Quimper	**Modèle OSI** **Prise à distance d'un élément réseau** **Communiquer et paramétrer un élément réseau** **Accès Sécurisé des réseaux**	**Travaux pratiques**

NOM: Lucas ALVES ROSA

OBJECTIFS :

- Comprendre le modèle OSI
- Prendre la main sur un élément du réseau en local ou à distance.
- Paramétrer un élément afin de l'insérer dans un réseau
- Configurer un élément selon un cahier des charger
- Utiliser différents protocoles de communications et leurs ports associés
- Sécuriser les communications entre 2 éléments

RESSOURCES:

- Vidéos

MISE EN SITUATION

SITUATION :

Vous êtes administrateur réseau dans l'entreprise SIO, et l'on vous demande de faire un état des lieux des accès réseaux et de sécuriser les accès au matériel réseau.
La protection des configurations des switchs est importante, elle évite les attaques de déni de service, limitation de débit, sécurise les données échangées...

TRAVAIL PERSONNEL MAISON :

✔ Indiquer à quelle couche du modèle OSI correspond la configuration et la sécurisation des switchs ?

Consulter les vidéos sur le modèle OSI :

https://www.youtube.com/watch?v=YG57te3jqE8

https://www.youtube.com/watch?v=t3NZsApAfQA

Couche 2 (Classique) et Couche 3 (Administratif)

7	Application
6	Présentation
5	Session
4	Transport
3	Réseau
2	Liaison
1	Physique

Le modèle OSI

Consultez ce site **https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006149839/2008-11-05/** pour répondre aux questions ci dessous :

✔ Trouvez la peine encourue pour le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données : **2 ans de prison et 30000 euros d'amende.**

› **Article 323-3** Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 () JORF 22 juin 2004

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Versions Liens relatifs

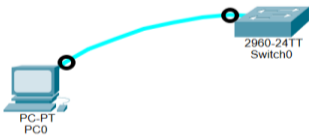
✔ Citez le numéro de l'article de loi en vigueur concernant ce méfait : **Loi 323-1 du Code Pénal**

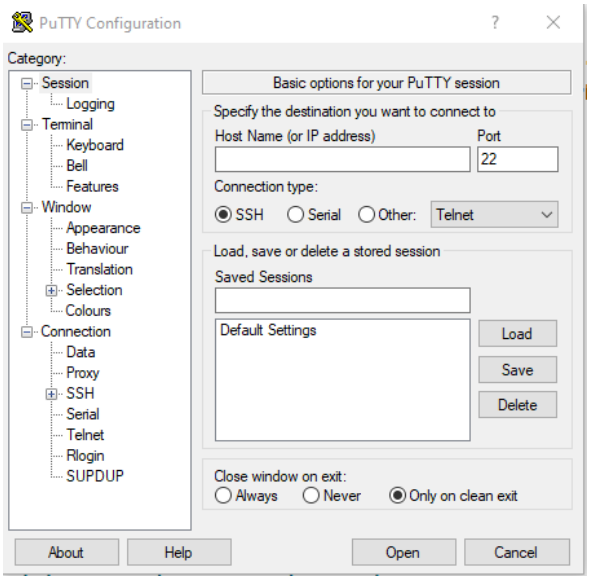
Plan de traitement des risques :

De nombreux moyens techniques peuvent être mis en œuvre pour assurer une sécurité du système d'information.
Il convient de choisir les moyens nécessaires, suffisants, et justes.
Voici une liste non exhaustive de moyens techniques pouvant répondre à certains besoins en matière de sécurité du système d'information :

1. Marquer les SI (Systèmes d'information)
2. Contrôle des accès au système d'information ;
3. Surveillance du réseau : sniffer, système de détection d'intrusion ;
4. Sécurité applicative : séparation des privilèges, audit de code, rétro-ingénierie ;
5. Emploi de technologies *ad hoc* : pare-feu, UTM, anti-logiciels malveillants (antivirus, anti-spam, anti-logiciel espion) ;
6. Cryptographie : authentification forte, infrastructure à clés publiques, chiffrement.
7. Plan de continuité d'activité : sauvegarde et restauration de données, Plan de Reprise d'activité.

TRAVAIL DEMANDE : On désire dans un premier temps communiquer avec le switch de niveau 2 (configurable).
Nous allons dans un premier temps prendre la main sur cet élément par une liaison série que nous allons configurer.





Installer le logiciel PUTTY sur votre ordinateur et lancer l'application.

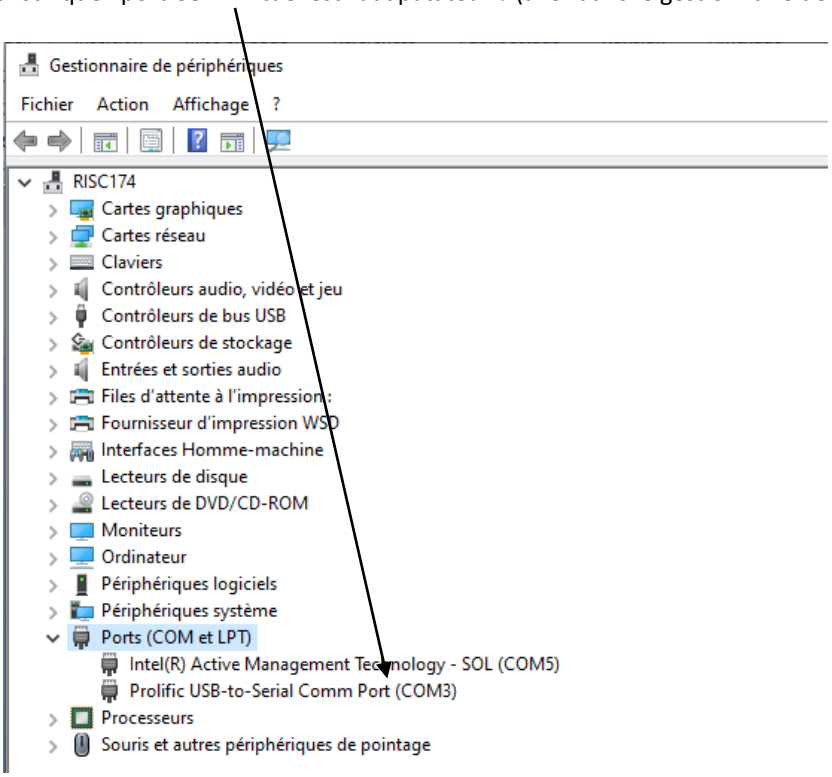
PuTTY est un émulateur de terminal doublé d'un client pour les protocoles SSH, Telnet, rlogin, et TCP brut.
Il permet également des connexions directes par liaison série RS-232.
À l'origine disponible uniquement pour Windows, il est à présent porté sur diverses plates-formes Unix

