est bien coché.

2: Depuis le poste de PC en mode console

```
Jimmy>show flash
Directory of flash:/

    1  -rw-     4670455          <no date>  2960-lanbasek9-mz.150-2.SE4.bin
    5  -rw-        1153          <no date>  config.text

64016384 bytes total (59344776 bytes free)
```

2

Rentrer la commande « **show flash** » pour lister les fichiers présents dans la mémoire flash.

- **Nom de l'image de configuration :** 2960-lanbasek9-mz.150-2.SE4.bin ;
- **Taille de l'image :** 4 670 455 octets (~4,5 mo).

Sauvegarder son fichier de démarrage dans le serveur TFTP

```
Jimmy>en
Password:
Jimmy#
Jimmy#
Jimmy#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Jimmy#
Jimmy#copy startup-config tftp
Address or name of remote host []? 192.168.6.2
Destination filename [Jimmy-confg]?

Writing startup-config...!!
[OK - 1153 bytes]

1153 bytes copied in 0 secs
Jimmy#
```

Rentrer la commande « **copy running-config startup-config** » qui sauvegarde la configuration en cours du switch dans la mémoire de démarrage.

Puis « **copy startup-config tftp** » suivit de l'adresse IP du serveur. Cette commande transfert le fichier sur le serveur TFTP qui nous sera utile après pour reconfigurer un switch sans refaire les étapes intermédiaires.

Restaurer le fichier de configuration de démarrage à partir du serveur TFTP

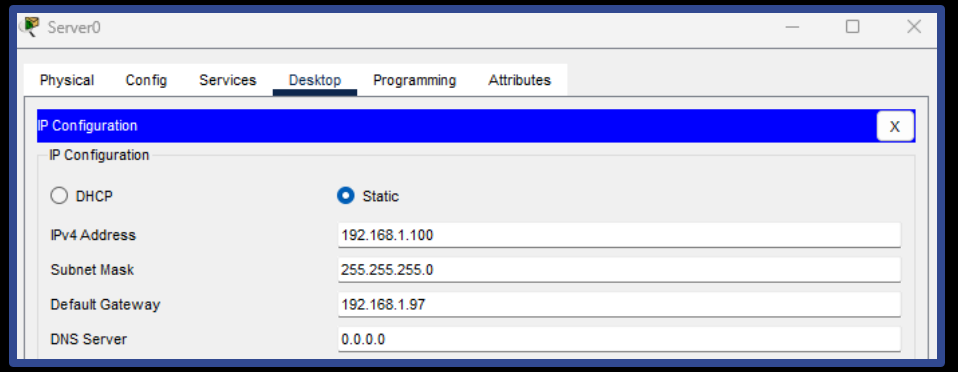
Afin de tester la restauration d'une configuration à partir d'un fichier stocké sur le serveur TFTP, nous supprimerons le switch et on en rajoutera un nouveau.

```
Switch>en
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#interface vlan 1
Switch(config-if)#
Switch(config-if)#ip address 192.168.1.102 255.255.255.224
Switch(config-if)#
Switch(config-if)#no sh

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#
Switch(config-if)#exit
Switch(config)#
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#write memory
Building configuration...
[OK]
Switch#
Switch#reload
Proceed with reload? [confirm]
```

1: A partir du PC console

Il faut ré adresser l'interface vlan 1, comme vu précédemment, sauf que les adresses IP seront différentes (**192.168.1.102** / **255.255.255.224** /27).
Puis quitter le mode de configuration terminal et retourner en mode privilégié et rentrer la commande « **write memory** » et « **reload** ».

2: Dans l'interface serveur



Affecter une nouvelle adresse IP pour le serveur. Sachant que nous avons affecté l'IP **192.168.1.102/27** alors on pourra utiliser les adresses à partir de **192.168.1.96** à **192.168.1.127**.

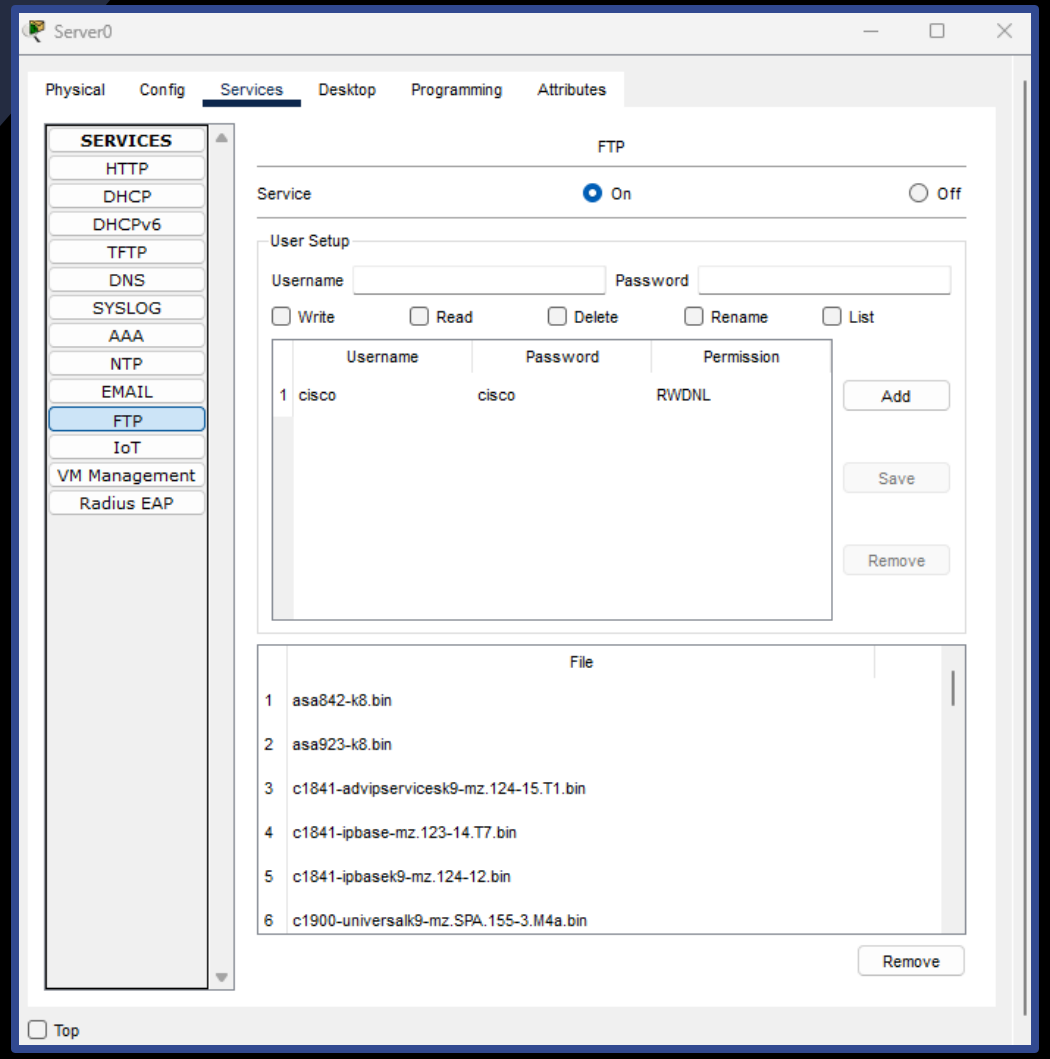
Remise en état des services

```
Switch>en
Switch#
Switch#copy tftp: startup-config
Address or name of remote host []? 192.168.1.100
Source filename []? Jimmy-confg
Destination filename [startup-config]?

Accessing tftp://192.168.1.100/Jimmy-confg....
Loading Jimmy-confg from 192.168.1.100: !
[OK - 1153 bytes]

1153 bytes copied in 3.005 secs (383 bytes/sec)
Switch#
Switch#reload
Proceed with reload? [confirm]
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: 00E0.8F6D.06C2
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 2 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4671608
flashfs[0]: Bytes available: 59344776
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:/2960-lanbasek9-mz.150-2.SE4.bin"...
#####################
```

Copier le fichier startup avec la commande « **copy tftp: startup-config** », l'adresse de votre serveur TFTP puis le nom de votre fichier.
Faites un **reload** afin de recharger la configuration, confirmer et avec la commande « **show startup-config** », regarder si vos anciens paramètres sont bien de retour.
Comme nous pouvons le voir le commutateur « **Jimmy** » s'affiche donc la configuration a été un succès.

```
Jimmy>en
Password:
Jimmy#show ru
Building configuration...

Current configuration : 1153 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Jimmy
!
enable password sio2024
!
```

BONUS : Transférer un fichier en FTP (Cisco Packet Tracer)

