


| | | |
|--|--|--|
|  Quimper | <p align="center">Modèle OSI</p> <p align="center">Prise à distance d'un élément réseau</p> <p align="center">Communiquer et paramétrer un élément réseau</p> <p align="center">Accès Sécurisé des réseaux</p> | <p align="center">Travaux pratiques</p> |
| NOM: | | |

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 charges
- 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 switches 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 switches ?

Consulter les vidéos sur le modèle OSI :

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

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

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

Le modèle ISO

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 : **trois ans d'emprisonnement et de 100 000 € d'amende.**

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 : Article 323-1 Modifié par LOI n°2023-22 du 24 janvier 2023 - art. 6

Plan de traitement des risques :

De nombreux moyens techniques peuvent être mis en œuvre pour assurer une sécurité du système d'information.

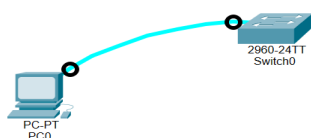
Il convient de choisir les moyens nécessaires, suffisants, et justes.

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.

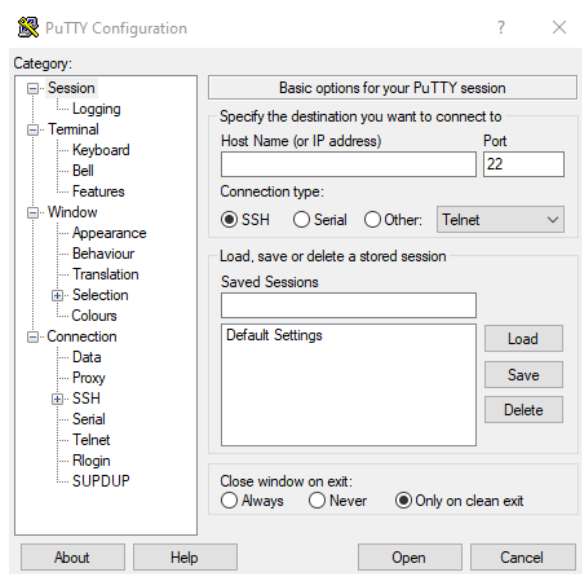
À l'origine disponible uniquement pour Windows, il est à présent porté sur diverses plates-formes Unix

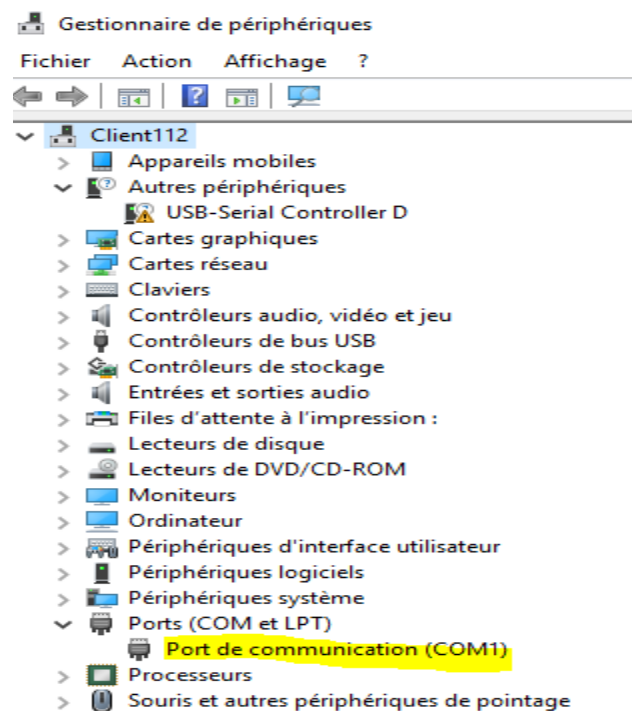
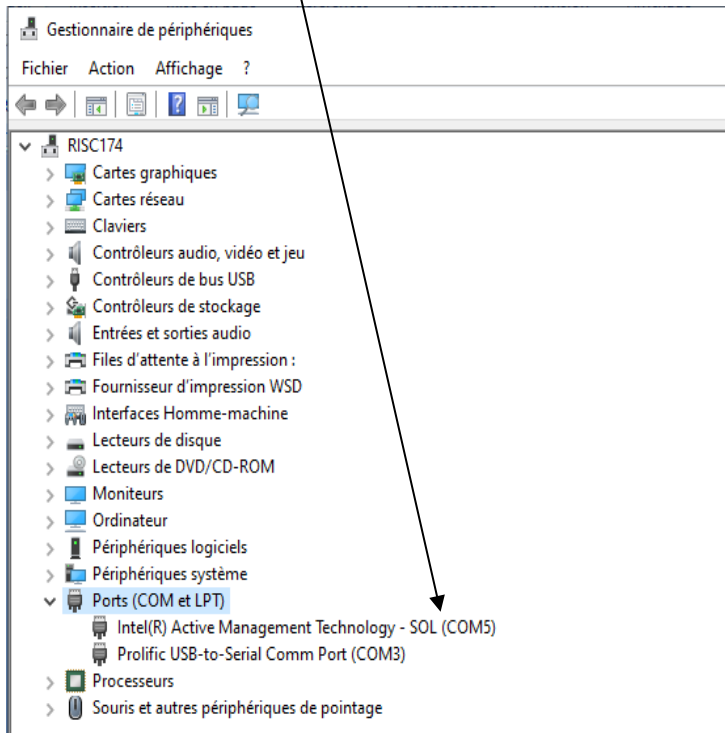
Caractéristiques :

- Est portable. Aucune installation n'est nécessaire; il suffit de lancer l'exécutable téléchargé pour l'utiliser.
- Conserve les paramètres 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.

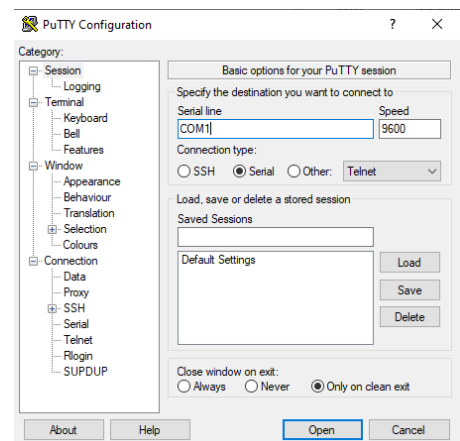
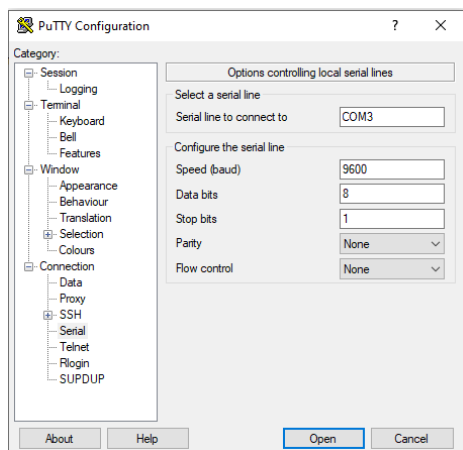
Sécuriser l'accès au switch par mot de passe mode console:

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

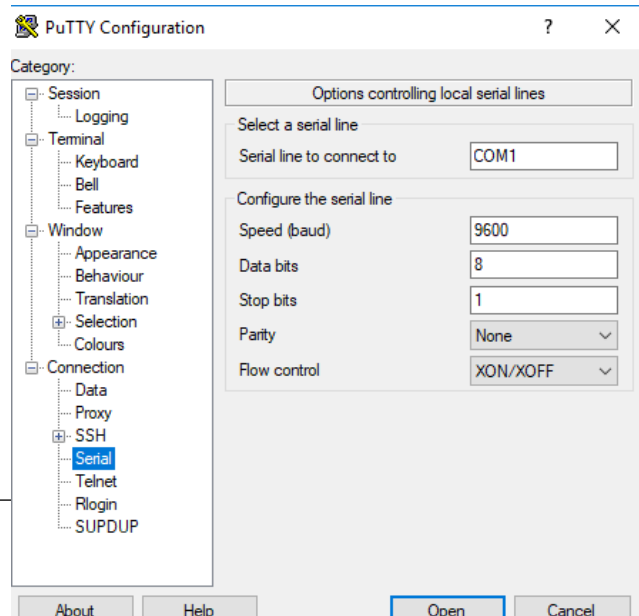
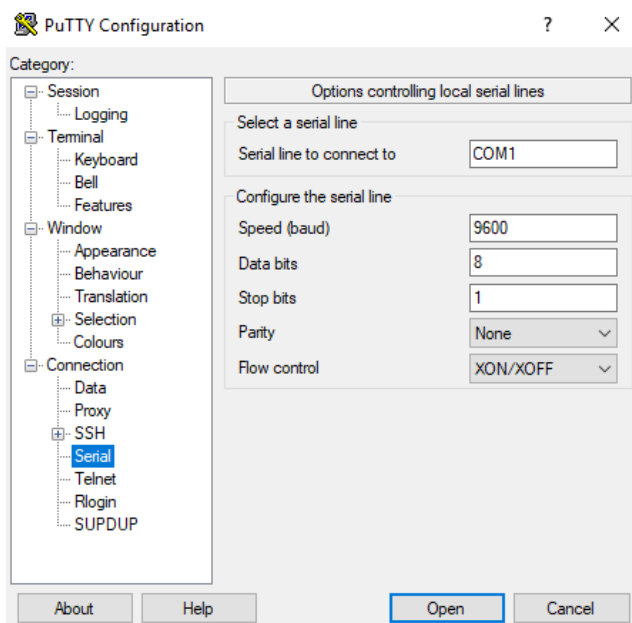




✓ Paramétrer la liaison série comme ci-dessous en y indiquant le numéro de port utilisé :



✓ Lancer une communication par le logiciel putty (en sélectionnant sérial / en y indiquant le numero du port série)



→ Switch>

- ✓ 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 ?

```
Switch>ena
Switch#show run
Building configuration...

Current configuration : 3089 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
!
!
!
!
!
--More--
```

Le switch n'est pas configuré.

Installer le marquage afin d'informer tout utilisateur de l'aspect restreint de l'accès :

Recommandations pour les architectures des systèmes d'information sensible ou diffusion restreinte ANSSI :

R36

Marquer les informations sensibles

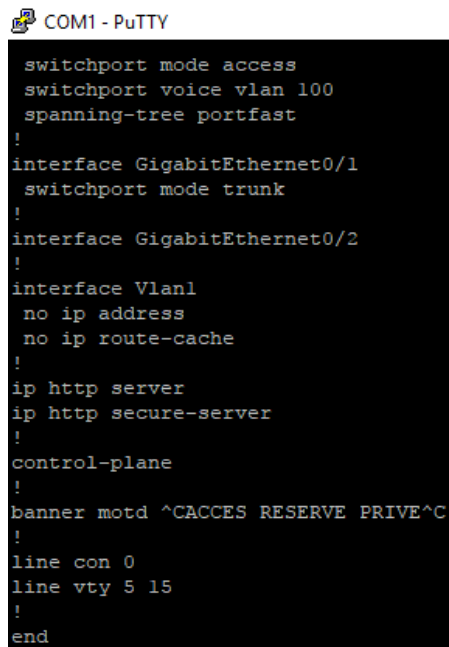
Il est fortement recommandé que l'entité mettant en œuvre un SI sensible se dote des moyens permettant le marquage des fichiers sensibles (tampons, conventions de nommage...) et des applications sensibles (bannières, adaptation de l'interface homme-machine...). Elle doit en outre sensibiliser les utilisateurs du SI sensible à l'importance de marquer les informations dès leur création. Les informations DR doivent être marquées avec la mention DIFFUSION RESTREINTE.

- ✓ Configurer une bannière contenant un message du jour :

```
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!
```

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



```
COM1 - PuTTY

switchport mode access
switchport voice vlan 100
spanning-tree portfast
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
no ip route-cache
!
ip http server
ip http secure-server
!
control-plane
!
banner motd ^CACCES RESERVE PRIVE^C
!
line con 0
line vty 5 15
!
end
```

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
```

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname THEPOT
THEPOT(config)#exit
THEPOT#s
*Mar  3 00:16:04.968: %SYS-5-CONFIG_I: Configured from console by consolehow run
Building configuration...

Current configuration : 1302 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname THEPOT
```

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

```
Switch(config)#hostname THEPOT
THEPOT(config)#exit
THEPOT#
*May  5 22:31:50.798: %SYS-5-CONFIG_I: Configured from console by console
```

- ✓ 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 Thepot2025
switch(config)#username admin privilege 15 secret Rootthepot2025
```

```
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$dAdj$1oCU4VH3bUnHv5bU/
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
```

```
THEPOT(config)#username etudiant password Thepot2025
THEPOT(config)#g)#username admin
```

```
% Invalid input detected at '^' marker.
```

```
THEPOT(config)#g)#username admin
```

```
% Invalid input detected at '^' marker.
```

```
THEPOT(config)#g)#username admin privilege 15 secret Rootthepot2025
```

```
% Invalid input detected at '^' marker.
```

```
THEPOT(config)#ena
% Incomplete command.
```

```
THEPOT(config)#username admin privilege 15 secret Rootthepot2025
THEPOT(config)#
```

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

On remarque que le mot de passe pour l'admin n'est pas visible contrairement à l'utilisateur etudiant

```
THEPOT con0 is now available

Press RETURN to get started.

ACCES RESERVE PRIVE
THEPOT>ena
THEPOT#show run
Building configuration...

Current configuration : 3231 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 Thepot2025
username admin privilege 15 secret 5 $1$NG6o$SUa7QcxPUDlpTzbnzPs1Y/
no aaa new-model
system mtu routing 1500
ip subnet-zero
```

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

```
switch>ena
switch#conf t
switch(config)#enable password Rootthepot2025
```

```
Press RETURN to get started.