Caractéristiques :

- Est portable. Aucune installation n'est nécessaire;
  il suffit de lancer l'exécutable téléchargé pour l'utiliser.
- Conserve les paramétrages des hôtes et leurs préférences pour une utilisation ultérieure.
- Comprend un client SFTP en ligne de commande appelé psftp.
- Contrôle la clé de chiffrement et la version du protocole SSH.
- Permet le contrôle de la translation de port sur SSH en dynamique, local et distant.
- Prend en charge IPv6.
- Gère les chiffrements Data Encryption Standard
- Gère l'authentification par clé publique.
- Gère les protocoles Telnet, SSH et rlogin, ainsi que les liaisons RS-232.

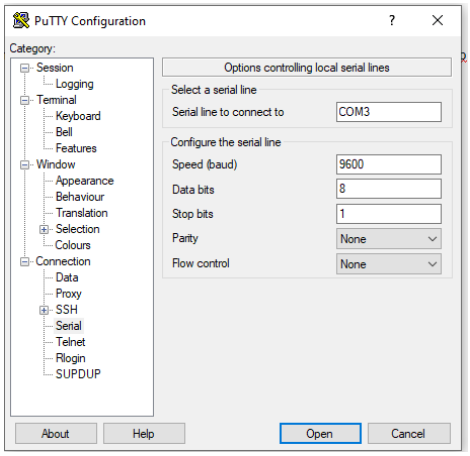
Sécuriser l'accès au switch par mot de passe mode console:

- ✔ Raccorder le port console du switch à l'adaptateur USB série.
- ✔ Repérer sur quel port COM virtuel est l'adapatateur ? (aller dans le gestionnaire de périphériques)

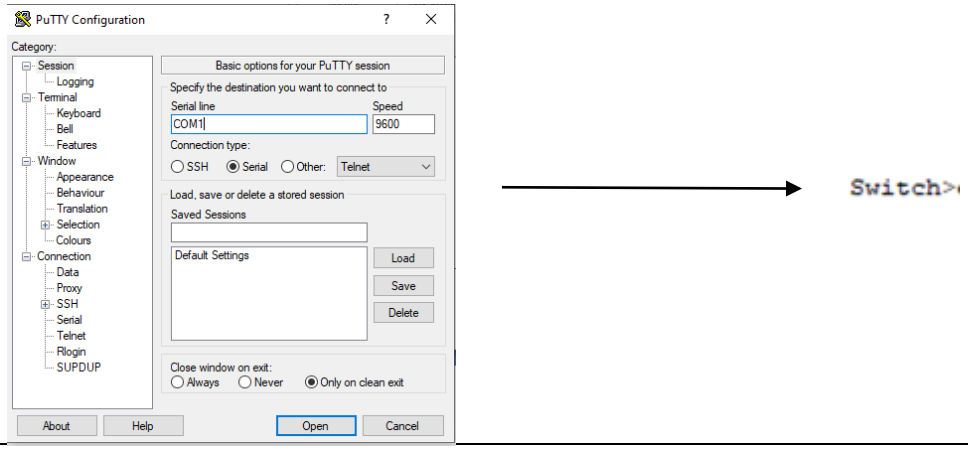


C'est généralement COM1, mais j'ai changé plusieurs fois de postes.

- ✔ Paramétrer la liaison série comme ci-dessous en y indiquant le numéro de port utilisé :



- ✔ Lancer une communication par le logiciel putty (en sélectionant sérial / en y indiquant le numero du port série)



✔ Autoriser une communication avec le switch ? Un mot de passe est il demandé ?

```
Switch>ena
Switch#
```

✔ Visualiser la configuration du switch avec la commande show run (ou show running-config) ? Est il configuré ?

Non, il n'est pas configuré.

COM4 - PuTTY

```
% Unknown command or computer name, or unable to find computer address
Switch>ena
Switch#
Switch#show run
Building configuration...

Current configuration : 1305 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
ip domain-name thepot
!
!

Switch#
```

Instal

✔

switch>en
switch#conf t
switch(config)#**banner motd !ACCES RESERVE PRIVE !**

```
Switch#ena
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#banner motd !ACCES RESERVE PRIVE!
Switch(config)#^Z
```

Vérification par la commande show run: ❑ Valider par une croix

Installer les accès sécurisés distincts

✔ Donner un nom à l'équipement pour le repérer dans le réseau (THEPOT) :

```
switch>ena
switch#conf t
switch(config)#hostname THEPOT - FLYHER
```

```
THEPOT-FLYHER#show run
Building configuration...

Current configuration : 1412 byte
!
version 12.2
no service pad
service timestamps debug datetime
service timestamps log datetime m
no service password-encryption
!
hostname THEPOT-FLYHER
!
```

Vérifier que le switch est bien passé en THEPOT au niveau du prompt: ❑ Valider par une croix

✔ Afin de lancer une communication future avec le switch, nous allons configurer un mot de passe et un login pour l'accès standard etudiant et root (enable) admin au switch de la manière suivante :
login etudiant/ mdp : Thepot20XX et login admin / mdp : Rootthepot20XX.

```
switch>ena
switch#conf t
switch(config)#username etudiant password thepot2026
switch(config)#username admin privilege 15 secret Rootthepot2026
```

```
THEPOT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
THEPOT(config)#username etudiant password Thepot2022
THEPOT(config)#username admin privilege 15 secret Rootthepot2022
THEPOT(config)#exit
THEPOT#s
*Mar  3 00:27:01.594: %SYS-5-CONFIG_I: Configured from console by consolehow run
Building configuration...

Current configuration : 1410 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname THEPOT
!
boot-start-marker
boot-end-marker
!
!
username etudiant password 0 Thepot2022
username admin privilege 15 secret 5 $1$aa8H$dAdjS1oCU4VH3bUnHv5bU/
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
```

Vérifier par la commande show run la prise en compte de ces 2 comptes: ❑ Valider par une croix
Que constatez vous?

```
username alves password 0 Thepot2026
username admin privilege 15 secret 5 $1$xPnO$EPpBbp6LO287.Q/wyNHMf.
no aaa new-model
```

