

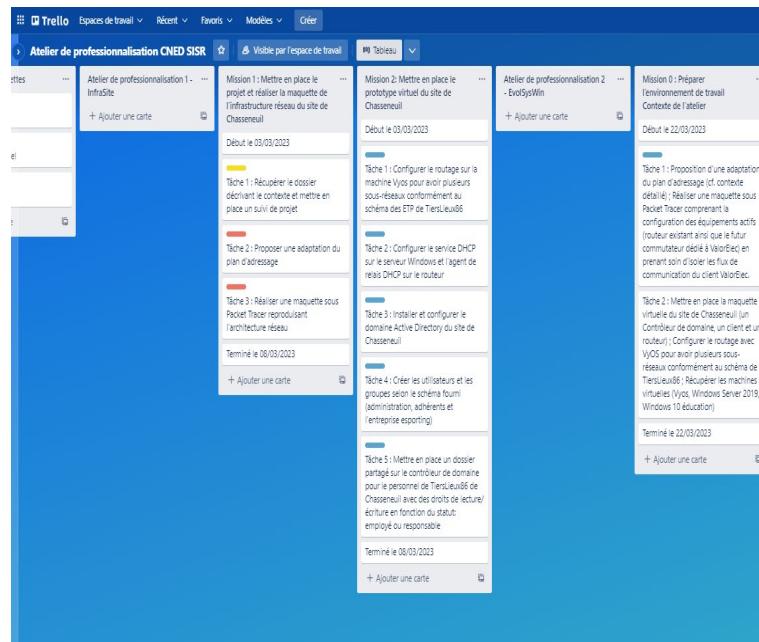
Atelier de professionnalisation 3

EvollInfra

Sommaire

Contexte.....	2
Partie 1 : Améliorer la gestion globale des équipements d'interconnexion	3
Mission 1 : Maquettage et Serveur NTP	3
Mission 2 : sauvegarde des équipements réseaux.....	36
Mission 3 : segmentation du réseau	54
Mission 4 : centralisation des journaux	66
Partie 2 : Mettre en place la haute-disponibilité et la sécurisation des équipements d'interconnexion	23
Mission 5 : tolérance aux pannes	76
Mission 6 : amélioration de la bande passante	80
Mission 7 : tolérance aux pannes des commutateurs	89
Mission 8 : tolérance aux pannes des routeurs	93
Sources (Partie 1)	75
Sources (Partie 2)	100

Cet atelier de professionnalisation se concentre sur l'évolution de l'infrastructure réseau du site de Chasseneuil. Pour un suivi du projet reportez-vous au Trello en cliquant [ici](#) ou sur l'image.



Contexte

Le cahier des charges du projet dénommé **EvolInfra**, que TiersLieux86 a confié à IT Services86 vaut pour l'étude, le maquettage et la validation d'une solution d'agrandissement du site de Chasseneuil. Il s'agit dans un premier temps d'améliorer la gestion globale des équipements d'interconnexion et d'assurer une meilleure sécurité du réseau.

Dans un deuxième temps, TiersLieux86 désire étudier la mise en place de la tolérance de pannes de ses équipements réseaux tout en améliorant la bande passante. Le but étant de réaliser une maquette opérationnelle qui sera ensuite déployée après l'acquisition des nouveaux matériels nécessaires. Le technicien informatique de TiersLieux86 n'a ni le temps ni les compétences techniques pointues pour se pencher sur ces questions d'infrastructure réseau.

Cet atelier professionnel se décompose en deux parties contenant différentes missions. L'une de ses parties est orientée sur l'optimisation de la gestion globale des équipements d'interconnexion alors que l'autre est penchée sur la haute disponibilité et la sécurisation des équipements d'interconnexion.

Partie 1 : Améliorer la gestion globale des équipements d'interconnexion

Mission 1 : Maquettage et Serveur NTP

Cette mission se concentre sur la création d'un serveur NTP (Network Time Protocol) pour synchroniser l'horloge des différents équipements que nous retrouvons sur notre maquette.

Mais qu'est-ce que le NTP ?