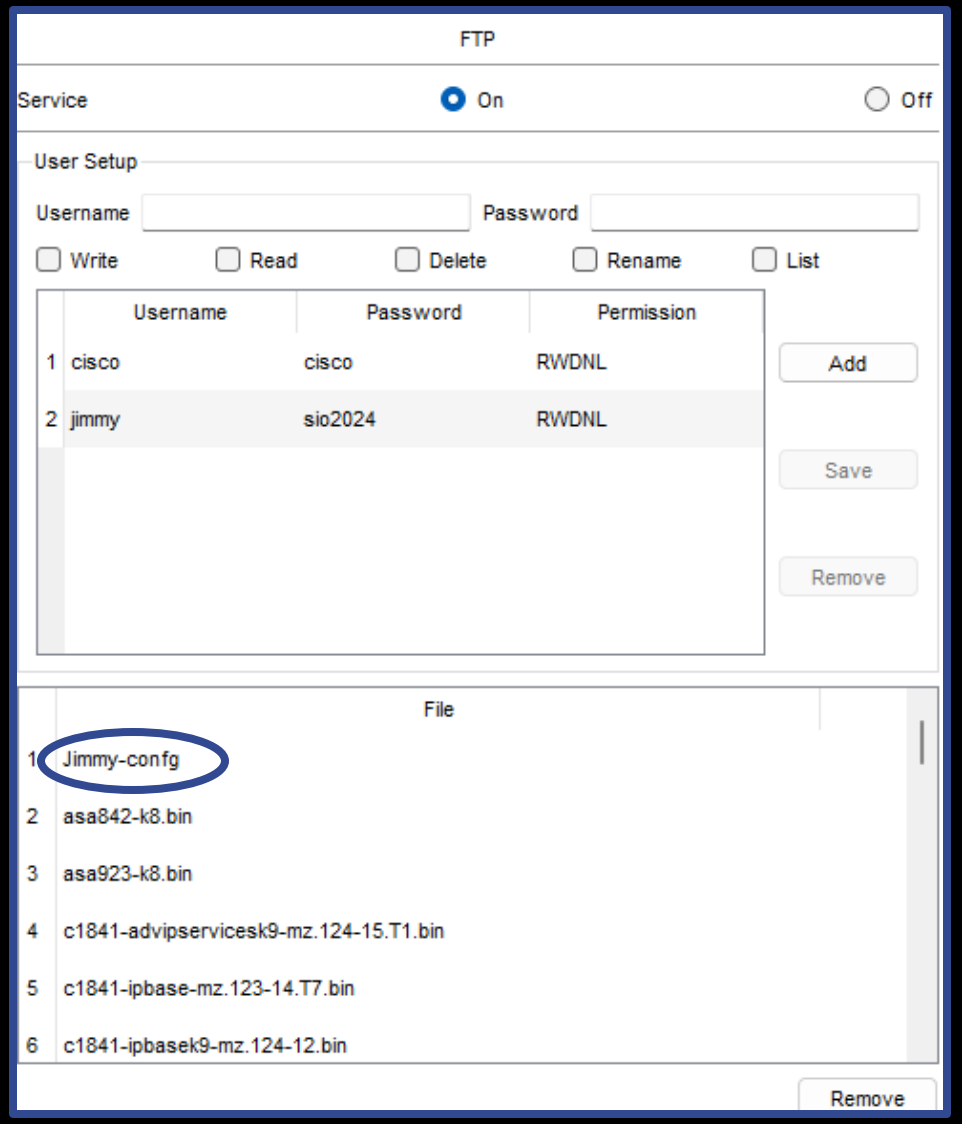



```
Jimmy#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Jimmy(config)#
Jimmy(config)#ip ftp username jimmy
Jimmy(config)#
Jimmy(config)#ip ftp password sio2024
Jimmy(config)#
```

```
Jimmy#copy running-config ftp
Address or name of remote host []? 192.168.6.2
Destination filename [Jimmy-confg]?

Writing running-config...
[OK - 1199 bytes]

1199 bytes copied in 0.088 secs (13000 bytes/sec)
Jimmy#
```

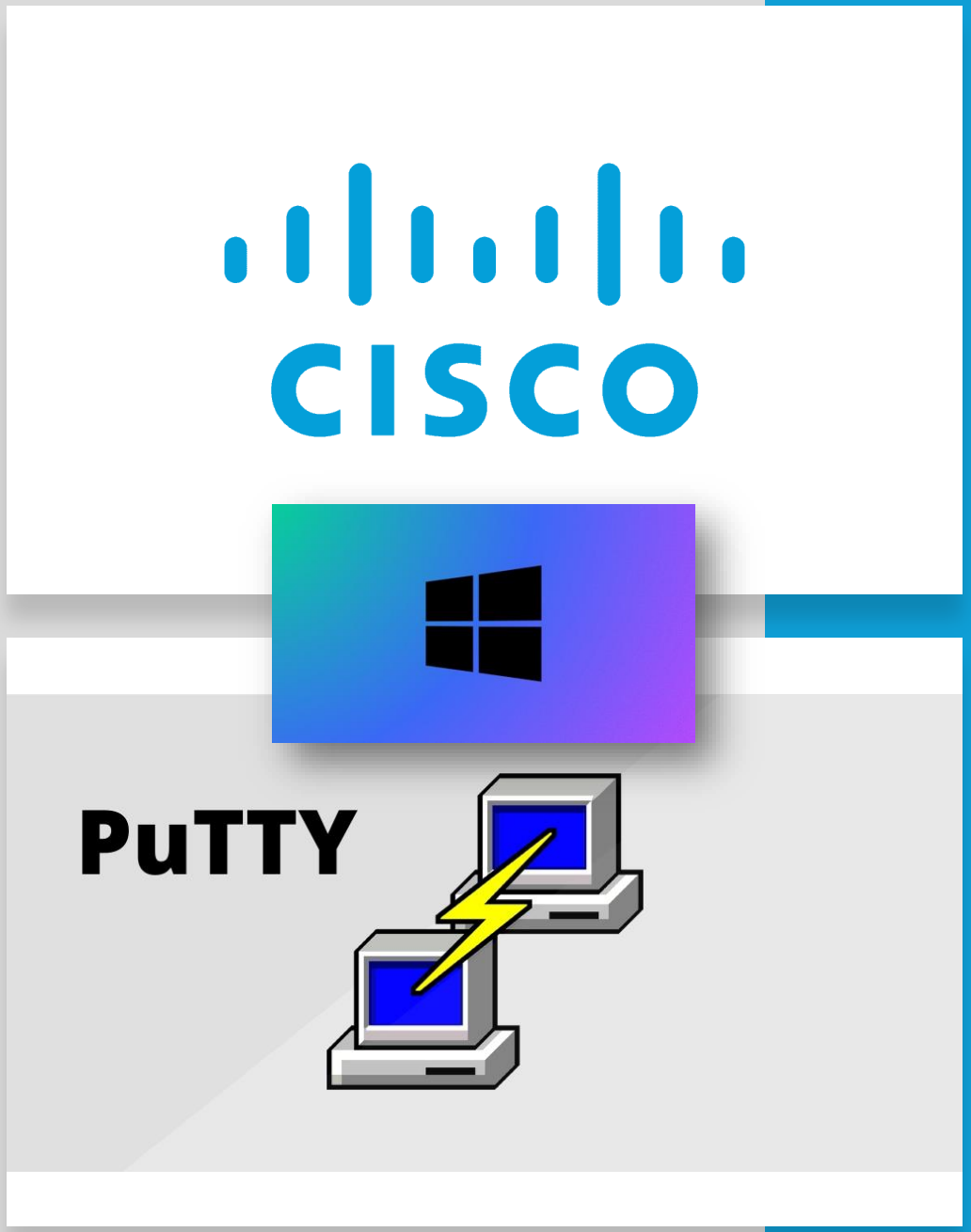
En retournant dans la partie « **Services** » du serveur, il y a un onglet « **FTP** », assurez-vous que le service est bien actif et créé un utilisateur sinon le transfert ne marchera pas.

Comme le TFTP, la commande est similaire, simplement changer « **TFTP** » par « **FTP** » à la fin de la commande et renseigner l'IP du serveur et votre fichier pourra se transférer dans votre serveur FTP.



Voici le résultat, le fichier backup de la configuration du switch est bien disponible dans mon répertoire FTP.