Le mot de passe d'Admin est crypté alors que le mot de passe d'Alves est visible dans le show run

✔ Configurer un login pour le mode enable (root) avec pour mot de passe Rootthepot20XX

```
switch>ena
switch#conf t
switch(config)#enable password Rootthepot2026
```

✔ Configurer un login et mot de passe pour le mode console avec pour mot de passe Thepot20XX

```
switch>en
switch#conf t
switch(config)#line con 0
switch(config-line)# password Thepot2026
switch(config-line)#login local
switch(config-line)#exit
switch(config)#exit
switch#exit
```

✔ Sauver vos configurations (enregistrement de la running config dans la nvram)

```
switch>ena
switch#conf t
switch(config)#write mem
```

```
THEPOT-FLYHER#
*Mar  1 01:02:07.880: %SYS-5-CONFIG_I: Configured from console by admin on console
THEPOT-FLYHER#write mem
Building configuration...
[OK]
THEPOT-FLYHER#exit
```

✔ Tester le bon fonctionnement, connectez vous en enable (faire un reload) et consulter la configuration en cours.

❑ Valider par une croix

Que dire de la visibilité des mots de passe ?

Les mots de passes ne sont pas affichés lorsqu'on entre les caractères.

```
ACCES RESERVE PRIVE

User Access Verification

Username: admin
Password:
THEPOT-FLYHER#
```

✓ Chiffrer les mots de passe dans la running config . Que constatez vous?

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

```
enable password 7 046904091B35444B1916114542595A
!
username alves password 7 02320C5E1B091B731C1C5F
username admin privilege 15 secret 5 $1$xPnO$EPpBbp6LO287.Q/wyNHMf.
no aaa new-model
system mtu routing 1500
ip subnet-zero
```

✓ Vérifier le chiffrement des mots de passe :
https://davidbombal.com/cisco-type-7-password-decryption/
Tester avec https://www.frameip.com/decrypter-dechiffrer-cracker-password-cisco-7/
Que concluez vous?

Les mots de passes sont effectivement cryptés, il faut aller sur les sites en question pour décrypter

HASH Cisco 7 demandé : 046904091b35444b1916114542595a
Mot de passe correspondant : Rootthepot2026

❑ Valider par une croix

https://www.frameip.com/decrypter-dechiffrer-cracker-password-cisco-7/

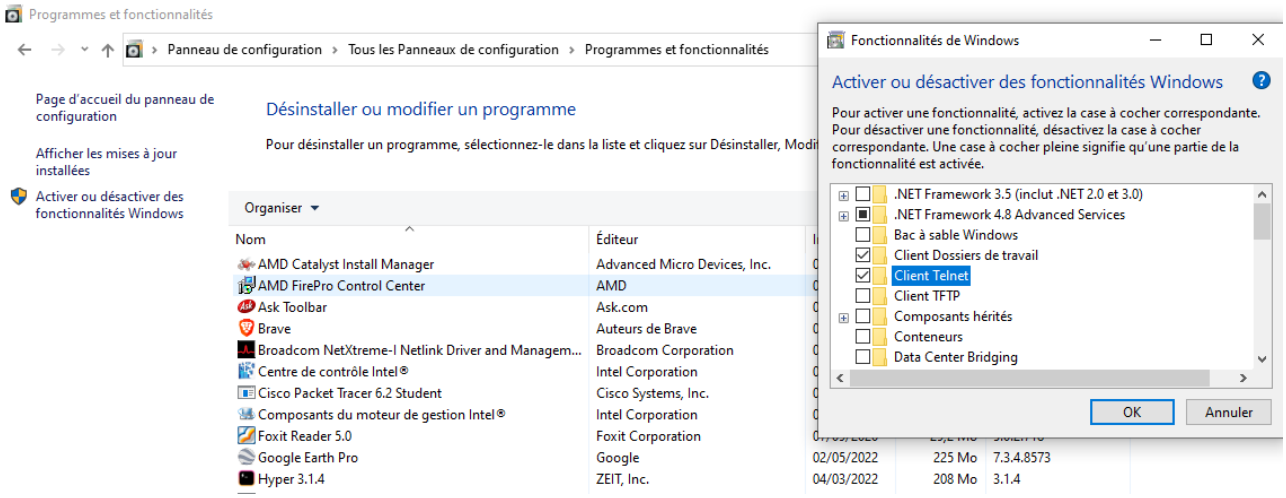
❑ Valider par une croix.

Sécuriser l'accès au switch à distance par mot de passe mode Virtual Terminal Line :

Visualiser la vidéo "Configuration IP telnet et SSH" : https://www.youtube.com/watch?v=yAuAJQbxzLQ
https://www.youtube.com/watch?v=f0pdje93NSY

Le switch dispose de 16 lignes d'accès à distance (La commande « line vty 0 15 » permet de rentrer dans la configuration des 16 lignes d'accès à distance).

Installer le client TELNET sur votre poste : ☒ Valider par une croix



La communication TELNET :

✓ De la même manière que pour le mode console (même mot de passe Thepot20XX), configurer les 16 lignes d'accès à distance : ❑ Valider par une croix

```
switch>en
switch#conf t
switch(config)#line vty 0 15
switch(config-line)#speed 9600
switch(config-line)# password Thepot2026
switch(config-line)#login local
switch(config-line)#exit
switch(config)#exit
switch#exit
```

✓ Affecter une adresse IP au switch sur le vlan 1 (172.20.6.XXX / : Numero de votre poste) pour permettre la communication à distance par ethernet: : ☒ Valider par une croix

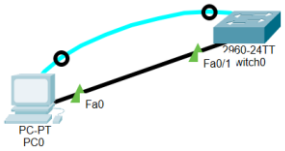
```
switch>en
switch#conf t
switch(config)#ip default-gateway 172.20.6.1
switch(config)#ip name-server 172.20.6.254
switch(config)#int vlan 1
switch(config-if)#ip address 172.20.6.111 255.255.0.0
switch(config-if)#no shutdown
```

✓ Vérifier la bonne configuration IP par la commande show run: ☒ Valider par une croix

```
THEPOT-FLYHER#ping 172.20.6.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.6.11, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
THEPOT-FLYHER#ping 172.20.6.111

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.6.111, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
THEPOT-FLYHER#
```