Le serveur NTP est un serveur qui donne à ses clients une heure de référence. Cela permet la synchronisation des horloges internes des machines. Mais au-delà de ça, c'est utile dans le cas d'une centralisation de logs car les machines retourneront alors des logs sur un serveur dédié à cela et de manière synchronisée, amenant un confort et une efficacité lors de leur lecture. De plus, synchroniser le temps permet de générer la programmation des sauvegardes, ainsi tous les équipements feront leur sauvegarde sur le même créneau horaire. Des serveurs NTP sont disponibles à l'image de ntp.u-strasbg.fr via l'IP 130.79.14.177. Or nous souhaitons dans notre cas que le serveur NTP fasse partie de notre réseau et pour nos machines seulement.

Tâche 1

Cette tâche consiste en la configuration basique des éléments de notre maquette qui ressemble pour le moment à cela.

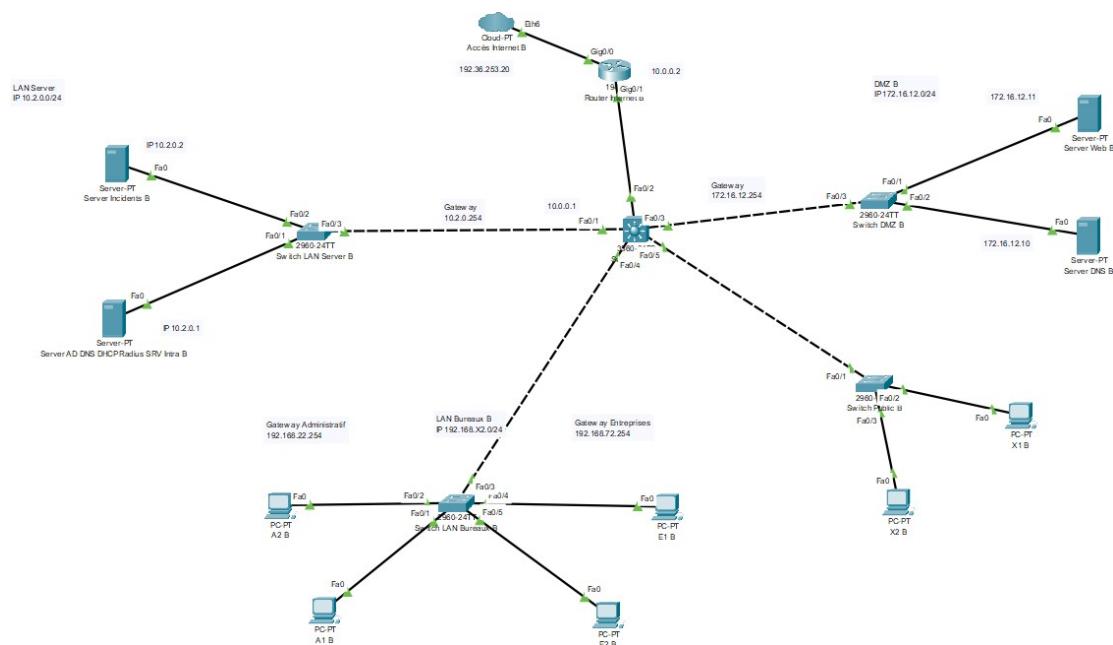


Figure 1 : Maquette

Voici une liste des différents objectifs à réaliser lors de cette tâche :

- Les équipements doivent posséder un nom unique explicite ;
- Ils doivent être configurés en tant que clients NTP (Network Time Protocol) afin de faciliter la gestion des logs de TiersLieux86 ;
- Une bannière doit-être mise en place ;
- Le mot de passe console sera « **Cisco** » ;
- Le mot de passe privilégié sera « **ENP@ssw0rd** » ;
- Les équipements devront pouvoir être administrés par SSH2 avec le user « **admin** » et le mot de passe « **SSHP@ssw0rd** ».