ACCES RESERVE PRIVE
THEPOT>ena
THEPOT#conf t
Enter configuration commands, one per line. End with CNTL/Z.
THEPOT(config)#enable password Rootthepot2025
THEPOT(config)#
```

- ✓ Configurer un login et mot de passe pour le mode console avec pour mot de passe Thepot2025

```
switch>en
switch#conf t
switch(config)#line con 0
```

```
switch(config-line)# password _____  
switch(config-line)#login local  
switch(config-line)#exit  
switch(config)#exit  
switch#exit
```

```
THEPOT(config)#ena  
% Incomplete command.  
  
THEPOT(config)#^Z  
THEPOT#  
*May 5 23:18:36.569: %SYS-5-CONFIG_I: Configured from console by console  
THEPOT#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
THEPOT(config)#line con0  
^  
% Invalid input detected at '^' marker.  
  
THEPOT(config)#line con 0  
THEPOT(config-line)#password Thepot2025  
THEPOT(config-line)#login local  
THEPOT(config-line)#exit  
THEPOT(config)#exit  
THEPOT#  
*May 5 23:20:10.287: %SYS-5-CONFIG_I: Configured from console by consoleexit
```

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

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

```
THEPOT#write mem  
Building configuration...  
[OK]  
  
ACCES RESERVE PRIVE  
  
User Access Verification  
  
Username: etudiant  
Password:  
THEPOT>ena  
Password:  
THEPOT#write mem  
Building configuration...  
[OK]  
THEPOT#
```

- ✓ 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 ? Ils sont tous visible sauf celui pour l'admin

```
Current configuration : 3323 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
!
enable password Rootthepot2025
!
username etudiant password 0 Thepot2025
username admin privilege 15 secret 5 $1$NG6o$Sua7QcxPUDlpTzbnzPslY/
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
--More--
```

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

switch(config)# service password-encryption

```
Current configuration : 3364 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname THEPOT
!
boot-start-marker
boot-end-marker
!
enable password 7 122B0A18061F04013A24307A636777
!
username etudiant password 7 00301B0314541F545F7319
username admin privilege 15 secret 5 $1$NG6o$Sua7QcxPUDlpTzbnzPslY/
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
--More--
```

je constate que les mots de passes sont encrypté .

- ✓ Vérifier le chiffrement des mots de passe :

<https://davidbombal.com/cisco-type-7-password-decryption/> (lien non fonctionnel - erreur 404)

Tester avec <https://www.frameip.com/decrypter-dechiffrer-cracker-password-cisco-7/>

Que concluez vous?

☒ Valider par une croix

1 – Recherche en ligne

HASH Cisco 7 demandé : 00301b0314541f545f7319

Mot de passe correspondant : Thepot2025

HASH Cisco 7 (Exemple : 062B0A33)

On peut déduire que le chiffrement cisco type 7 n'est pas très sécurisé car on peut facilement le déchiffrer sur un site internet.

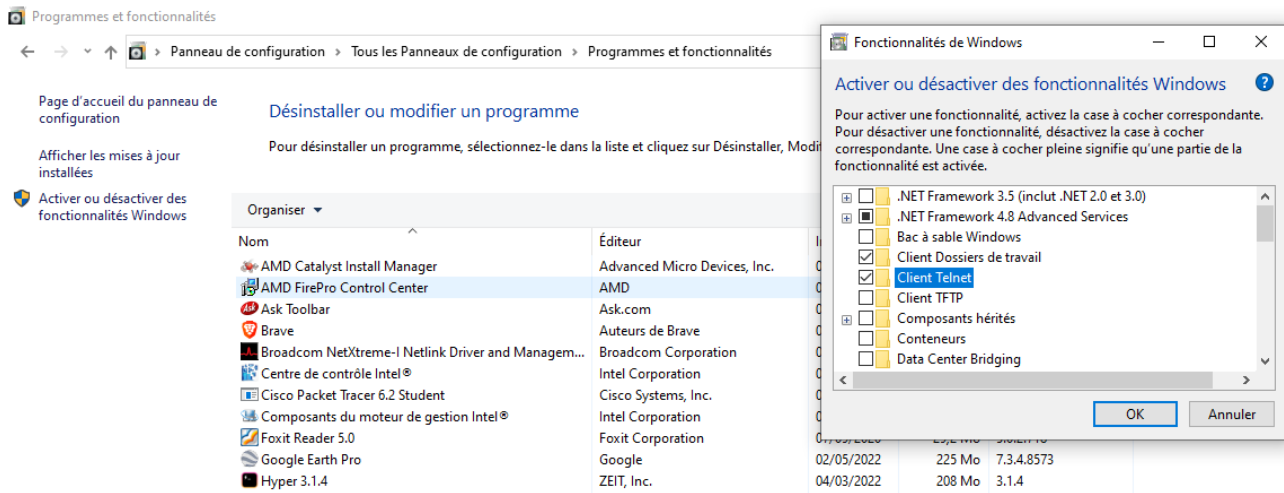
☒ Valider par une croix.

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



```
Microsoft Windows [version 10.0.15063]
(c) 2017 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>dism /online /Enable-Feature /FeatureName:TelnetClient

Outil Gestion et maintenance des images de déploiement
Version : 10.0.15063.0

Version de l'image : 10.0.15063.0

Activation de la ou des fonctionnalités
[=====]
===== 0.1% [=====] 12.5% [=====] 15.0% [=====]
===== 17.5% [=====] 20.0% [=====] 22.5% [=====]
===== 25.0% [=====] 27.5% [=====] 30.0% [=====]
===== 31.7% [=====] 33.4% [=====] 38.9% [=====]
===== 34.4% [=====] 35.0% [=====] 40.0% [=====]
===== 36.1% [=====] 36.1% [=====] 41.7% [=====]
===== 37.8% [=====] 37.8% [=====] 43.4% [=====]
===== 39.5% [=====] 39.5% [=====] 45.0% [=====]
===== 41.2% [=====] 41.2% [=====] 46.7% [=====]
===== 42.9% [=====] 42.9% [=====] 48.3% [=====]
===== 44.6% [=====] 44.6% [=====] 50.0% [=====]
===== 46.3% [=====] 46.3% [=====] 51.7% [=====]
===== 48.0% [=====] 48.0% [=====] 53.3% [=====]
===== 49.7% [=====] 49.7% [=====] 55.0% [=====]
===== 51.4% [=====] 51.4% [=====] 56.7% [=====]
===== 53.1% [=====] 53.1% [=====] 58.3% [=====]
===== 54.8% [=====] 54.8% [=====] 60.0% [=====]
===== 56.5% [=====] 56.5% [=====] 61.7% [=====]
===== 58.2% [=====] 58.2% [=====] 63.3% [=====]
===== 59.9% [=====] 59.9% [=====] 65.0% [=====]
===== 61.6% [=====] 61.6% [=====] 66.7% [=====]
===== 63.3% [=====] 63.3% [=====] 68.3% [=====]
===== 65.0% [=====] 65.0% [=====] 70.0% [=====]
===== 66.7% [=====] 66.7% [=====] 71.7% [=====]
===== 68.4% [=====] 68.4% [=====] 73.3% [=====]
===== 70.1% [=====] 70.1% [=====] 75.0% [=====]
===== 71.8% [=====] 71.8% [=====] 76.7% [=====]
===== 73.5% [=====] 73.5% [=====] 78.3% [=====]
===== 75.2% [=====] 75.2% [=====] 80.0% [=====]
===== 76.9% [=====] 76.9% [=====] 81.7% [=====]
===== 78.6% [=====] 78.6% [=====] 83.3% [=====]
===== 80.3% [=====] 80.3% [=====] 85.0% [=====]
===== 82.0% [=====] 82.0% [=====] 86.7% [=====]
===== 83.7% [=====] 83.7% [=====] 88.3% [=====]
===== 85.4% [=====] 85.4% [=====] 90.0% [=====]
===== 87.1% [=====] 87.1% [=====] 91.7% [=====]
===== 88.8% [=====] 88.8% [=====] 93.3% [=====]
===== 90.5% [=====] 90.5% [=====] 95.0% [=====]
===== 92.2% [=====] 92.2% [=====] 96.7% [=====]
===== 93.9% [=====] 93.9% [=====] 98.3% [=====]
===== 95.6% [=====] 95.6% [=====] 100.0% [=====]
L'opération a réussi.