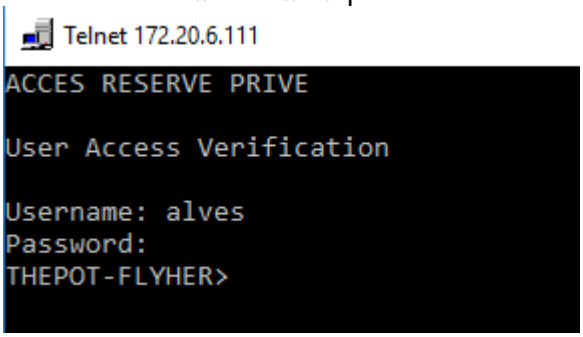


✓ Brasser votre poste sur le switch et tester la bonne connexion de votre poste ave commande : ping 172.20 . 6 . 111

❑ Valider par une croix

✓ Ouvrir une session telnet dans l'invite de commande (Telnet 172.20.6.XXX)

Username : admin / password : Rootthepot2026 ❑ Valider par une croix



Que constatez vous ?

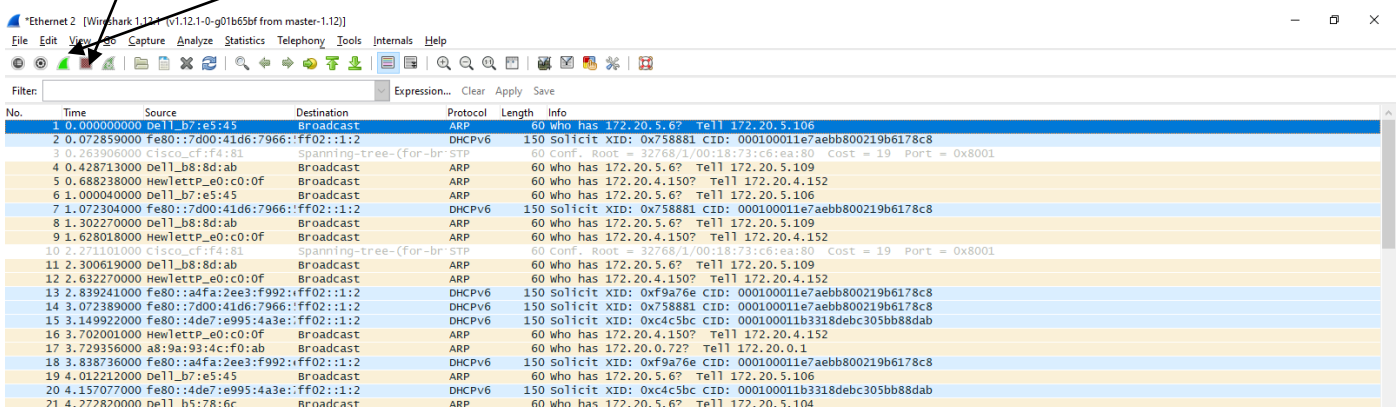
Sur l'image on voit alves, mais l'on peut se connecter en admin, la connexion se fait sans problème.

❑ Valider par une croix

✓ Installer le logiciel wireshark (ainsi que Wincap).

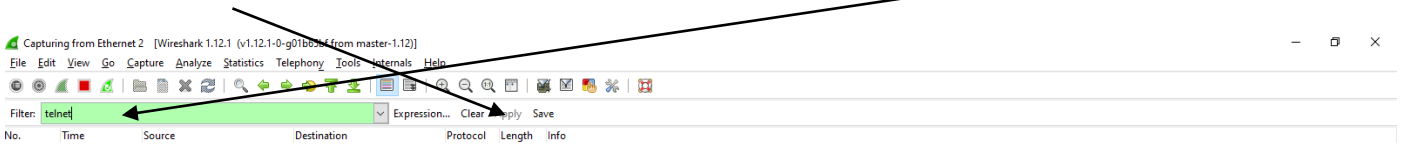
✓ Lancer le logiciel et une capture de trame.

Arrêtez la capture de trame. ❑ Valider par une croix



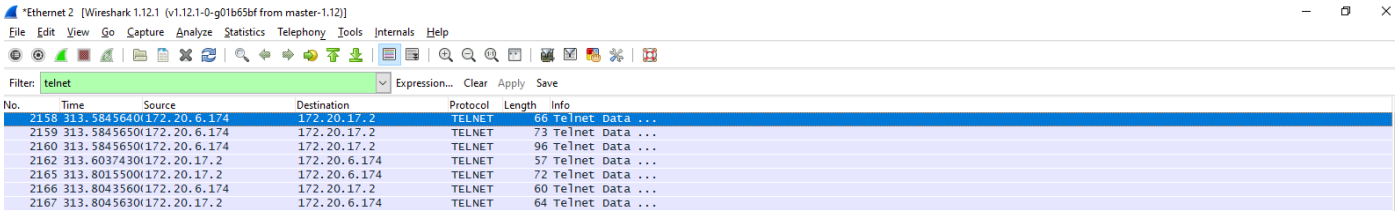
On constate que le logiciel capte toutes les trames passant par le PC sur le réseau.

Nous allons capturer et observer désormais les trames lorsque les mots de passes sont tapés lors d'une connexion telnet.
Pour alléger la visualisation du traffic, nous allons sélectionner que les trames telnet (filter les paquets telnet et appliquer « Apply »)