Nous constatons dans un premier temps que les équipements possèdent déjà des noms explicite voici la liste des noms des équipements présents sur la maquette (de gauche à droite) :

Nom sur la maquette	HostName
Serveur Incident B Server AD DNS DHCP Radius SRV Intra B Switch LAN Server B PC Administratif A1 B et A2 B Switch LAN Bureaux B PC Entreprise E1 B et E2 B Switch Coeur (Switch central) Internet B Routeur Internet B Switch Public B PC Public X1 B et X2 B Switch DMZ B Serveur Web B Serveur DNS B	SwitchServer SwitchBureaux Switchcoeur RouterInternet Switchpublic Switch DMZ

~~Les équipements doivent posséder un nom unique explicite;~~

Protocole NTP

Le but est donc désormais de synchroniser l'horodatage des machines pour faciliter la lecture des logs qui ont déjà été facilités via l'implantation de noms uniques et concrets.

Cette tâche sera donc divisée en deux parties, l'une sera centrée sur Cisco Packet tracer alors que l'autre sera concentrée sur un environnement virtuel composé d'un routeur Vyos, d'un serveur Windows Server 2019 qui fera office de serveur de temps et de DHCP, DNS, AD ainsi que d'une machine cliente.

Cisco Packet Tracer

Nous devons créer un serveur de temps sur un serveur Windows ou Debian, sous Packet Tracer nous devons configurer un serveur pour accueillir le service NTP, donc ici notre serveur Incident B avec l'IP 10.2.0.2. Dans mon cas, ce sera le 10.2.0.1, ce qui ne change rien en soit puisque les deux serveurs sont synchronisés entre eux.

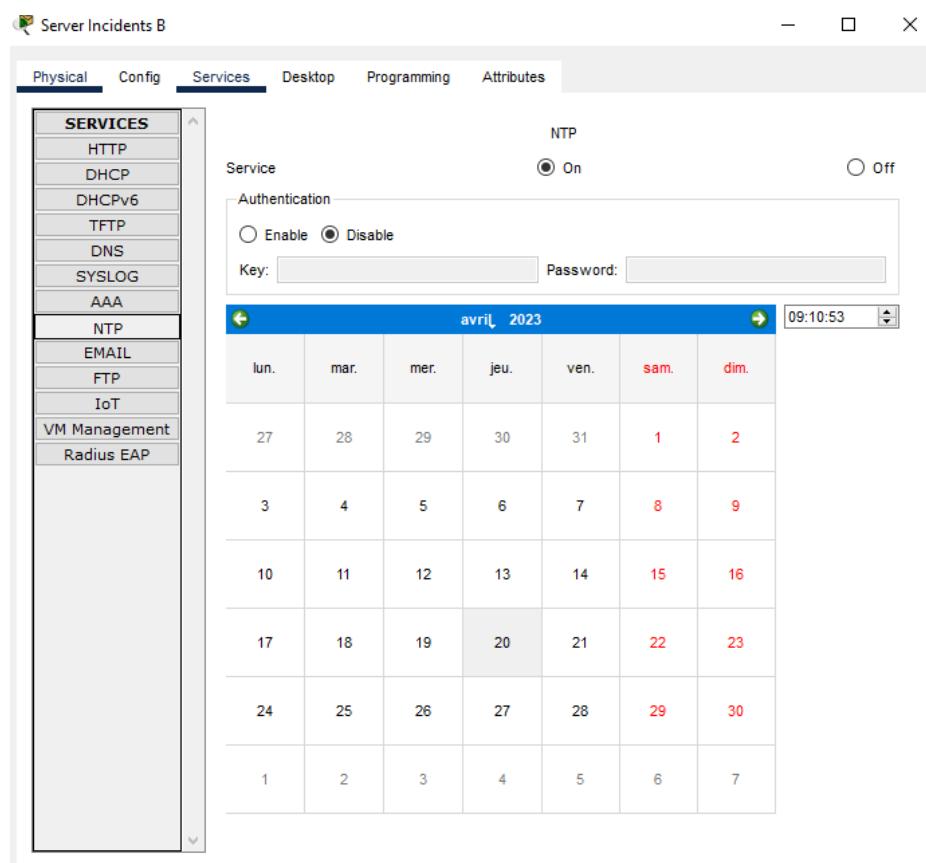


Figure 3 : Configuration 10.2.0.2 service NTP

Nous devons ensuite configurer le serveur NTP sur notre switch de couche 3 qui est le cœur du réseau via la commande :

```
enable
configure terminal
ntp server 10.2.0.2
exit
```