TP – Cisco en physique avec PuTTY sur Windows

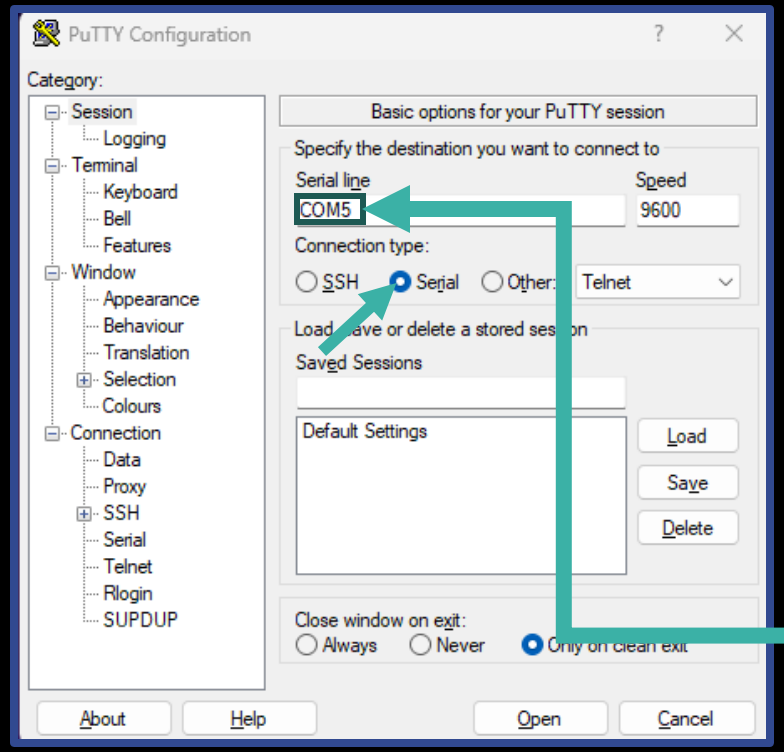


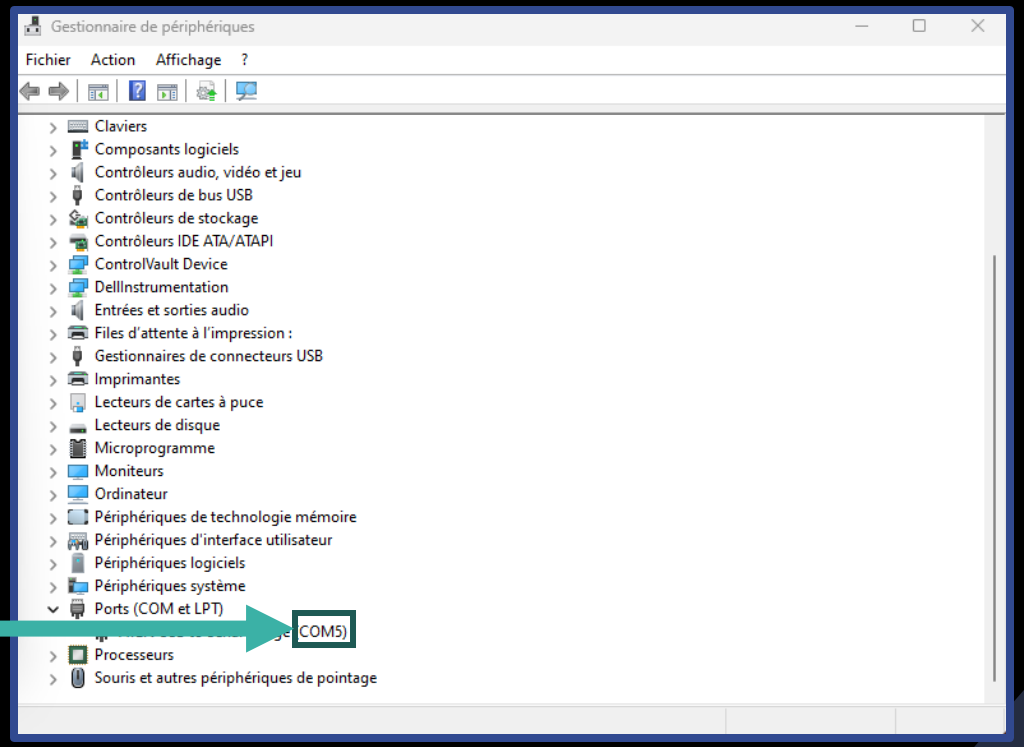
Prérequis :

- Un switch Cisco
- Un câble console
- Un adaptateur USB vers série, si vous n’avez pas de port COM sur votre PC.
- Installer le logiciel PuTTY et le pilote **UC232A** (Adaptateur USB à RS-232) si vous êtes sur Windows, en revanche ce n’est pas nécessaire sur une machine Linux.

Se connecter sur PuTTY avec le câble console

Relier le câble console du switch jusqu'à votre PC, et aller dans le logiciel PuTTY, cocher la case « **Serial** » et rentrer le n° de COM correspondant à celui dans votre gestionnaire de périphériques.
Enfin, cliquez sur « **Open** »