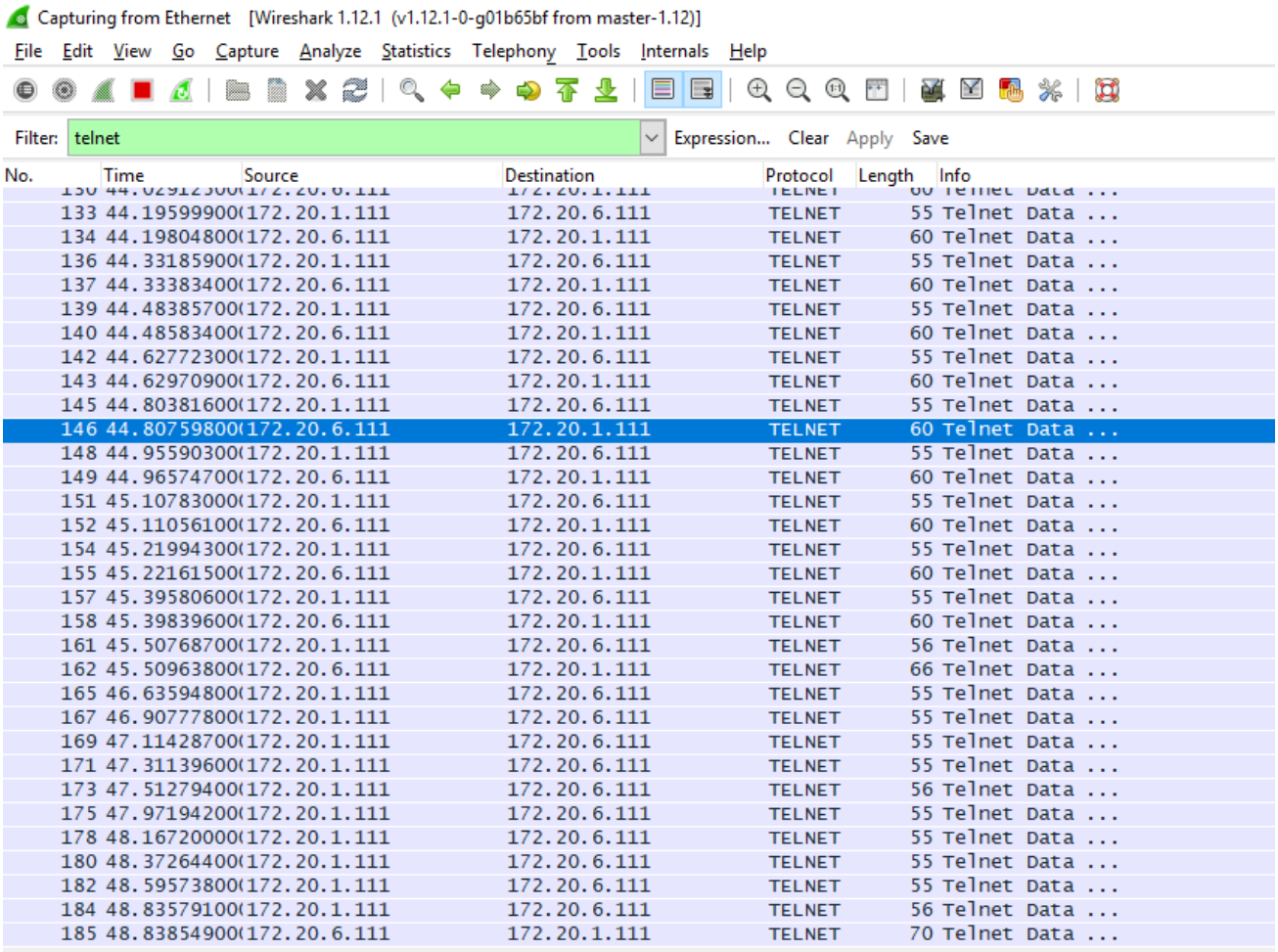


Lancer les captures. Pour l'instant, rien ne se passe car aucune demande n'est pour l'instant demandé.

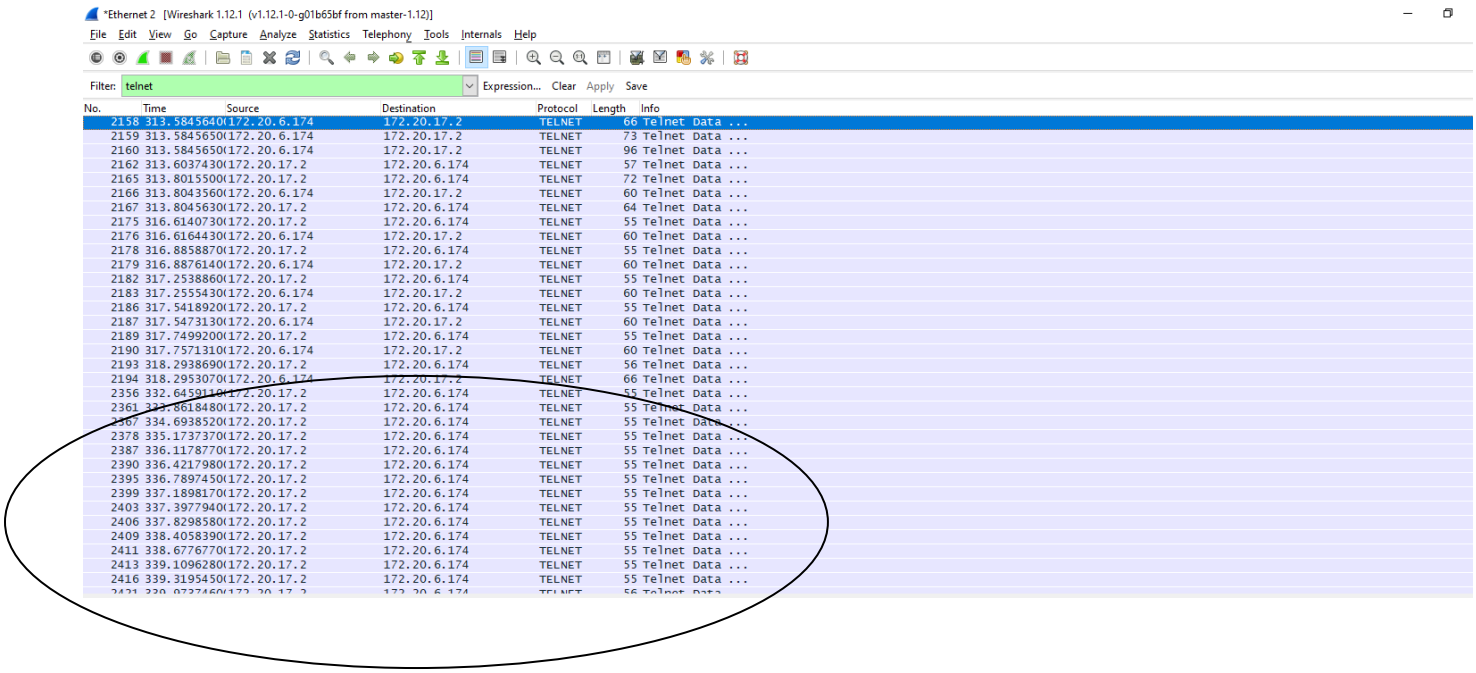
- ✓ Relancer une ouverture de demande de connexion telnet. Une fois la connexion établie, stopper la capture de trame.