The screenshot shows a Cisco IOS Command Line Interface (CLI) window titled "Switch Coeur". The window has tabs for "Physical", "Config", "CLI" (which is selected), and "Attributes". The main area displays the following CLI session:

```
User Access Verification
Password:
Switchcoeur>en
Switchcoeur>enable
Password:
Switchcoeur#show ntp status
Clock is synchronized, stratum 2, reference is 10.2.0.1
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E79D0FC2.000001FD (21:14:42.509 UTC Mon Mar 20 2023)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 131.52 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 9 sec ago.
Switchcoeur#Switchcoeur#
Switchcoeur#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switchcoeur(config)#interface FastEthernet0/2
Switchcoeur(config-if)#Switchcoeur(config-if)#exit
Switchcoeur(config)#
Switchcoeur(config)#exit
Switchcoeur#
SYS-5-CONFIG_I: Configured from console by console

Switchcoeur#show ntp status
Clock is synchronized, stratum 2, reference is 10.2.0.1
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E79D1214.000002B7 (21:24:36.695 UTC Mon Mar 20 2023)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 140.40 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 4 sec ago.
Switchcoeur#
```

Figure 4 : Configuration NTP switch cœur

Une fois le switch l3 configuré nous configurons les switch l2 en tant que client eux aussi mais du switch l3, car la synchronisation ne serait pas exacte si nous configurons directement sur le 10.2.0.2. Nous utilisons donc l'adresse IP 192.168.1.254 pour configurer les autres clients. Nous faisons donc les commandes :

```
enable  
configure terminal  
ntp server 192.168.1.254
```

Ainsi le switch cœur fera office de serveur de temps pour le matériel qui lui est relié, tout en les synchronisant indirectement au serveur 10.2.0.2 qui est la référence.