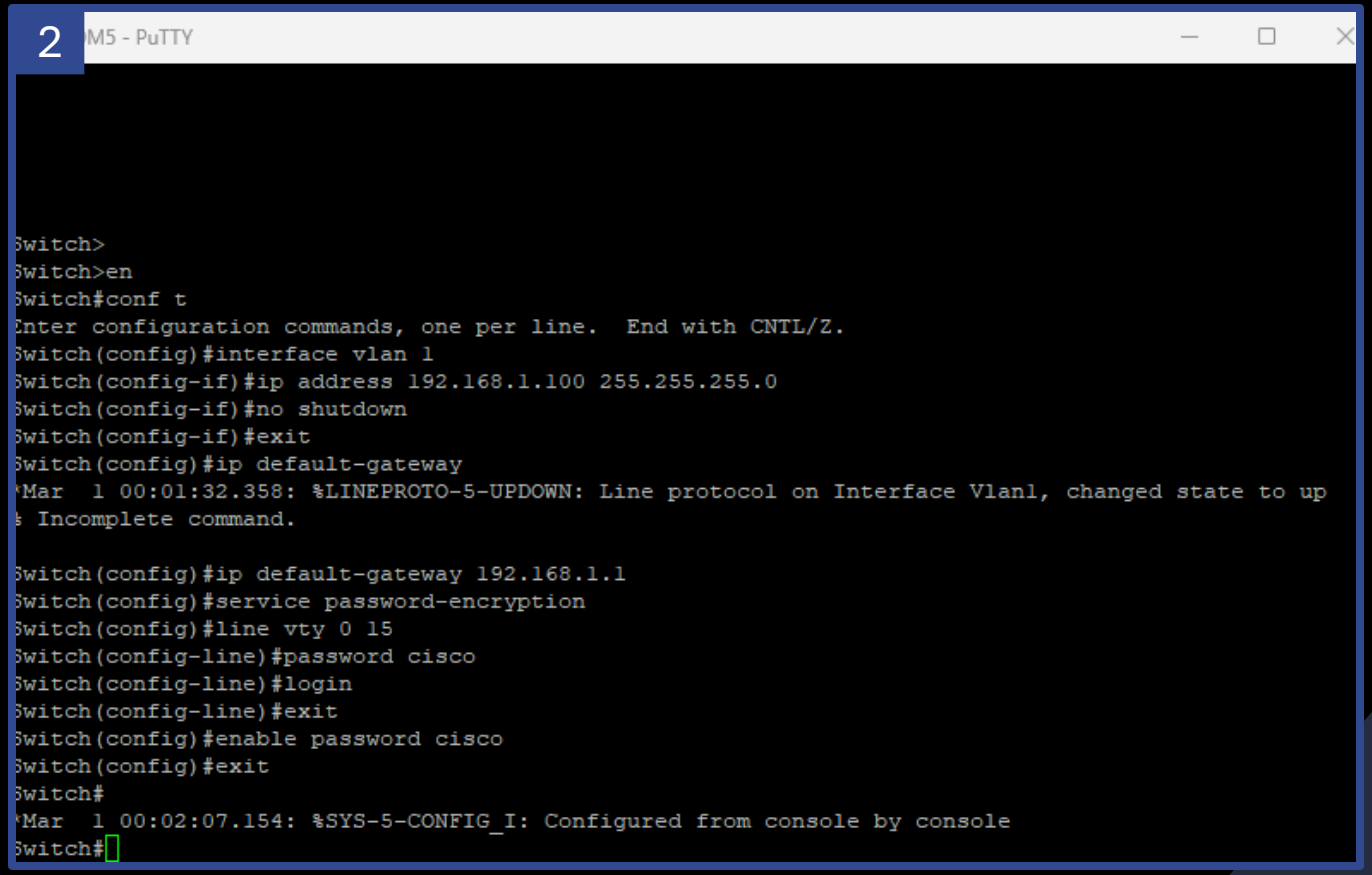




Configuration de l'interface VLAN 1 et du Telnet

1

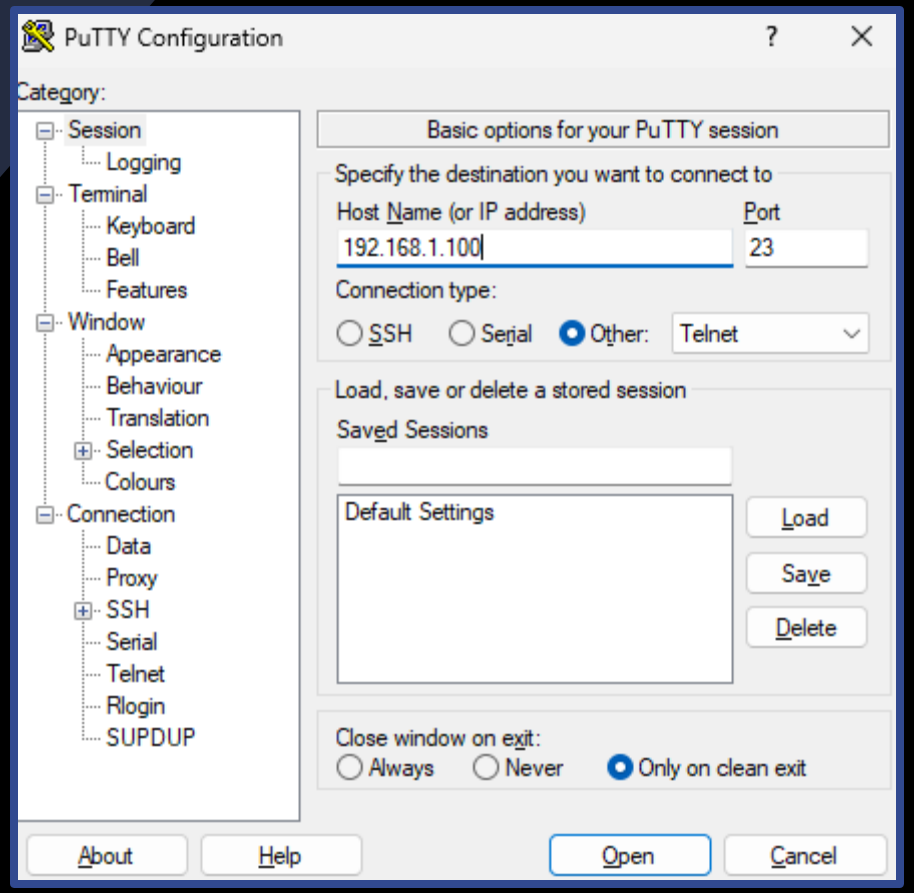
2

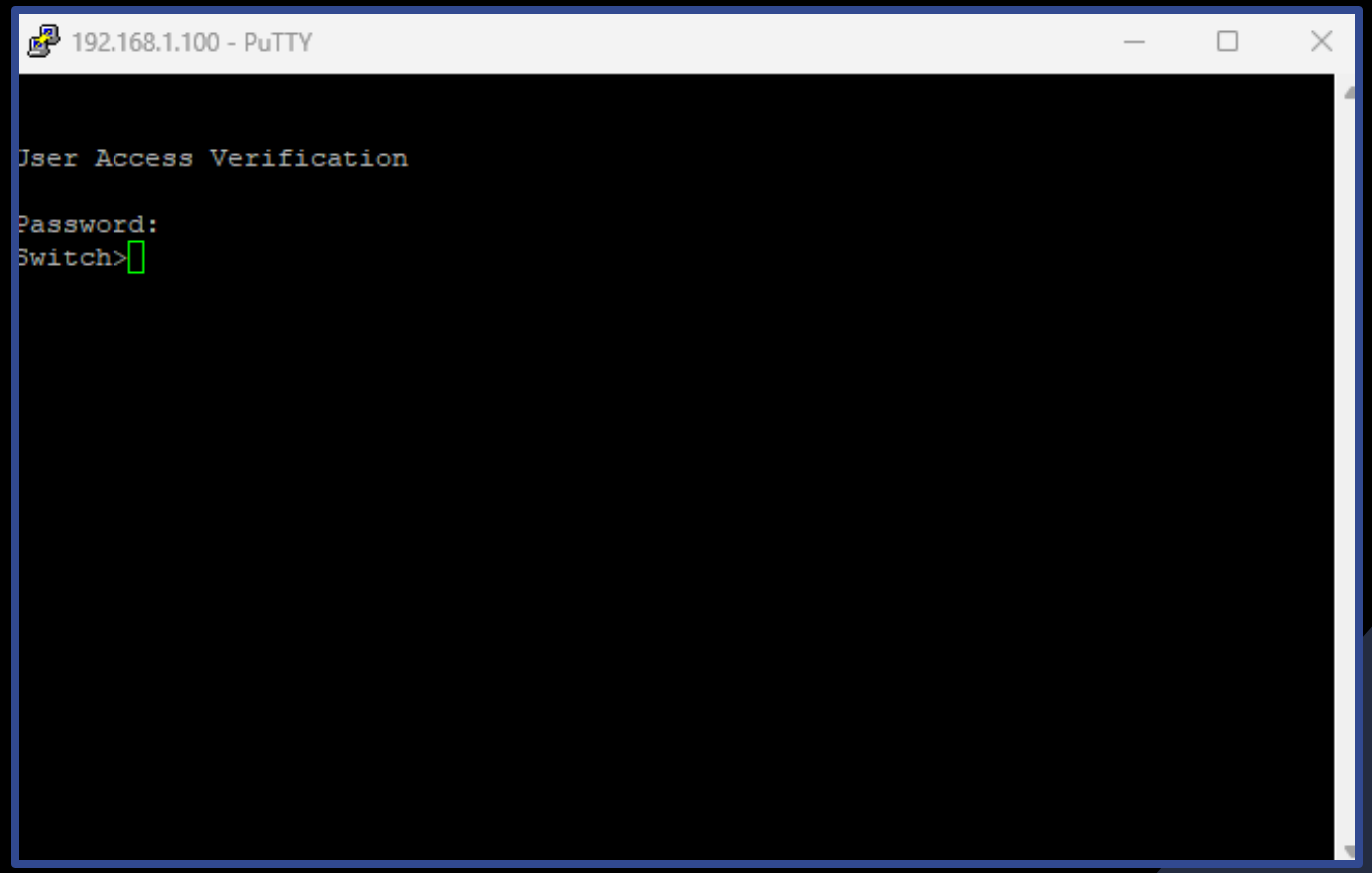


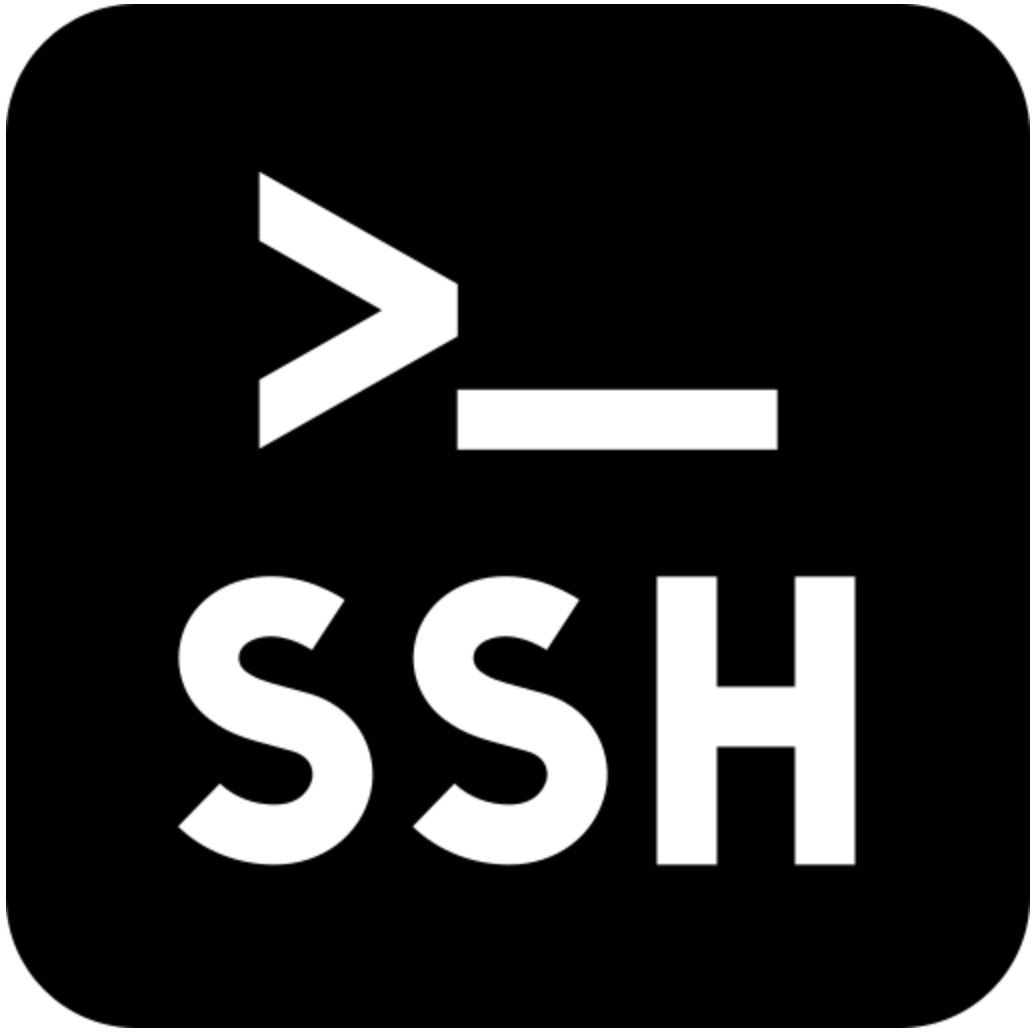
Lors du premier lancement, ou à la suite d'une réinitialisation des paramètres, on vous demandera si vous souhaitez utiliser l'assistant pour configurer. Ecrivez « **no** », nous rentrerons les commandes comme vu précédemment.