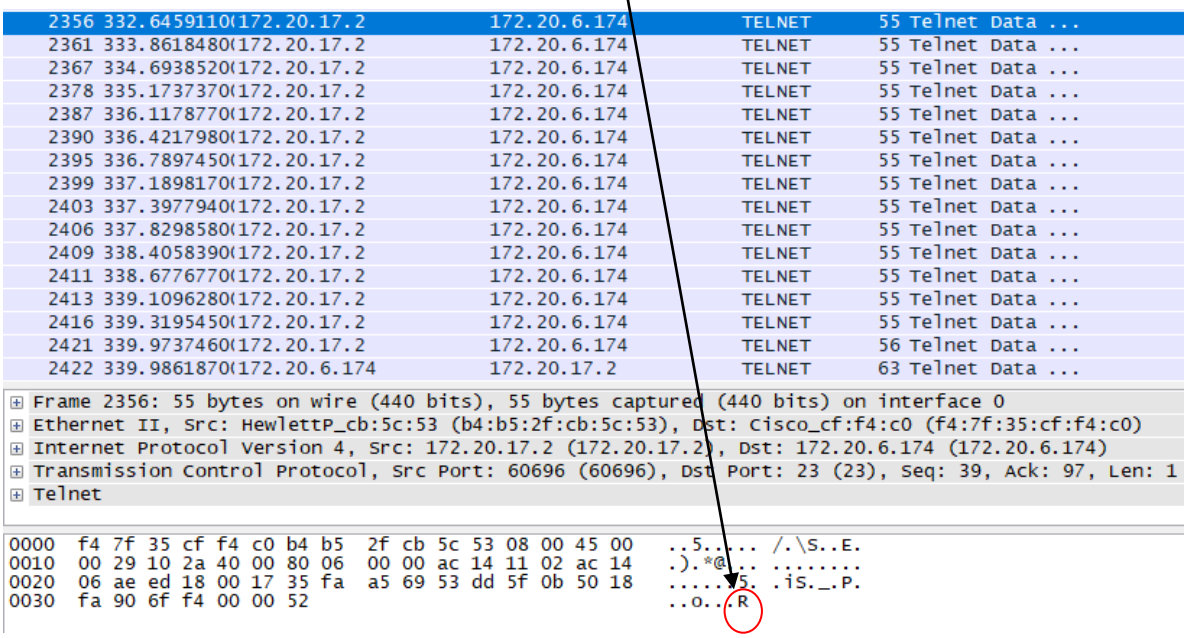
Que constatez vous ? Wireshark trace mon adresse IP, le protocole, le VLAN et sait que je suis connécté



Nous allons voir les trames envoyées du Pc vers le switch lorsque le mot de passe est demandé.



Nous allons voir les trames envoyées du Pc vers le switch lorsque le mot de passe est demandé.
Cliquez successivement sur les trames pour voir si les lettres du mot de passe apparaissent.



✓ Reconstituez le mot de passe. Qu'en déduisez vous ?

Thepot2026. Telnet peut tracer mon mot de passe, ce qui n'est pas sécuriré.

✓ Proposer un protocole de communication sécurisé.

Le SSH est un protocole de communication sécurisé, contrairement à Telnet.

LA COMMUNICATION SSH :

Visualiser la vidéo sur la communication SSH: https://www.youtube.com/watch?v=gxQKw7A6qDM

- ***LE PROTOCOLE SSH***

Secure Shell (**SSH**) est à la fois un **programme informatique** et un **protocole de communication sécurisé**.
Le protocole **SSH** (***Secure Shell***) a été mis au point en 1995 par le Finlandais Tatu Ylönen.
Il s'agit d'un protocole permettant à un **client** (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une **machine distante** (**serveur**) afin d'envoyer des commandes ou des fichiers de manière **sécurisée** :

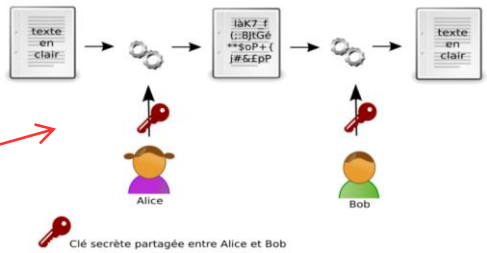
- Les **données** circulant entre le client et le serveur sont **chiffrées**, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.
- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

La *version 1* du protocole (SSH1) proposée dès 1995 possédait toutefois une faille permettant à un pirate d'insérer des données dans le flux chiffré. C'est la raison pour laquelle en 1997 la version 2 du protocole (**SSH2**). *Secure Shell Version 2* propose également une solution de transfert de fichiers sécurisé (***SFTP***, *Secure File Transfer Protocol*).

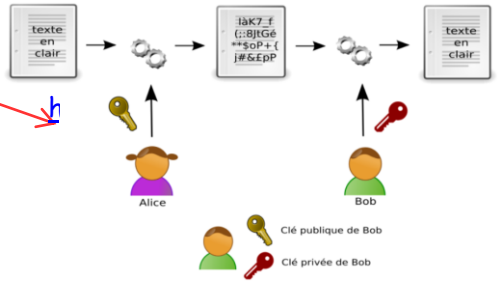
SSH est un protocole, c'est-à-dire une méthode standard permettant à des machines d'établir une communication sécurisée. A ce titre, il existe de nombreuses implémentations de clients et de serveurs SSH. Certains sont payants, d'autres sont gratuits ou *open source.*

- ***FONCTIONNEMENT DU SSH***

Le protocole SSH de connexion impose un **échange de clés de chiffrement** en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés.
SSH utilise la cryptographie asymétrique RSA ou DSA. En cryptographie asymétrique, chaque personne dispose d'un couple de clef : une clé publique et une clef privée. La clé publique peut être librement publiée tandis que la clef privée doit rester secrète. La connaissance de la clef publique ne permet pas d'en déduire la clé privée.



SSH utilise également la cryptographie symétrique. Les algorithmes de chiffrement symétrique sont beaucoup moins gourmands en ressources processeur que ceux de chiffrement asymétrique (et 10 à 100 fois plus rapide). Dans le protocole SSL, qui est utilisé par SSH et par les navigateurs Web, **la cryptographie asymétrique est utilisée au début de la communication pour que Alice et Bob puissent s'échanger une clef secrète de manière sécurisée, puis la suite la communication est sécurisée grâce à la cryptographie symétrique en utilisant la clef secrète ainsi échangée.**



Visualiser la vidéo sur la sécurisation de l'IOS CISCO telnet et configuration SSH:
https://www.youtube.com/watch?v=amZzup8pS90

- ✓ Configurer l'accès en SSH :

Les communications en telnet ne sont pas chiffrées. Les étapes suivantes permettent de configurer un accès en SSH.