Figure 5 Schéma NTP simplifié

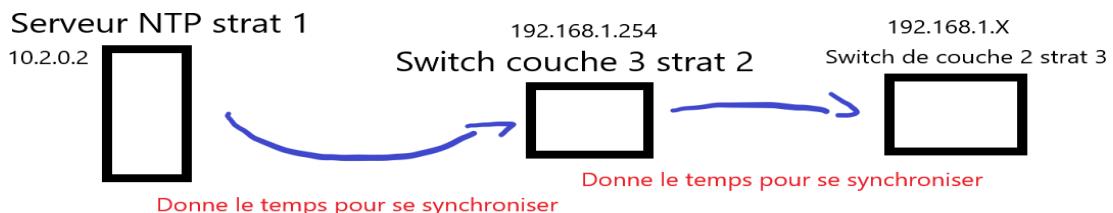
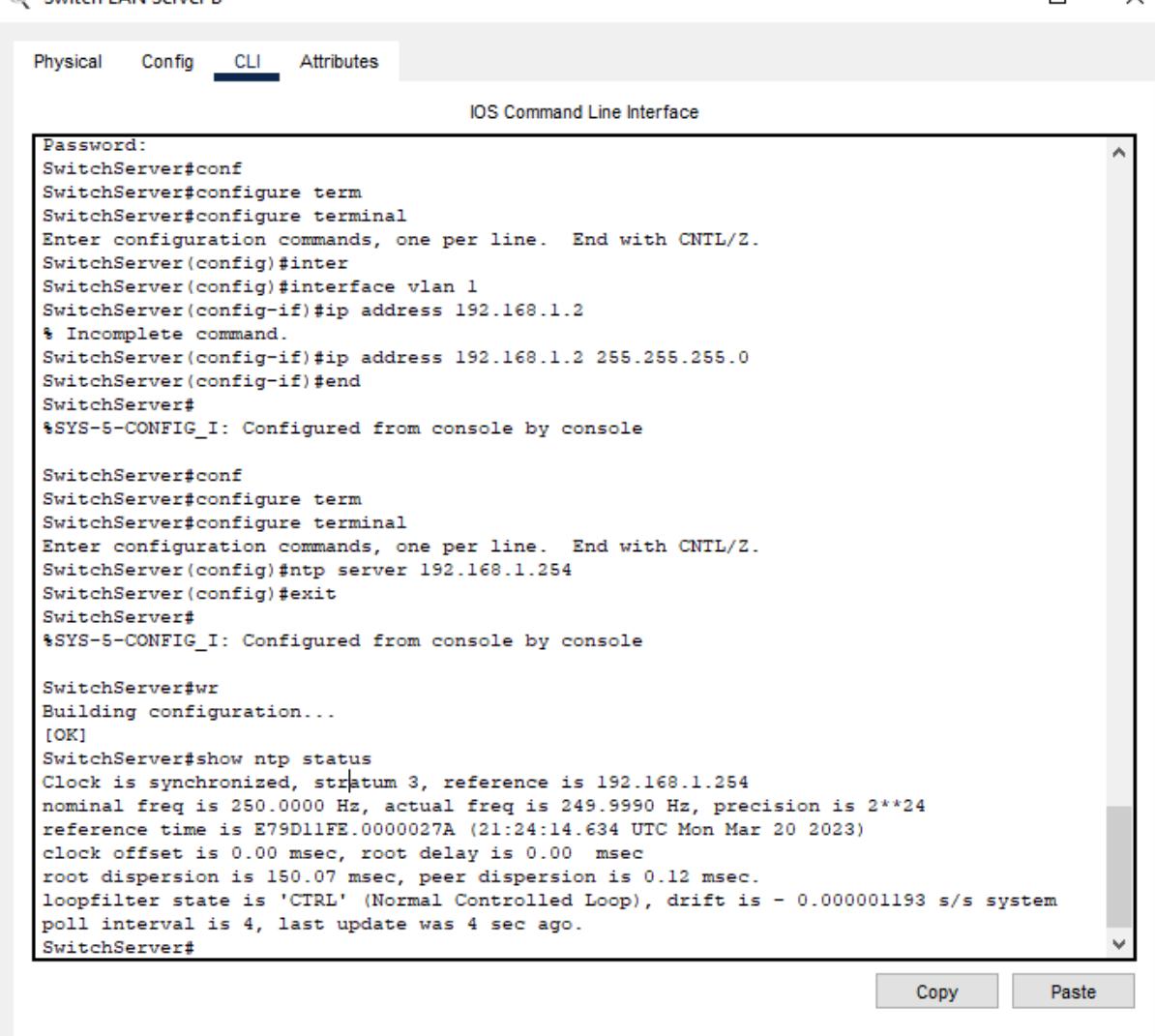


Schéma NTP simplifier

Ce qui donne le résultat suivant :



Switch LAN Server B

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Password:  
SwitchServer#conf  
SwitchServer#configure term  
SwitchServer#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
SwitchServer(config)#inter  
SwitchServer(config)#interface vlan 1  
SwitchServer(config-if)#ip address 192.168.1.2  
% Incomplete command.  
SwitchServer(config-if)#ip address 192.168.1.2 255.255.255.0  
SwitchServer(config-if)#end  
SwitchServer#  
%SYS-5-CONFIG_I: Configured from console by console  
  
SwitchServer#conf  
SwitchServer#configure term  
SwitchServer#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
SwitchServer(config)#ntp server 192.168.1.254  
SwitchServer(config)#exit  
SwitchServer#  
%SYS-5-CONFIG_I: Configured from console by console  
  