C:\Windows\system32>
```

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 Thepot2025
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 / : Numéro 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.XXX 255.255.0.0
switch(config-if)#no shutdown

```

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

```

interface Vlan1
 ip address 172.20.16.112 255.255.0.0
 no ip route-cache

```

- ✓ Brasser votre poste sur le switch et tester la bonne connexion de votre poste avec le switch avec la commande : ping 172.20.16.112

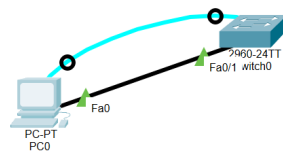
```

C:\Users\prepareteur>ping 172.20.16.112

Envoi d'une requête 'Ping' 172.20.16.112 avec 32 octets de données :
Réponse de 172.20.16.112 : octets=32 temps=2 ms TTL=255
Réponse de 172.20.16.112 : octets=32 temps=2 ms TTL=255
Réponse de 172.20.16.112 : octets=32 temps=2 ms TTL=255
Réponse de 172.20.16.112 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 172.20.16.112:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms

```



☐ Valider par une croix

- ✓ Ouvrir une session telnet dans l'invite de commande (Telnet 172.20.6.XXX)
Username : admin / password : Rootthepot20XX ☐ Valider par une croix

```

Telnet 172.20.6.174
ACCES RESERVE PRIVE
User Access Verification
Username: admin
Password:
THEPOT#

```

Que constatez vous ?

On dirait que l'on ouvre puTTY, il y a la même interface.

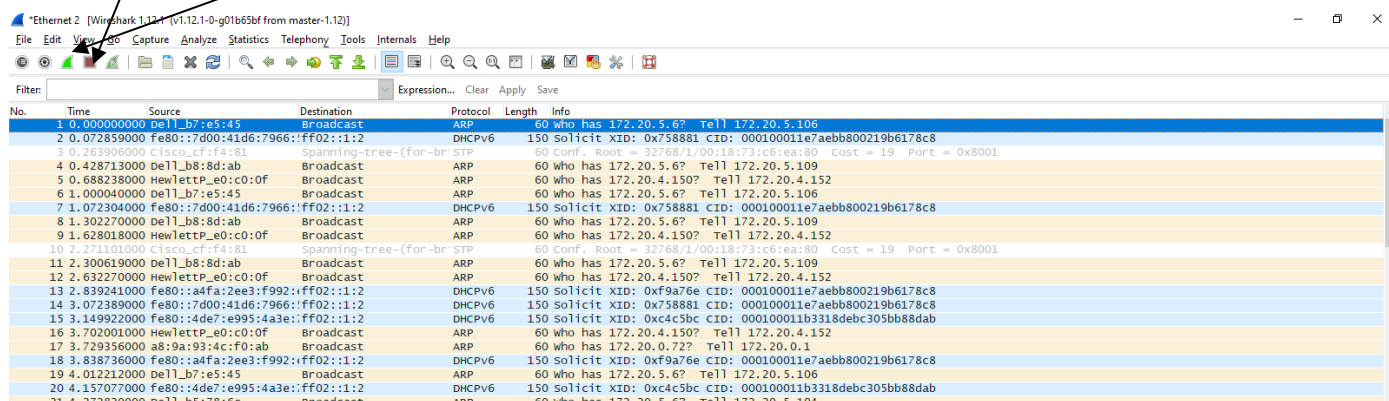
☐ Valider par une croix

✓ Installer le logiciel wireshark (ainsi que Wincap).

✓ Lancer le logiciel et une capture de trame.

Arrêtez la capture de trame.