1. Dans un premier temps, il est nécessaire de configurer un domaine pour le commutateur :

Switch(config)#**ip domain-name thepot.local**

```
THEPOT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
THEPOT(config)#ip domain-name thepot.local
THEPOT(config)#exit
```

Vérification par la commande show run : ❑ Valider par une croix

2. Activer l'accès en SSH (version2):

Switch(config)#**ip ssh version 2**

```
THEPOT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
THEPOT(config)#ip ssh version 2
```

3. Pour utiliser le chiffrement, il faut créer une clé RSA :

Switch(config)#**crypto key generate rsa**

```
THEPOT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
THEPOT(config)#crypto key generate rsa
The name for the keys will be: THEPOT.thepot.local
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]
```

Il est possible de rajouter des options :

- Un timeout de 60 secondes est ajouté pour les sessions ssh en cas d'inactivité .
- Nous laissons trois essais pour la connexion au switch.

Switch(config)#**ip ssh time-out 60**
Switch(config)#**ip ssh authentication-retries 3**

```
THEPOT(config)#ip ssh time-out 60
```

```
THEPOT(config)#ip ssh authentication-retries 3
```

Tout a été paramétré ici.

```
ACCES RESERVE PRIVE

User Access Verification

Username: admin
Password:
THEPOT-FLYHER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
THEPOT-FLYHER(config)#ip domain-name thepot.local
THEPOT-FLYHER(config)#ip ssh version 2
THEPOT-FLYHER(config)#crypto key generate rsa
The name for the keys will be: THEPOT-FLYHER.thepot.local
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]

THEPOT-FLYHER(config)#ip ssh time-out 60
THEPOT-FLYHER(config)#ip ssh authentication-retries 3
THEPOT-FLYHER(config)#username userssh password Rootthepot2026
```

4. Configuration de l'authentification SSH et l'ajout d'un compte administrateur :
   (login: userssh /mdp: Rootthepot20XX)

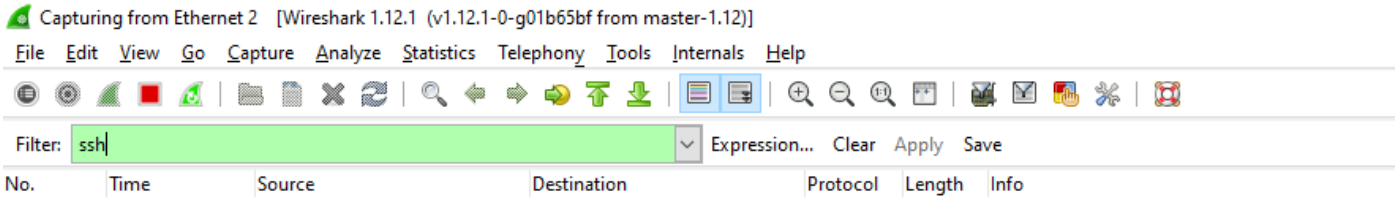
Switch(config)#**username userssh password** Rootthepot2026

5. Configuration de la connection SSH:

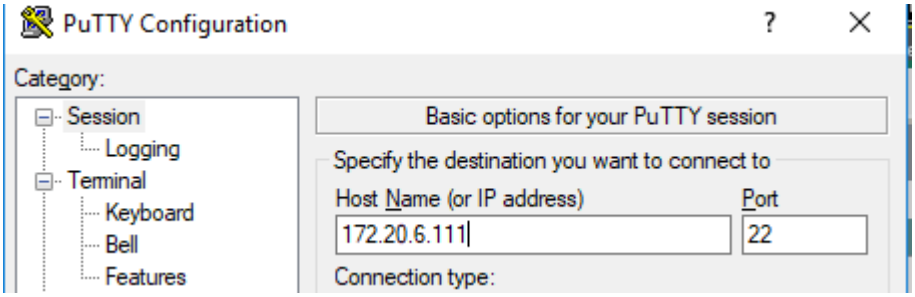
Switch(config)#**line vty 0 4**
Switch(config-line)#**login local**
Switch(config-line)#**transport input ssh**

```
THEPOT-FLYHER(config)#ip ssh time-out 60
THEPOT-FLYHER(config)#ip ssh authentication-retries 3
THEPOT-FLYHER(config)#username userssh password Rootthepot2026
THEPOT-FLYHER(config)#line vty 0 4
THEPOT-FLYHER(config-line)#login local
THEPOT-FLYHER(config-line)#transport input ssh
THEPOT-FLYHER(config-line)#
```

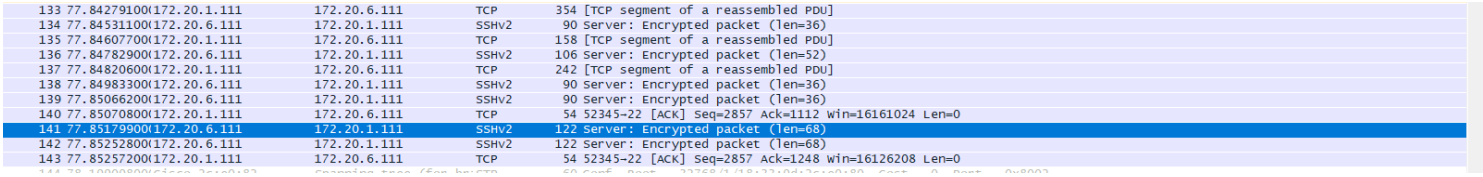
- ✓ Testez la communication à distance en SSH avec l'option simulation et en testant une connexion.
- ✓ Capturez les trames par wireshark (Filtrer uniquement les trames ssh)



- ✓ Connectez vous sur le switch en enable (par putty) et authentifiez vous.