SwitchServer#wr  
Building configuration...  
[OK]  
SwitchServer#show ntp status  
Clock is synchronized, stratum 3, reference is 192.168.1.254  
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24  
reference time is E79D11FE.0000027A (21:24:14.634 UTC Mon Mar 20 2023)  
clock offset is 0.00 msec, root delay is 0.00 msec  
root dispersion is 150.07 msec, peer dispersion is 0.12 msec.  
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system  
poll interval is 4, last update was 4 sec ago.  
SwitchServer#
```

Copy Paste

Figure 6 : Configuration server NTP sur switch LAN server

Environnement virtuel

Nous devons donc désormais configurer notre serveur du site de Chasseneuil en tant que serveur référence pour le temps.

Pour cela nous passons par l'interface graphique de notre Server Windows 2019, nous faisons : win+r>regedit pour ouvrir l'éditeur de registre de la machine.

Nous nous rendons ensuite dans :

HKEY_LOCAL_MACHINE\CurrentControlSer\SYSTEM\Services\Win32time
\Config, après dans AnnounceFlags et double clic, puis nous modifions la valeur par 5 ;

Nous nous rendons après cela dans :

HKEY_LOCAL_MACHINE\CurrentControlSer\SYSTEM\Services\Win32time
\Parameters et choisissons NtpServer puis nous rentrons Chasseneuil.fr, nous entrons ensuite dans Type et changeons la valeur par NTP

Nous vérifions que dans :

HKEY_LOCAL_MACHINE\CurrentControlSer\SYSTEM\Services\Win32time
\TimeProvider la valeur de NTPServer et NTPClient soit sur Enabled. Si c'est le cas alors, la ligne finira par un 1

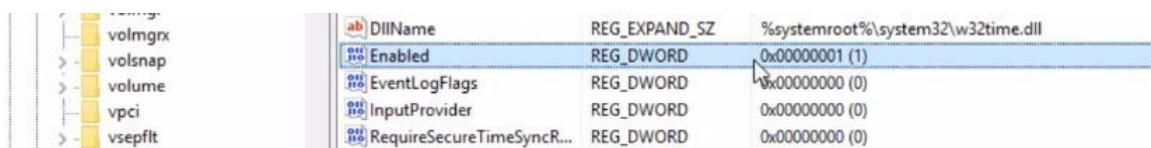


Figure 7 : Valeur Enabled pour NTPServer

Notre serveur de temps est donc configuré, nous devons ensuite redémarrer le service. Cela peut se faire dans le Command Prompt via la commande :

```
net stop w32time && net start w32time
```

Commande pour forcer l'arrêt et démarrer le service w32time

Nous pouvons ensuite vérifier la configuration via la commande :