On réutilise les adresses vues dans le premier TP, de même pour Telnet, et testons la connexion en branchant un câble RJ45 vers RJ45 du PC au switch sur le port 1.

Connexion depuis Telnet sur PuTTY






SSH

Remplacer Telnet par le SSH

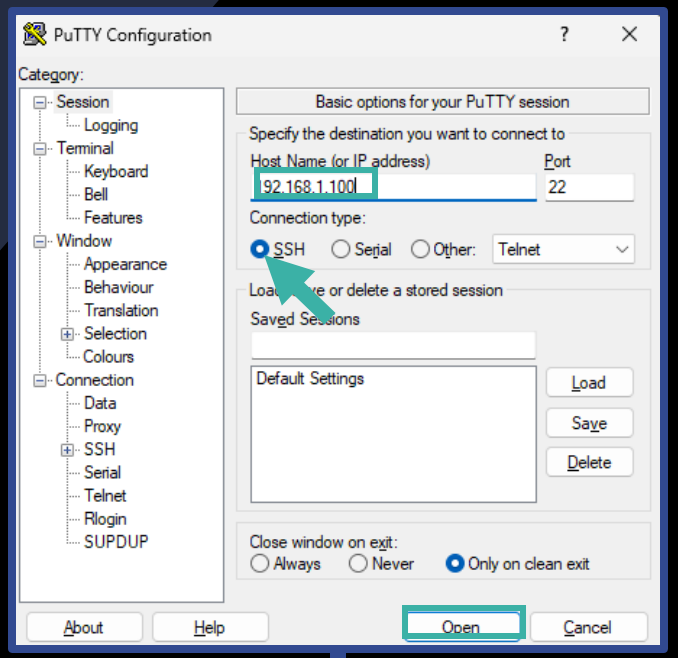
```
Switch>
Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Jimmy
Jimmy(config)#ip domain-name trioux.com
Jimmy(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Jimmy.trioux.com

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

*Mar  1 00:07:03.238: %SSH-5-ENABLED: SSH 1.99 has been enabled
Jimmy(config)#ip ssh version 2
Jimmy(config)#ip ssh logging events
Jimmy(config)#ip ssh time-out 60
Jimmy(config)#ip ssh authentication-retries 3
Jimmy(config)#username admin secret cisco
Jimmy(config)#line vty 0 15
Jimmy(config-line)#login local
Jimmy(config-line)#transport input ssh
Jimmy(config-line)#exit
Jimmy(config)#exit
Jimmy#
*Mar  1 00:08:01.967: %SYS-5-CONFIG_I: Configured from console by console
Jimmy#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 3
Jimmy#
```

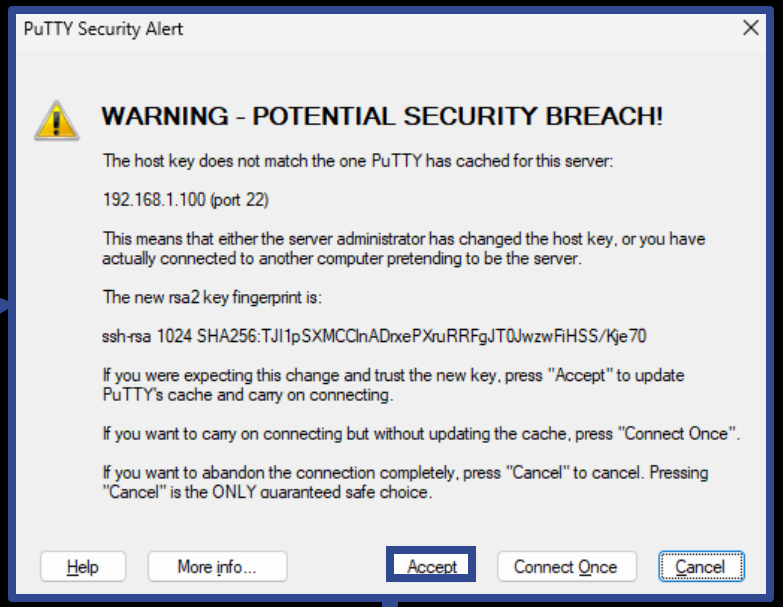
Retournez en configuration terminal, on affecte un hostname et un nom de domaine puis on génère une clé de cryptage.

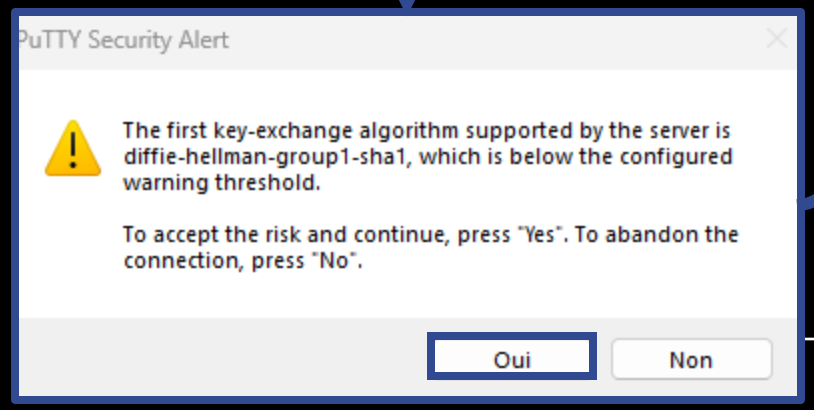
Enfin, on retourne dans la ligne vty 0 15 et on ajoute « **login local** » et « **transport input ssh** » et quitter.

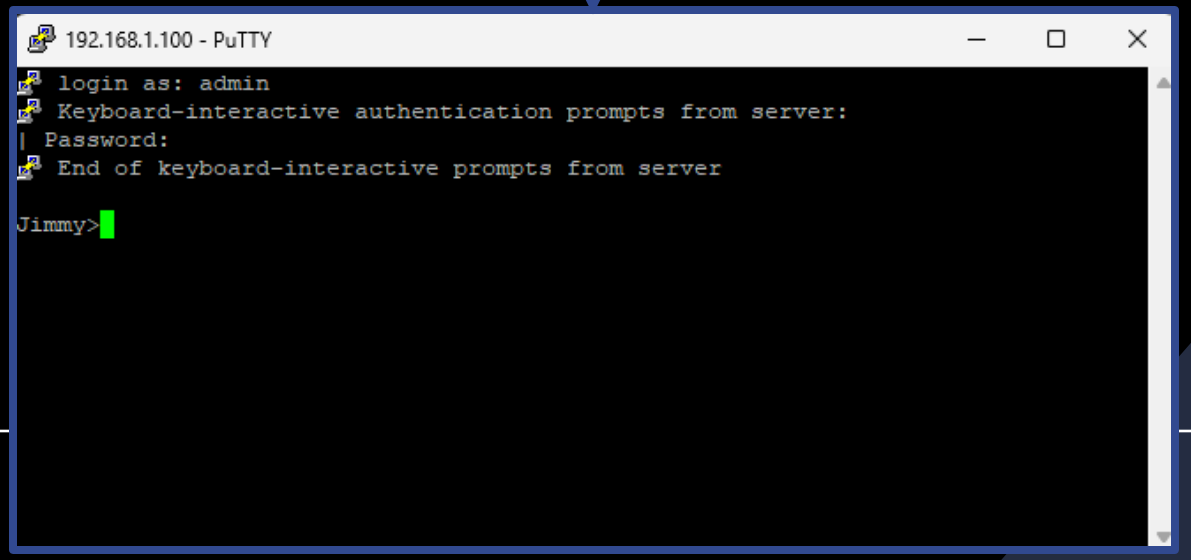
Vérifier avec la commande **show ip ssh**.