☒ Valider par une croix



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|---------------------------------|----------------------|----------|--------|---|
| 1 | 0.000000000 | De11_b7:e5:45 | Broadcast | ARP | 60 | who has 172.20.5.6? Tell 172.20.5.106 |
| 2 | 0.072859000 | fe80::d00:41d6:7966::ff02::1:2 | Broadcast | DHCPv6 | 150 | Solicit XID: 0x758881 CID: 000100011e7aebb800219b6178c8 |
| 3 | 0.263906000 | cisco_cf:f4:81 | Spanning-tree-for-br | STP | 60 | Conf. Root = 32768/1/0018:73:c6:ea:80 Cost = 19 Port = 0x8001 |
| 4 | 0.428713000 | De11_b8:8d:ab | Broadcast | ARP | 60 | who has 172.20.5.6? Tell 172.20.5.109 |
| 5 | 0.688238000 | HewlettP_e0:c0:0f | Broadcast | ARP | 60 | who has 172.20.4.150? Tell 172.20.4.152 |
| 6 | 1.000040000 | De11_b7:e5:45 | Broadcast | ARP | 60 | who has 172.20.5.6? Tell 172.20.5.106 |
| 7 | 1.072304000 | fe80::d00:41d6:7966::ff02::1:2 | Broadcast | DHCPv6 | 150 | Solicit XID: 0x758881 CID: 000100011e7aebb800219b6178c8 |
| 8 | 1.302270000 | De11_b8:8d:ab | Broadcast | ARP | 60 | who has 172.20.5.6? Tell 172.20.5.109 |
| 9 | 1.628018000 | HewlettP_e0:c0:0f | Broadcast | ARP | 60 | who has 172.20.4.150? Tell 172.20.4.152 |
| 10 | 2.271101000 | cisco_cf:f4:81 | Spanning-tree-for-br | STP | 60 | Conf. Root = 32768/1/0018:73:c6:ea:80 Cost = 19 Port = 0x8001 |
| 11 | 2.300619000 | De11_b8:8d:ab | Broadcast | ARP | 60 | who has 172.20.5.6? Tell 172.20.5.109 |
| 12 | 2.632270000 | HewlettP_e0:c0:0f | Broadcast | ARP | 60 | who has 172.20.4.150? Tell 172.20.4.152 |
| 13 | 2.839241000 | fe80::a4fa:2ee3:f992::ff02::1:2 | Broadcast | DHCPv6 | 150 | Solicit XID: 0xf9a76e CID: 000100011e7aebb800219b6178c8 |
| 14 | 3.072389000 | fe80::d00:41d6:7966::ff02::1:2 | Broadcast | DHCPv6 | 150 | Solicit XID: 0x758881 CID: 000100011e7aebb800219b6178c8 |
| 15 | 3.149922000 | fe80::4de7:e995:4a3e::ff02::1:2 | Broadcast | DHCPv6 | 150 | Solicit XID: 0xc4c5bc CID: 000100011b3318debc305bb88dab |
| 16 | 3.702001000 | HewlettP_e0:c0:0f | Broadcast | ARP | 60 | who has 172.20.4.150? Tell 172.20.4.152 |
| 17 | 3.729356000 | a8:9a:93:4c:f0:ab | Broadcast | ARP | 60 | who has 172.20.0.72? Tell 172.20.0.1 |
| 18 | 3.838736000 | fe80::a4fa:2ee3:f992::ff02::1:2 | Broadcast | DHCPv6 | 150 | Solicit XID: 0xf9a76e CID: 000100011e7aebb800219b6178c8 |
| 19 | 4.012212000 | De11_b7:e5:45 | Broadcast | ARP | 60 | who has 172.20.5.6? Tell 172.20.5.106 |
| 20 | 4.157077000 | fe80::4de7:e995:4a3e::ff02::1:2 | Broadcast | DHCPv6 | 150 | Solicit XID: 0xc4c5bc CID: 000100011b3318debc305bb88dab |
| 21 | 4.272820000 | De11_b5:78:6f | Broadcast | ARP | 60 | who has 172.20.5.6? Tell 172.20.5.104 |

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.

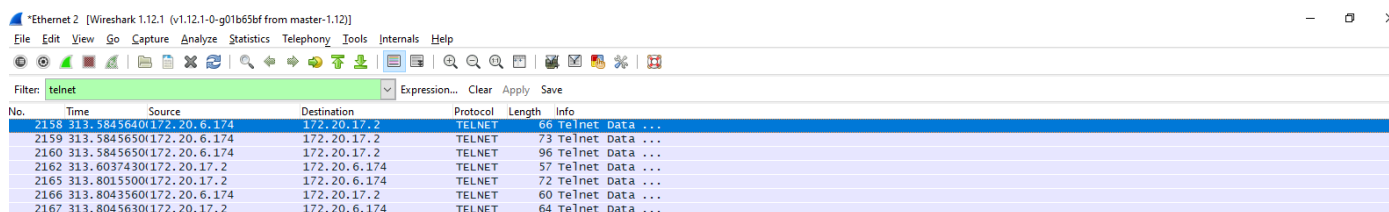
Pour alléger la visualisation du trafic, nous allons sélectionner que les trames telnet (filter les paquets telnet et appliquer « Apply »)



| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-------------|--------------|--------------|----------|--------|-----------------|
| 2158 | 313.5845640 | 172.20.6.174 | 172.20.17.2 | TELNET | 66 | Telnet Data ... |
| 2159 | 313.5845650 | 172.20.6.174 | 172.20.17.2 | TELNET | 73 | Telnet Data ... |
| 2160 | 313.5845650 | 172.20.6.174 | 172.20.17.2 | TELNET | 96 | Telnet Data ... |
| 2162 | 313.6037430 | 172.20.17.2 | 172.20.6.174 | TELNET | 57 | Telnet Data ... |
| 2165 | 313.8015500 | 172.20.17.2 | 172.20.6.174 | TELNET | 72 | Telnet Data ... |
| 2166 | 313.8043560 | 172.20.6.174 | 172.20.17.2 | TELNET | 60 | Telnet Data ... |
| 2167 | 313.8045630 | 172.20.17.2 | 172.20.6.174 | TELNET | 64 | Telnet Data ... |

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.



| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-------------|--------------|--------------|----------|--------|-----------------|
| 2158 | 313.5845640 | 172.20.6.174 | 172.20.17.2 | TELNET | 66 | Telnet Data ... |
| 2159 | 313.5845650 | 172.20.6.174 | 172.20.17.2 | TELNET | 73 | Telnet Data ... |
| 2160 | 313.5845650 | 172.20.6.174 | 172.20.17.2 | TELNET | 96 | Telnet Data ... |
| 2162 | 313.6037430 | 172.20.17.2 | 172.20.6.174 | TELNET | 57 | Telnet Data ... |
| 2165 | 313.8015500 | 172.20.17.2 | 172.20.6.174 | TELNET | 72 | Telnet Data ... |
| 2166 | 313.8043560 | 172.20.6.174 | 172.20.17.2 | TELNET | 60 | Telnet Data ... |
| 2167 | 313.8045630 | 172.20.17.2 | 172.20.6.174 | TELNET | 64 | Telnet Data ... |

Que constatez vous ? On remarque que les caractères du pseudo utilisateur et du mot de passe qu'on rentre lors de la connexion en telnet sont visible depuis la trame

Wireshark interface showing a packet capture on the 'telnet' filter. The packet list shows multiple Telnet packets from 172.20.1.53 to 172.20.16.112. Packet 81 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|-------------------------|
| 73 | 19.053199 | 172.20.16.112 | 172.20.1.53 | TELNET | 60 | Suboption Terminal Type |
| 74 | 19.053429 | 172.20.1.53 | 172.20.16.112 | TELNET | 64 | Suboption Terminal Type |
| 81 | 22.135687 | 172.20.1.53 | 172.20.16.112 | TELNET | 55 | 1 byte data |
| 82 | 22.137820 | 172.20.16.112 | 172.20.1.53 | TELNET | 60 | 1 byte data |
| 85 | 22.415623 | 172.20.1.53 | 172.20.16.112 | TELNET | 55 | 1 byte data |
| 86 | 22.417237 | 172.20.16.112 | 172.20.1.53 | TELNET | 60 | 1 byte data |
| 88 | 22.895637 | 172.20.1.53 | 172.20.16.112 | TELNET | 55 | 1 byte data |
| 89 | 22.897734 | 172.20.16.112 | 172.20.1.53 | TELNET | 60 | 1 byte data |
| 92 | 23.319378 | 172.20.1.53 | 172.20.16.112 | TELNET | 55 | 1 byte data |
| 93 | 23.322711 | 172.20.16.112 | 172.20.1.53 | TELNET | 60 | 1 byte data |
| 95 | 23.543975 | 172.20.1.53 | 172.20.16.112 | TELNET | 55 | 1 byte data |
| 96 | 23.546702 | 172.20.16.112 | 172.20.1.53 | TELNET | 60 | 1 byte data |
| 98 | 24.303381 | 172.20.1.53 | 172.20.16.112 | TELNET | 56 | 2 bytes data |
| 99 | 24.306253 | 172.20.16.112 | 172.20.1.53 | TELNET | 66 | 12 bytes data |
| 106 | 28.135622 | 172.20.1.53 | 172.20.16.112 | TELNET | 55 | 1 byte data |
| 109 | 29.199647 | 172.20.1.53 | 172.20.16.112 | TELNET | 55 | 1 byte data |
| 111 | 29.439600 | 172.20.1.53 | 172.20.16.112 | TELNET | 55 | 1 byte data |
| 114 | 29.759655 | 172.20.1.53 | 172.20.16.112 | TELNET | 55 | 1 byte data |
| 120 | 32.567614 | 172.20.1.53 | 172.20.16.112 | TELNET | 55 | 1 byte data |
| 122 | 33.103611 | 172.20.1.53 | 172.20.16.112 | TELNET | 55 | 1 byte data |