```
w32tm /query /status
```

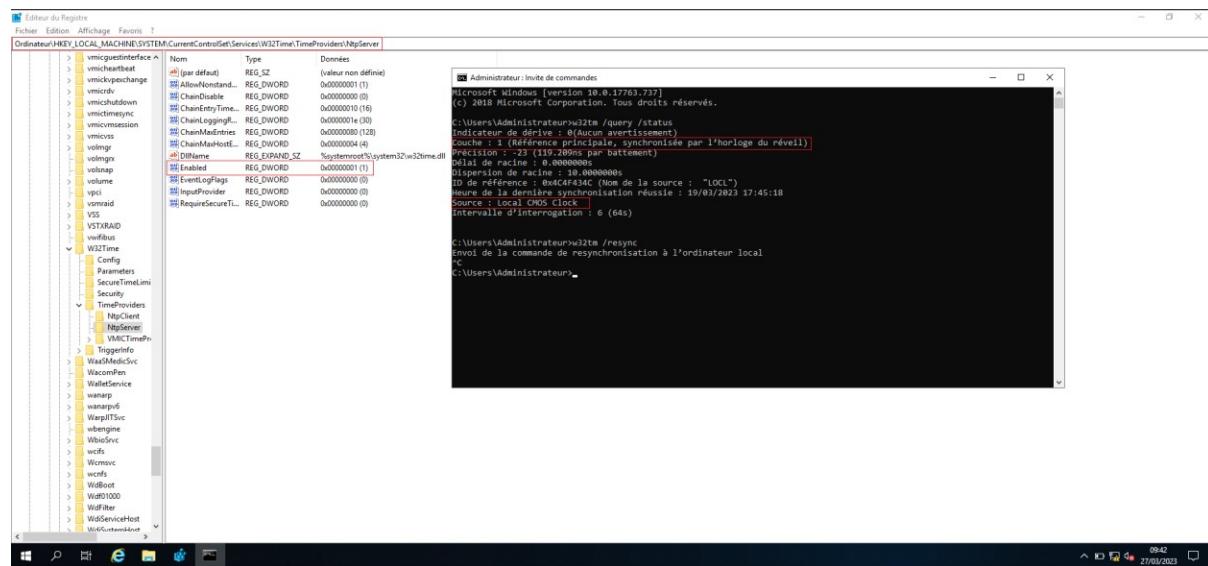


Figure 8 : Configuration du server NTP 1

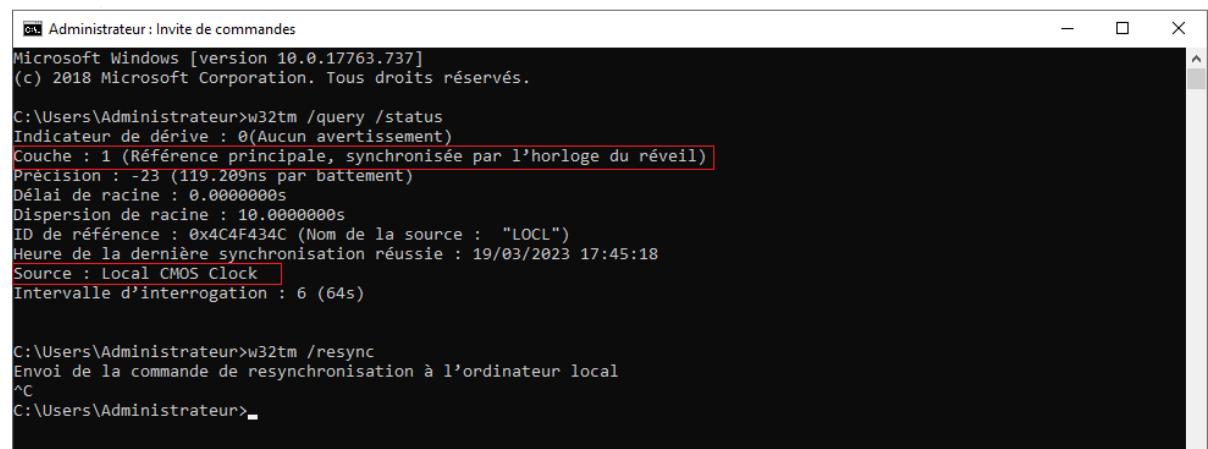
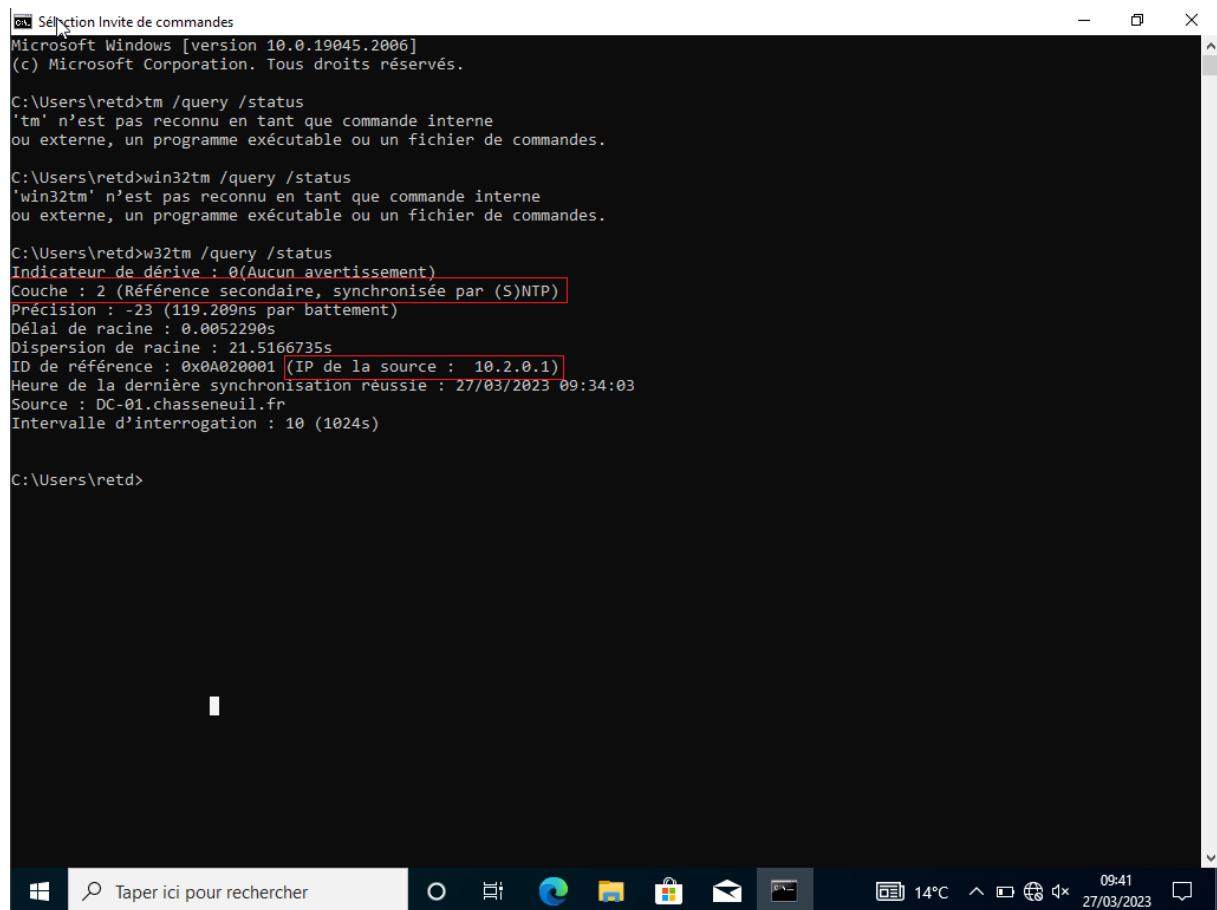


Figure 9 : Configuration du server NTP 2

Nous procédons ensuite à la vérification de la synchronisation avec un client Windows Server 2019. Nous exécutons la commande :