Connexion en SSH sur PuTTY

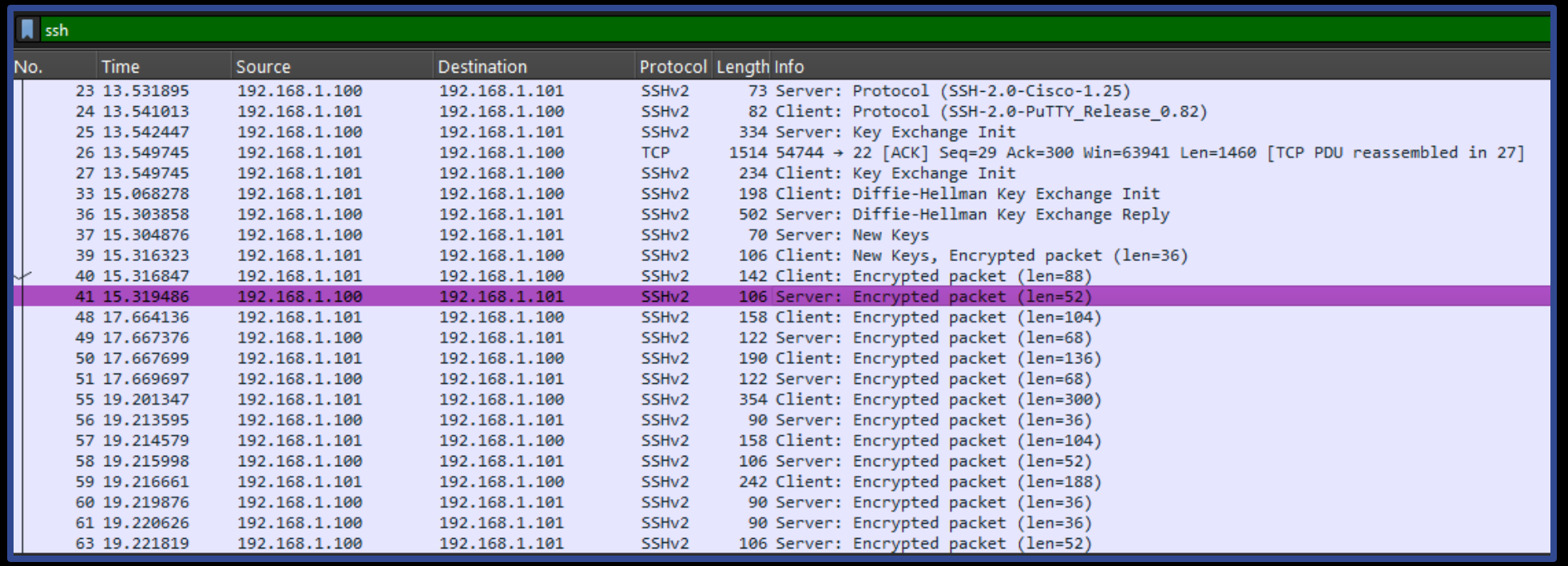








Sniffage d’une trame SSH sur Wireshark



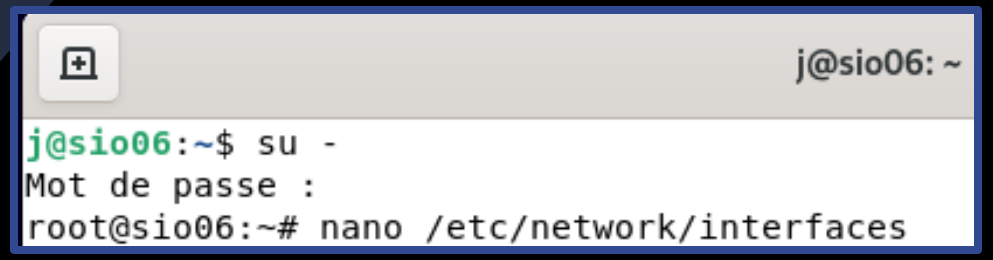
ssh

No.	Time	Source	Destination	Protocol	Length	Info
23	13.531895	192.168.1.100	192.168.1.101	SSHv2	73	Server: Protocol (SSH-2.0-Cisco-1.25)
24	13.541013	192.168.1.101	192.168.1.100	SSHv2	82	Client: Protocol (SSH-2.0-PuTTY_Release_0.82)
25	13.542447	192.168.1.100	192.168.1.101	SSHv2	334	Server: Key Exchange Init
26	13.549745	192.168.1.101	192.168.1.100	TCP	1514	54744 → 22 [ACK] Seq=29 Ack=300 Win=63941 Len=1460 [TCP PDU reassembled in 27]
27	13.549745	192.168.1.101	192.168.1.100	SSHv2	234	Client: Key Exchange Init
33	15.068278	192.168.1.101	192.168.1.100	SSHv2	198	Client: Diffie-Hellman Key Exchange Init
36	15.303858	192.168.1.100	192.168.1.101	SSHv2	502	Server: Diffie-Hellman Key Exchange Reply
37	15.304876	192.168.1.100	192.168.1.101	SSHv2	70	Server: New Keys
39	15.316323	192.168.1.101	192.168.1.100	SSHv2	106	Client: New Keys, Encrypted packet (len=36)
40	15.316847	192.168.1.101	192.168.1.100	SSHv2	142	Client: Encrypted packet (len=88)
41	15.319486	192.168.1.100	192.168.1.101	SSHv2	106	Server: Encrypted packet (len=52)
48	17.664136	192.168.1.101	192.168.1.100	SSHv2	158	Client: Encrypted packet (len=104)
49	17.667376	192.168.1.100	192.168.1.101	SSHv2	122	Server: Encrypted packet (len=68)
50	17.667699	192.168.1.101	192.168.1.100	SSHv2	190	Client: Encrypted packet (len=136)
51	17.669697	192.168.1.100	192.168.1.101	SSHv2	122	Server: Encrypted packet (len=68)
55	19.201347	192.168.1.101	192.168.1.100	SSHv2	354	Client: Encrypted packet (len=300)
56	19.213595	192.168.1.100	192.168.1.101	SSHv2	90	Server: Encrypted packet (len=36)
57	19.214579	192.168.1.101	192.168.1.100	SSHv2	158	Client: Encrypted packet (len=104)
58	19.215998	192.168.1.100	192.168.1.101	SSHv2	106	Server: Encrypted packet (len=52)
59	19.216661	192.168.1.101	192.168.1.100	SSHv2	242	Client: Encrypted packet (len=188)
60	19.219876	192.168.1.100	192.168.1.101	SSHv2	90	Server: Encrypted packet (len=36)
61	19.220626	192.168.1.100	192.168.1.101	SSHv2	90	Server: Encrypted packet (len=36)
63	19.221819	192.168.1.100	192.168.1.101	SSHv2	106	Server: Encrypted packet (len=52)

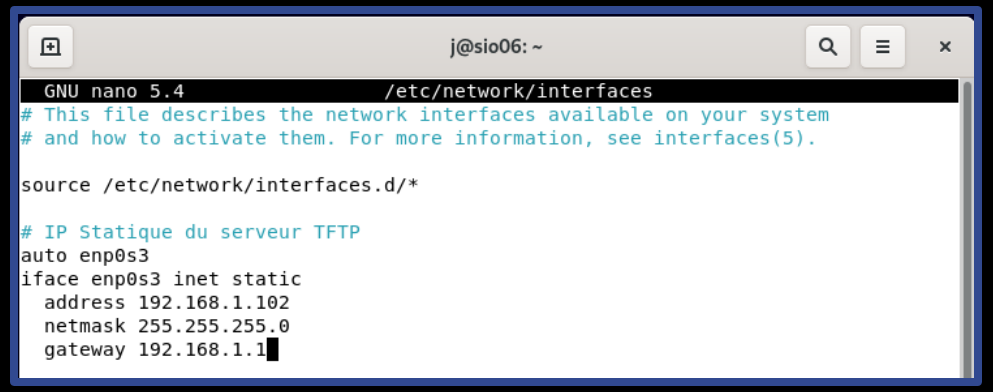
J’ai sniffé la trame de mon protocole SSH, la connexion vers mon serveur est bien encryptée donc quelqu’un de malveillant ne pourrait ni récupérer les identifiants, ni les mots de passe en utilisant cet outil.