Frame 81: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF... Ethernet II, Src: Dell_a9:c3:af (f8:b1:56:a9:c3:af), Dst: Cisco_2c:e0:c0 (18:33:9d:2c:e0:c0) Internet Protocol Version 4, Src: 172.20.1.53, Dst: 172.20.16.112 Transmission Control Protocol, Src Port: 49889, Dst Port: 23, Seq: 32, Ack: 80, Len: 1 Telnet

0000 18 33 9d 2c e0 c0 f8 b1 56 a9 c3 af 08 00 45 00 .3.....V.....E.
0010 00 29 56 5a 40 00 80 06 00 00 ac 14 01 35 ac 14 .)VZ@.....5..
0020 10 70 c2 e1 00 17 34 73 fd 6b 77 cf df cd 50 18 p....4s..kw...P..
0030 fa a1 69 c5 00 00 61a

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

Wireshark interface showing a packet capture on the 'telnet' filter. The packet list shows multiple Telnet packets from 172.20.17.2 to 172.20.6.174. Packet 2356 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-------------|--------------|--------------|----------|--------|-----------------|
| 2158 | 313.5845640 | 172.20.6.174 | 172.20.17.2 | TELNET | 66 | Telnet Data ... |
| 2159 | 313.5845650 | 172.20.6.174 | 172.20.17.2 | TELNET | 73 | Telnet Data ... |
| 2160 | 313.5845650 | 172.20.6.174 | 172.20.17.2 | TELNET | 96 | Telnet Data ... |
| 2162 | 313.6037430 | 172.20.17.2 | 172.20.6.174 | TELNET | 57 | Telnet Data ... |
| 2165 | 313.8015500 | 172.20.17.2 | 172.20.6.174 | TELNET | 72 | Telnet Data ... |
| 2166 | 313.8043560 | 172.20.6.174 | 172.20.17.2 | TELNET | 60 | Telnet Data ... |
| 2167 | 313.8045630 | 172.20.17.2 | 172.20.6.174 | TELNET | 64 | Telnet Data ... |
| 2175 | 316.6140730 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2176 | 316.6164430 | 172.20.6.174 | 172.20.17.2 | TELNET | 60 | Telnet Data ... |
| 2178 | 316.8858870 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2179 | 316.8876140 | 172.20.6.174 | 172.20.17.2 | TELNET | 60 | Telnet Data ... |
| 2182 | 317.2538860 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2183 | 317.2555430 | 172.20.6.174 | 172.20.17.2 | TELNET | 60 | Telnet Data ... |
| 2186 | 317.5418920 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2187 | 317.5473130 | 172.20.6.174 | 172.20.17.2 | TELNET | 60 | Telnet Data ... |
| 2189 | 317.7499200 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2190 | 317.7571310 | 172.20.6.174 | 172.20.17.2 | TELNET | 60 | Telnet Data ... |
| 2193 | 318.2938690 | 172.20.17.2 | 172.20.6.174 | TELNET | 56 | Telnet Data ... |
| 2194 | 318.2953070 | 172.20.6.174 | 172.20.17.2 | TELNET | 66 | Telnet Data ... |
| 2356 | 332.6459110 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2361 | 333.8618480 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2367 | 334.6938520 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2378 | 335.1737370 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2387 | 336.1178770 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2390 | 336.4217980 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2395 | 336.7897450 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2399 | 337.1898170 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2403 | 337.3977940 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2406 | 337.8298580 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2409 | 338.4058390 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2411 | 338.6776770 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2413 | 339.1096280 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2416 | 339.3195450 | 172.20.17.2 | 172.20.6.174 | TELNET | 55 | Telnet Data ... |
| 2421 | 339.9737460 | 172.20.17.2 | 172.20.6.174 | TELNET | 56 | Telnet Data ... |
| 2422 | 339.9861870 | 172.20.17.2 | 172.20.6.174 | TELNET | 63 | Telnet Data ... |

Frame 2356: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0 Ethernet II, Src: HewlettP_cb:5c:53 (b4:b5:2f:cb:5c:53), Dst: Cisco_cf:f4:c0 (f4:7f:35:cf:f4:c0) Internet Protocol Version 4, Src: 172.20.17.2 (172.20.17.2), Dst: 172.20.6.174 (172.20.6.174) Transmission Control Protocol, Src Port: 60696 (60696), Dst Port: 23 (23), Seq: 39, Ack: 97, Len: 1 Telnet

0000 f4 7f 35 cf f4 c0 b4 b5 2f cb 5c 53 08 00 45 00 ..5....../.\S..E.
0010 00 29 10 2a 40 00 80 06 00 00 ac 14 11 02 ac 14 .).*@.....
0020 06 ae ed 18 00 17 35 fa a5 69 53 dd 5f 0b 50 185..iS..P..
0030 fa 90 6f f4 00 00 52R

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

Le mot de passe est transmis du pc vers le switch sans être crypté.

- ✓ Proposer un protocole de communication sécurisé.

Il existe SSH

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**).

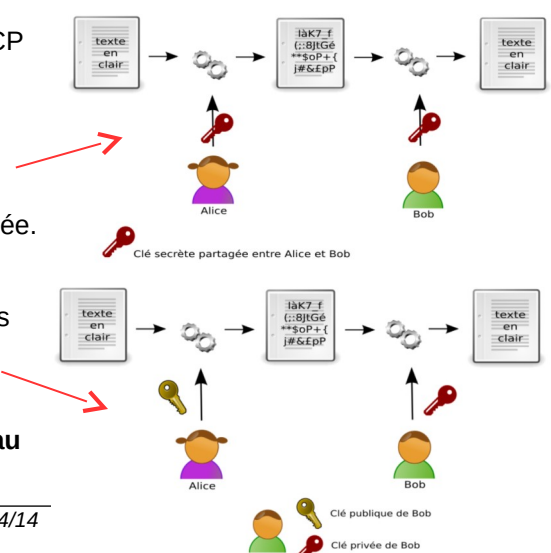
SSH est un protocole, c'est-à-dire une méthode standard permettant à des machines d'établir une communication sécurisée. A ce titre, il existe de nombreuses implémentations de clients et de serveurs SSH. Certains sont payants, d'autres sont gratuits ou *open source*.