- ✓ Émettez des consignes sur le switch en ssh et capturez les trames par wireshark (Filtrer uniquement les trames ssh)

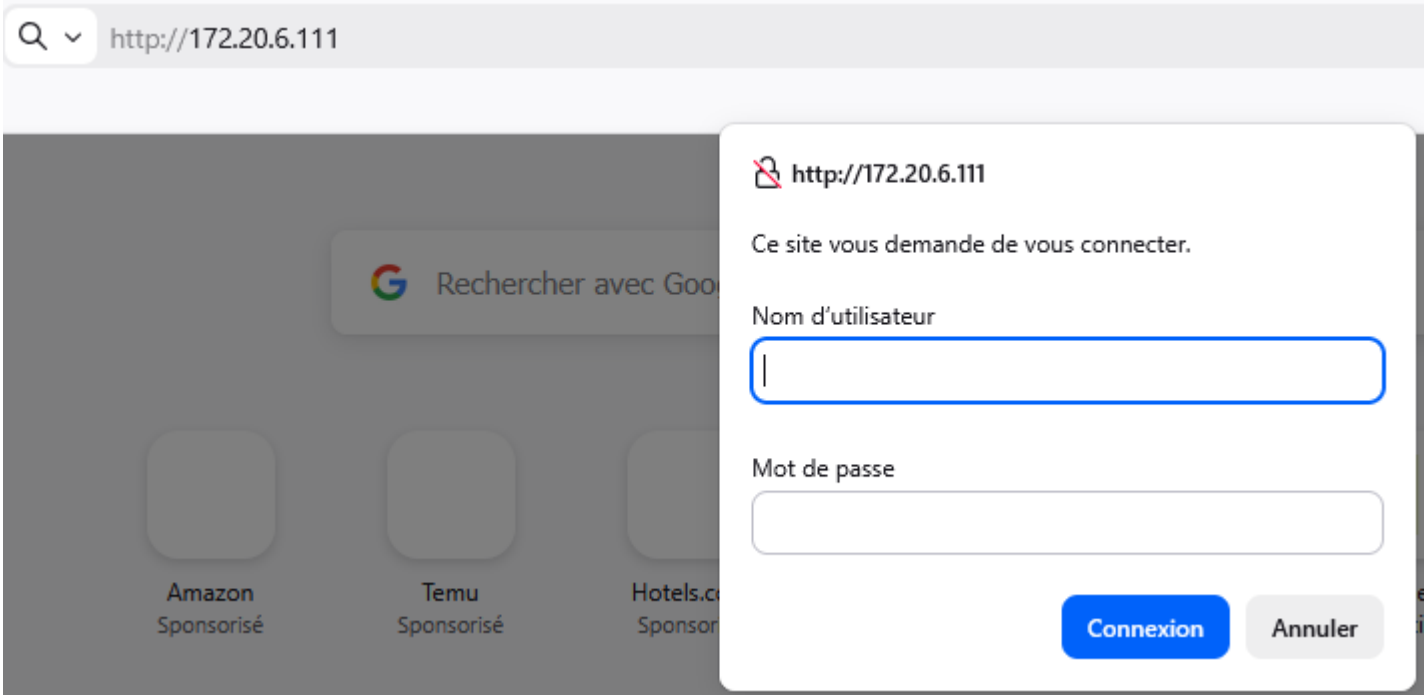


- ✓ SSH est il un protocole de communication sécurisé ?

Oui, c'est un protocole de communication sécurisé. On ne peut pas tracer les mots de passe sur wireshark en protocole SSHV2.

PRISE EN MAIN DU SWITCH PAR L'INTERFACE GRAPHIQUE DU SWITCH:

Tapez l'adresse IP du switch dans l'URL de votre navigateur :

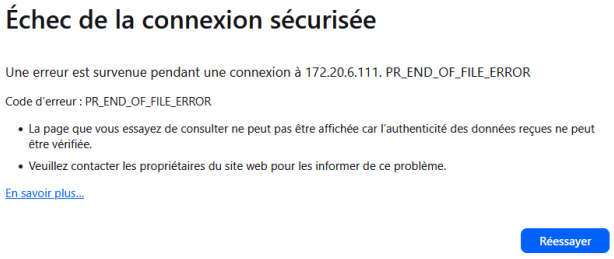


Authentifiez vous (admin/Rootthepot2026). Quelle indication vous est proposée ?

On arrive sur un rapport de démarrage avant de pouvoir aller sur le site sécurisé ou non.

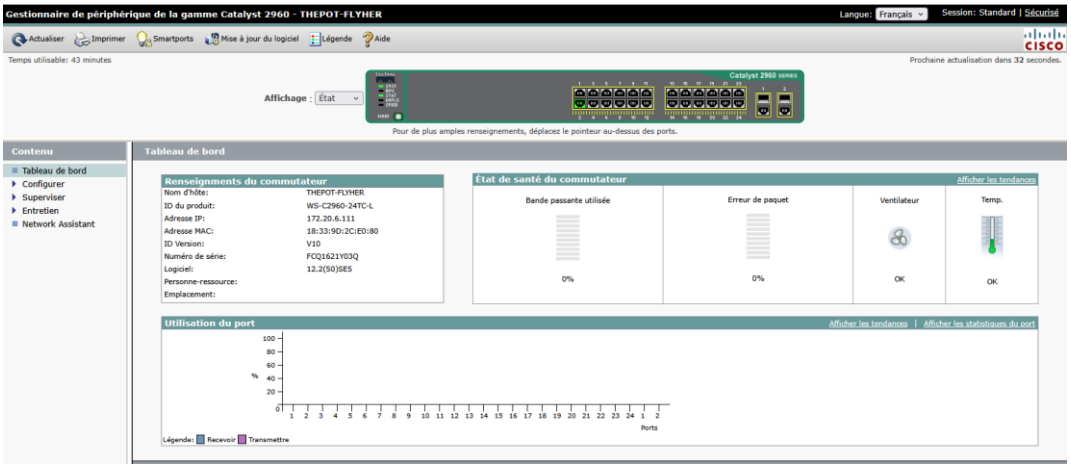
Répondez par oui. Que constatez vous ?

On arrive sur une page d'erreur car on a mis oui, hors le telnet n'est pas sécurisé donc l'accès va être refusé.



Répondez par non. Que constatez vous ? On accède à l'interface graphique du switch en session standard non sécurisé.
Vérifiez vos configurations sur cette interface graphique. ❑ Valider par une croix

On arrive sur ue page qui affiche l'interface graphique de la switch THEPOT-FLYHER.



TP : REINITIALISATION DU SWITCH (En présence du formateur)

✔ Réinitialiser le switch par les commandes suivantes:

```
Thepot> ena
Thepot# delete flash:vlan.dat
Thepot# erase startup-config ou write erase
Thepot# reload
Switch>
```