TFTP

Configuration du serveur TFTP sur Debian 11



Mettez-vous en superutilisateur puis aller dans le répertoire d'interface réseau (nano /etc/network/interfaces)



On se met en statique puis on rentre l'adresse IP du serveur, son masque et sa passerelle.

Relancer le réseau, mettez à jour les paquets puis installer tftpd avec la commande « **apt install tftpd-hpa –y** ».
Puis « **nano /etc/default/tftpd-hpa** » permet de se rendre dans le fichier de configuration du serveur.

Création du dossier « tftp » et permissions

```
j@sio06: ~
  GNU nano 5.4                    /etc/default/tftpd-hpa
# /etc/default/tftpd-hpa

TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/srv/tftp"
TFTP_ADDRESS="0.0.0.0:69"
TFTP_OPTIONS="--secure --create"
```

Il est important de modifier la ligne **TFTP_ADDRESS=« 0.0.0.0:69 »** comme ceci car **l'adresse IP 0.0.0.0** permet au serveur TFTP d'écouter sur toutes les interfaces réseaux disponibles sur la machine et préciser « **--secure –create** » dans la ligne **TFTP_OPTIONS**. Autrement, si vous souhaitez le limiter alors remplacer les 0 par l'adresse IP souhaitée. Le port 69 est le port standard pour le protocole TFTP. Sauvegarder et quitter.

On crée le dossier tftp, on affecte les droits pour l'utilisateur TFTP et son groupe

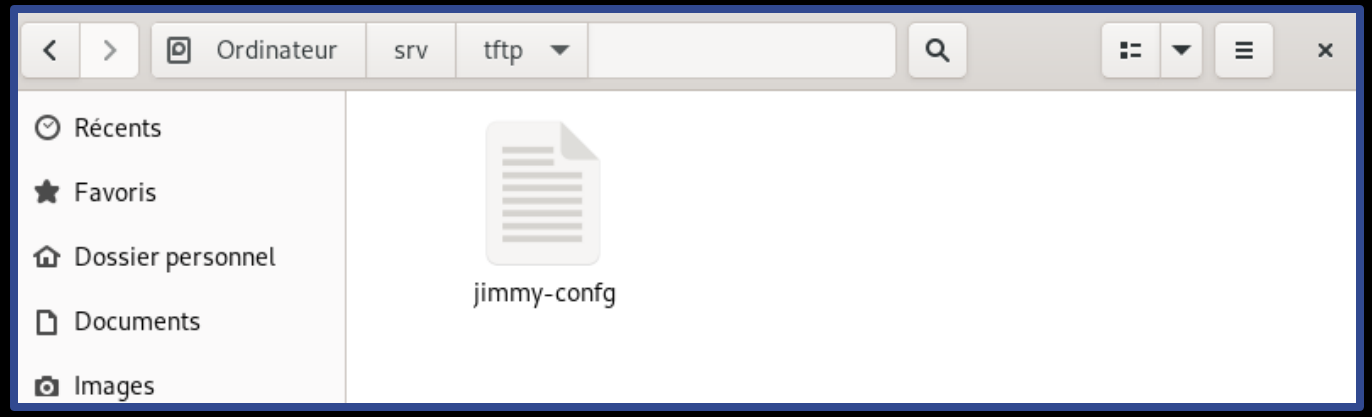
```
root@sio06:~# mkdir -p /srv/tftp
root@sio06:~#
root@sio06:~# chown -R tftp:tftp /srv/tftp
root@sio06:~#
root@sio06:~# chmod -R 755 /srv/tftp
```

```
root@sio06:~# systemctl restart tftpd-hpa
root@sio06:~# systemctl enable tftpd-hpa
tftpd-hpa.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable tftpd-hpa
root@sio06:~# systemctl status tftpd-hpa
● tftpd-hpa.service - LSB: HPA's tftp server
     Loaded: loaded (/etc/init.d/tftpd-hpa; generated)
     Active: active (running) since Mon 2025-01-20 20:32:32 CET; 14s ago
       Docs: man:systemd-sysv-generator(8)
      Tasks: 1 (limit: 14058)
     Memory: 436.0K
        CPU: 34ms
     CGroup: /system.slice/tftpd-hpa.service
             └─3108 /usr/sbin/in.tftpd --listen --user tftp --address 0.0.0.0:6>

janv. 20 20:32:32 sio06 systemd[1]: Starting LSB: HPA's tftp server...
janv. 20 20:32:32 sio06 tftpd-hpa[3100]: Starting HPA's tftpd: in.tftpd.
janv. 20 20:32:32 sio06 systemd[1]: Started LSB: HPA's tftp server.
lines 1-13/13 (END)
```

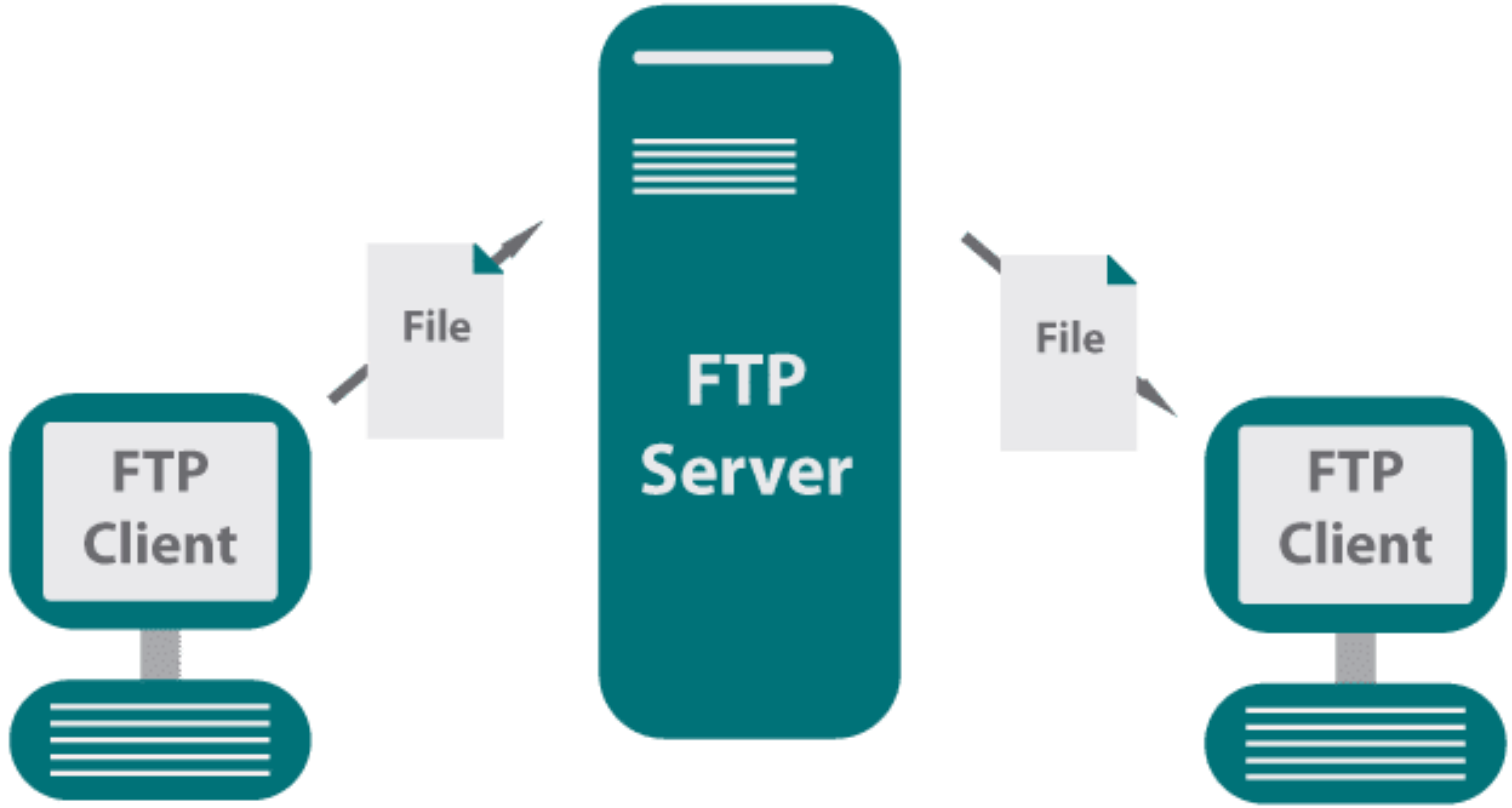
Relancer TFTPD, activer le à chaque démarrage puis vérifier si l'état du serveur est actif.