• 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

```
ACCES RESERVE PRIVE

User Access Verification

Username:
Username: etudiant
Password:
THEPOT>ena
Password:
THEPOT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
THEPOT(config)#ip domain-name thepot.local
THEPOT(config)#exit
THEPOT#
*May  6 03:35:37.313: %SYS-5-CONFIG_I: Configured from console by etudiant on console
show run
Building configuration...

Current configuration : 1755 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname THEPOT
!
boot-start-marker
boot-end-marker
!
enable password 7 122B0A18061F04013A24307A636777
!
username etudiant password 7 00301B0314541F545F7319
username admin privilege 15 secret 5 $1$NG6o$SUa7QcxPUDlpTzbnzPslY/
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
!
ip domain-name thepot.local
ip name-server 172.20.6.254
```

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]
```

```
THEPOT#
THEPOT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
THEPOT(config)#ip ssh version 2
Please create RSA keys to enable SSH (of atleast 768 bits size) to enable SSH v2.
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]

*May  6 03:40:48.128: %SSH-5-ENABLED: SSH 2.0 has been enabled
THEPOT(config)#
```

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
```


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

```
Switch(config)#username userssh password _____
```

5. Configuration de la connection SSH:

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

```
THEPOT(config)#line vty 0 4  
THEPOT(config-line)#login local  
THEPOT(config-line)#transport input ssh
```

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]

*May 6 03:40:48.128: %SSH-5-ENABLED: SSH 2.0 has been enabled

```
THEPOT(config)#username userssh password Rootthepot2025
```

```
THEPOT(config)#line vty 0 4
```

```
THEPOT(config-line)#login local
```

```
THEPOT(config-line)#transport input ssh
```

```
THEPOT(config-line)#
```

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)

Capturing from Ethernet 2 [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]

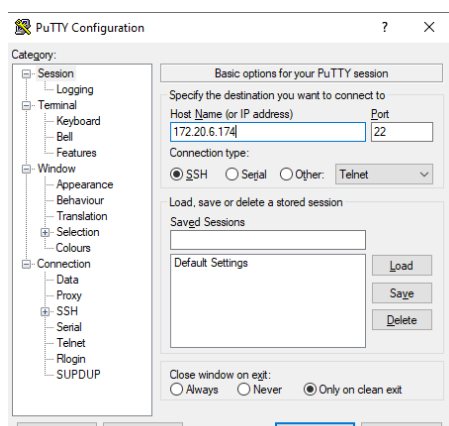
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ssh

Expression... Clear Apply Save

No. Time Source Destination Protocol Length Info

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



Filter: ssh

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-------------|--------------|--------------|----------|--------|---|
| 1825 | 213.4710420 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 73 | Server: Protocol (SSH-2.0-Cisco-1.25) |
| 1826 | 213.4761470 | 172.20.17.2 | 172.20.6.174 | SSHv2 | 82 | Client: Protocol (SSH-2.0-PuTTY_Release_0.76) |
| 1827 | 213.4814200 | 172.20.17.2 | 172.20.6.174 | SSHv2 | 1310 | Client: Key Exchange Init |
| 1828 | 213.4820720 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 334 | Server: Key Exchange Init |
| 1859 | 218.7678740 | 172.20.17.2 | 172.20.6.174 | SSHv2 | 198 | Client: Diffie-Hellman Key Exchange Init |
| 1861 | 219.0056210 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 502 | Server: Diffie-Hellman Key Exchange Reply |
| 1862 | 219.0085930 | 172.20.17.2 | 172.20.6.174 | SSHv2 | 106 | New Keys |
| 1863 | 219.0086320 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 70 | Server: New Keys |
| 1866 | 219.0115940 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 106 | Server: Encrypted packet (len=52) |
| 2010 | 238.7722260 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 122 | Server: Encrypted packet (len=68) |
| 2012 | 238.7747220 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 122 | Server: Encrypted packet (len=68) |
| 2045 | 253.4608670 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 90 | Server: Encrypted packet (len=36) |
| 2047 | 253.4671890 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 106 | Server: Encrypted packet (len=52) |
| 2049 | 253.4690680 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 90 | Server: Encrypted packet (len=36) |
| 2050 | 253.4699010 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 90 | Server: Encrypted packet (len=36) |
| 2052 | 253.4710710 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 122 | Server: Encrypted packet (len=68) |
| 2053 | 253.4719200 | 172.20.6.174 | 172.20.17.2 | SSHv2 | 106 | Server: Encrypted packet (len=52) |

```
login as: userssh  
Keyboard-interactive authentication prompts from server:  
Passwords:  
End of keyboard-interactive prompts from server  
ACCESS RESERVE PRIVE  
THEPOT#
```

AMEDO
Source :

Capture en cours de Ethernet

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

ssh

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|---------------|---------------|----------|--------|---|
| 370 | 331.057453 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 73 | Server: Protocol (SSH-2.0-Cisco-1.25) |
| 371 | 331.057588 | 172.20.1.53 | 172.20.16.112 | SSHv2 | 82 | Client: Protocol (SSH-2.0-PuTTY_Release_0.82) |
| 372 | 331.059649 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 334 | Server: Key Exchange Init |
| 373 | 331.060062 | 172.20.1.53 | 172.20.16.112 | SSHv2 | 1694 | Client: Key Exchange Init |
| 384 | 337.318149 | 172.20.1.53 | 172.20.16.112 | SSHv2 | 198 | Client: Diffie-Hellman Key Exchange Init |
| 386 | 337.554445 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 502 | Server: Diffie-Hellman Key Exchange Reply |
| 387 | 337.555183 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 70 | Server: New Keys |
| 403 | 344.997164 | 172.20.1.53 | 172.20.16.112 | SSHv2 | 106 | Client: New Keys, Encrypted packet (len=36) |
| 404 | 344.997256 | 172.20.1.53 | 172.20.16.112 | SSHv2 | 142 | Client: Encrypted packet (len=88) |
| 405 | 345.000136 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 106 | Server: Encrypted packet (len=52) |
| 423 | 360.993982 | 172.20.1.53 | 172.20.16.112 | SSHv2 | 158 | Client: Encrypted packet (len=104) |
| 424 | 360.996059 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 122 | Server: Encrypted packet (len=68) |
| 425 | 360.996221 | 172.20.1.53 | 172.20.16.112 | SSHv2 | 190 | Client: Encrypted packet (len=136) |
| 426 | 361.009122 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 122 | Server: Encrypted packet (len=68) |
| 443 | 372.905984 | 172.20.1.53 | 172.20.16.112 | SSHv2 | 354 | Client: Encrypted packet (len=300) |
| 444 | 372.908690 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 90 | Server: Encrypted packet (len=36) |
| 445 | 372.909199 | 172.20.1.53 | 172.20.16.112 | SSHv2 | 158 | Client: Encrypted packet (len=104) |
| 446 | 372.911202 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 106 | Server: Encrypted packet (len=52) |
| 447 | 372.911434 | 172.20.1.53 | 172.20.16.112 | SSHv2 | 242 | Client: Encrypted packet (len=188) |
| 448 | 372.917109 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 90 | Server: Encrypted packet (len=36) |
| 449 | 372.917938 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 90 | Server: Encrypted packet (len=36) |
| 451 | 372.919150 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 122 | Server: Encrypted packet (len=68) |
| 452 | 372.919880 | 172.20.16.112 | 172.20.1.53 | SSHv2 | 106 | Server: Encrypted packet (len=52) |

> Frame 370: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF...
 > Ethernet II, Src: Cisco_2c:e0:c0 (18:33:9d:2c:e0:c0), Dst: Dell_a9:c3:af (f8:b1:56:a9:c3:af)
 > Internet Protocol Version 4, Src: 172.20.16.112, Dst: 172.20.1.53
 > Transmission Control Protocol, Src Port: 22, Dst Port: 49901, Seq: 1, Ack: 1, Len: 19
 > SSH Protocol

0000 f8 b1 56 a9 c3 af 18 33 9d 2c e0 c0 08 00 45 c0 ...V....3...E...
 0010 00 3b ad 9b 00 00 ff 06 a3 93 ac 14 10 70 ac 14 ...:.....:..p...
 0020 01 35 00 16 c2 ed cd 08 f6 36 08 1f ed 36 50 18 ...S.....6...6P...
 0030 10 20 28 f9 00 00 53 53 48 2d 32 2e 30 2d 43 69 ...(.SS H-2.0-Ci...
 0040 73 63 6f 2d 31 2e 32 35 0a ...sco-1.25...

Ethernet: <live capture in progress> Paquets: 476 - Affichés: 23 (4.8%) Profil: Default

✓ SSH est il un protocole de communication sécurisé ?

Oui, les paquets envoyés depuis l'ordinateur ou le switch sont encrypté grâce à une clé d'encryption

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

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

← → × 172.20.6.174 Rechercher

Les plus visités Débuter avec Firefox

172.20.6.174

Ce site vous demande de vous connecter.

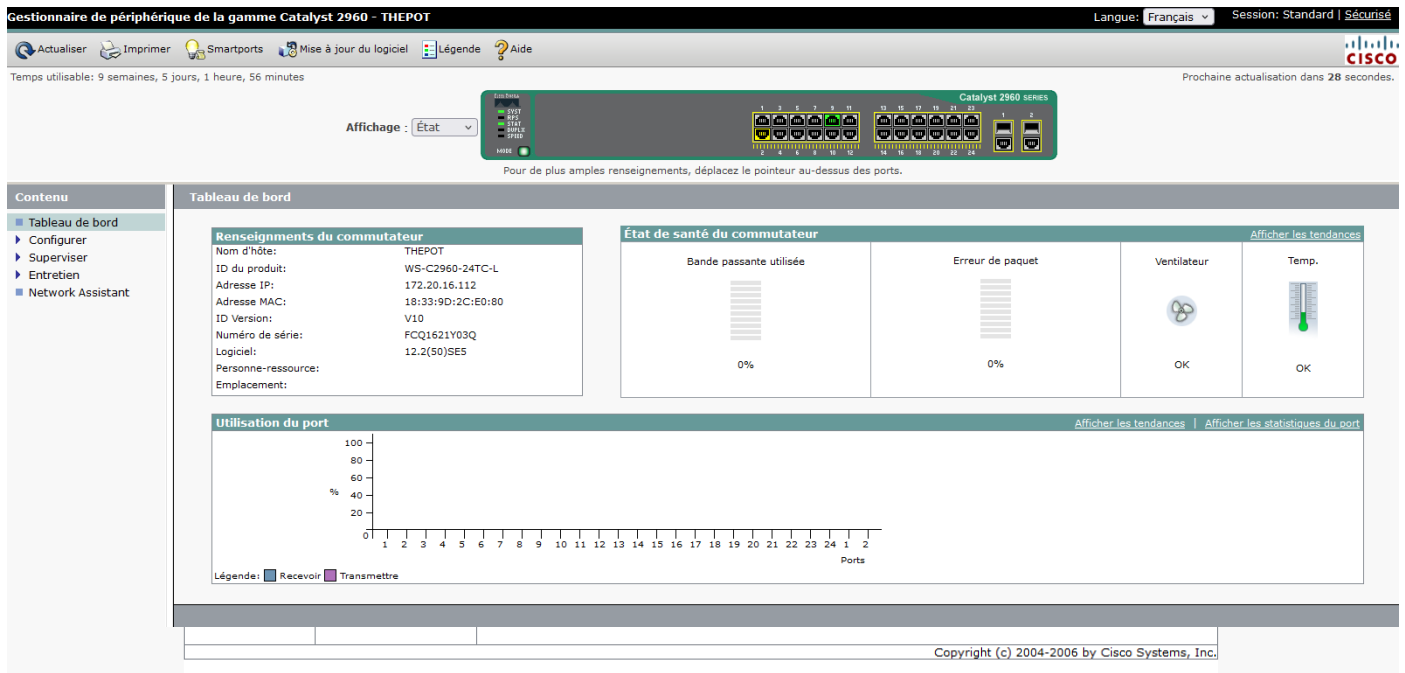
Nom d'utilisateur

Mot de passe

Connexion Annuler

Authentifiez vous (admin/Rootthepot20XX). Quelle indication vous est proposée ?

Lorsque qu'on s'identifie on arrive l'interface du switch, ce qui permet de le configurer, de pouvoir constater l'état des port, de le mettre à jour ect..

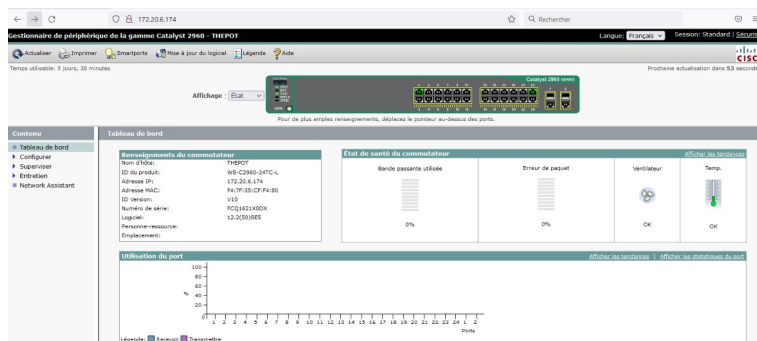


Que constatez vous ?

On peut configurer le switch comme par putty avec les ligne de commande mais en version interface graphique

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



FIN DU 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>
```