Envoi du fichier backup du switch vers le serveur TFTP

```
Jimmy#copy running-config tftp:
Address or name of remote host []? 192.168.1.102
Destination filename [jimmy-confg]?
!!
1118 bytes copied in 0.302 secs (3702 bytes/sec)
Jimmy#
```

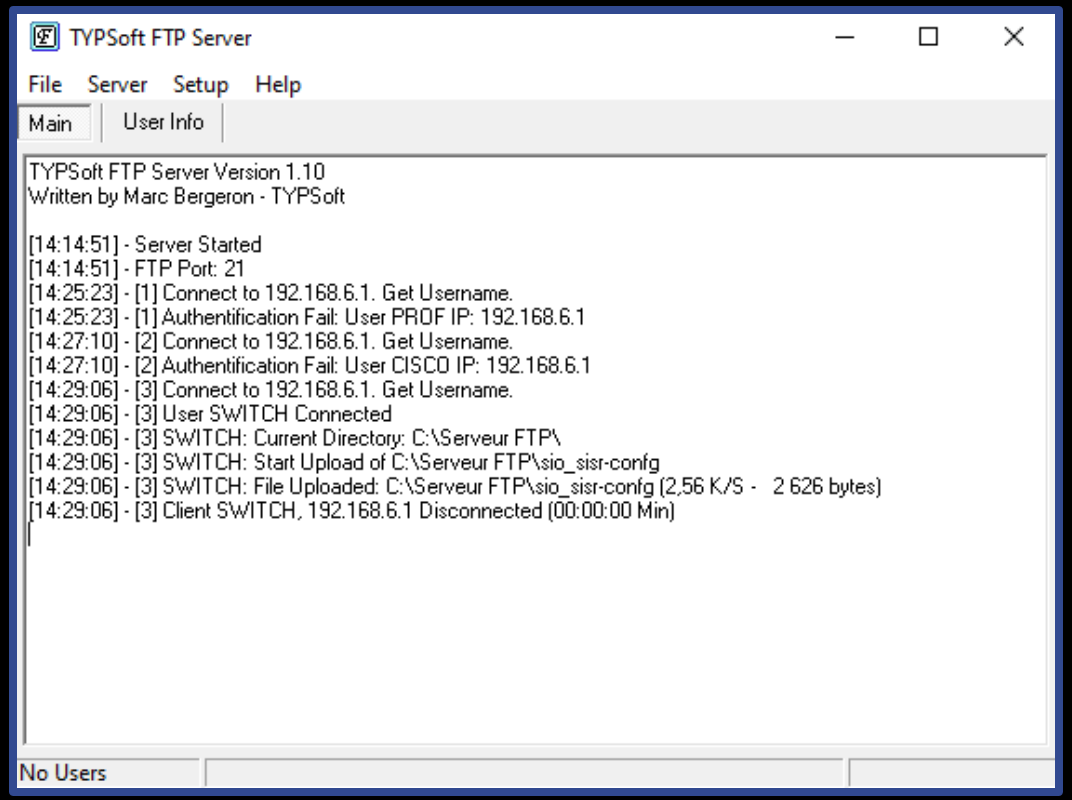


Comme vu précédemment, on rentre la commande permettant de copier vers le serveur TFTP, renseignez l'adresse IP du serveur et quand vous retournerez sur votre machine virtuelle dans le répertoire « **/srv/tftp** » vous pourrez y retrouver votre fichier backup.


File
FTP
Client
FTP
Server
File
FTP
Client

Configuration de l'utilisateur et copie du fichier vers le serveur FTP

Pour configurer votre serveur FTP, réitérez-vous à ce TP.



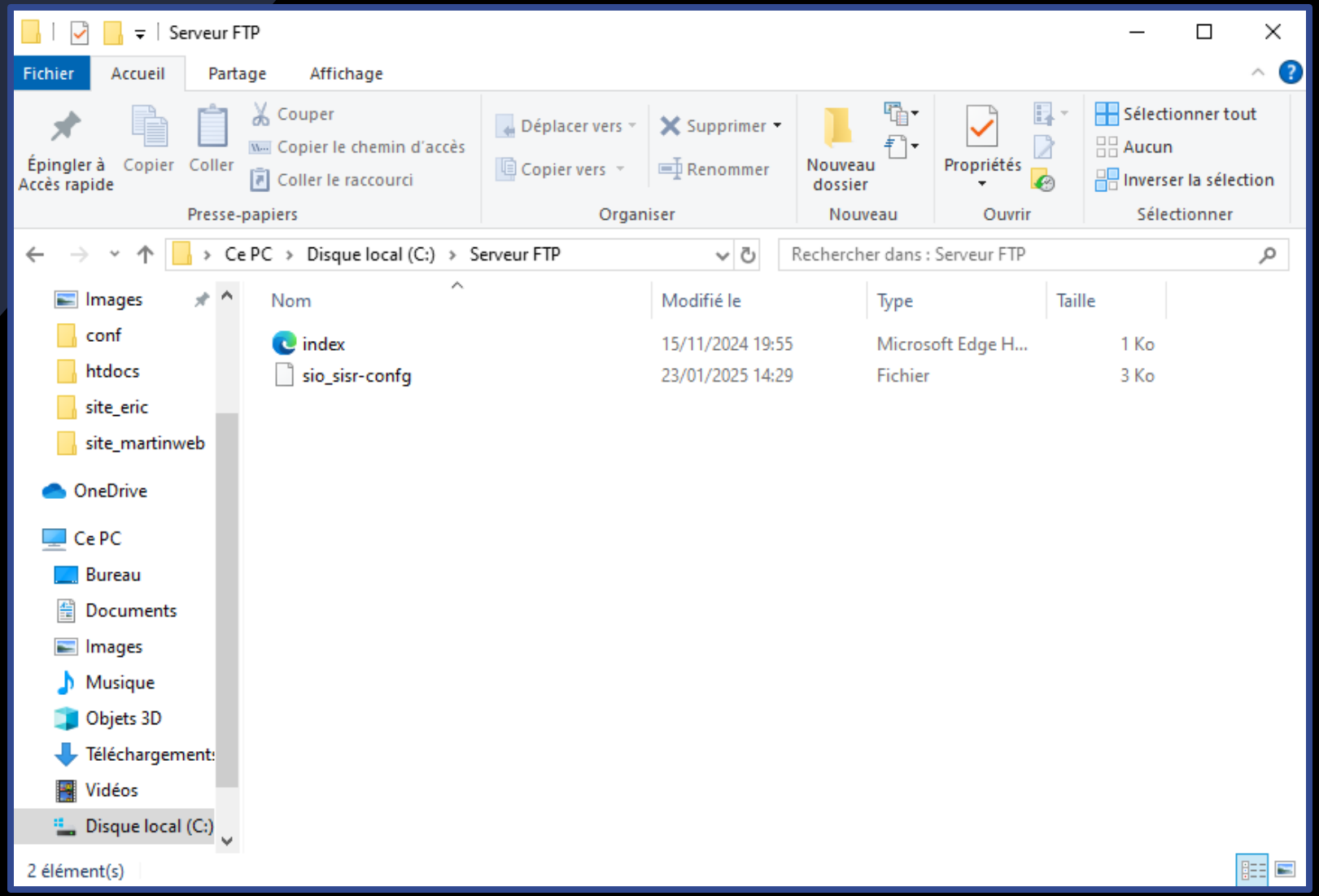

```
SIO_SISR(config)#ip ftp username switch
SIO_SISR(config)#
SIO_SISR(config)#ip ftp password cisco
SIO_SISR(config)#exit
SIO_SISR#copy running-config ftp:
Address or name of remote host []? 192.168.6.61
Destination filename [sio_sisr-confg]?
Writing sio_sisr-confg !
2626 bytes copied in 0.730 secs (3597 bytes/sec)
SIO_SISR#
```

Passer en mode de configuration terminal puis tapez les deux commandes « **ip ftp username/password** » sont essentielles puisqu'elles servent à configurer les informations d'identification.

Puis quittez et tapez la commande "**running-config ftp**" suivit de l'**adresse IP de votre serveur FTP** et votre fichier sera transférer.

Nous pouvons voir dans les logs du serveur FTP, le fichier a correctement été copié.

Résultat



Le transfert du fichier backup du switch vers mon serveur FTP sur une VM Windows 10 que j'ai réutilisais d'un précédemment TP fonctionne parfaitement !