```
w32tm /query /status
```



```
C:\ Sélection Invite de commandes
Microsoft Windows [version 10.0.19045.2006]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\retd>tm /query /status
'tm' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\retd>win32tm /query /status
'win32tm' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\retd>w32tm /query /status
Indicateur de dérive : 0(Aucun avertissement)
Couche : 2 (Référence secondaire, synchronisée par (S)NTP)
Précision : -23 (119.209ns par battement)
Délai de racine : 0.0052290s
Dispersion de racine : 21.5166735s
ID de référence : 0x0A020001 [IP de la source : 10.2.0.1]
Heure de la dernière synchronisation réussie : 27/03/2023 09:34:03
Source : DC-01.chasseneuil.fr
Intervalle d'interrogation : 10 (1024s)

C:\Users\retd>
```

Figure 10 : Configuration du client

~~ils doivent être configurés en tant que clients NTP (Network Time Protocol) afin de faciliter la gestion des logs de Tiers Lieux⁸⁶~~

Point sur cette tâche :

Cette tâche était compliquée à mettre en place, le temps d'initialisation du protocole NTP est déstabilisant et le principe n'est pas simple à mettre en place. Le fait d'écrire, faire des schémas permet de mieux comprendre et ainsi de mettre en place de manière plus aisée.

Par ailleurs, des problèmes de perte de synchronisation sont visibles ce qui est très frustrant car le matériel initialement synchronisé ne l'est plus sans raison valable.

Bannière

Une bannière est un texte qui s'affiche lors de la connexion à un matériel. Ce texte a pour but dans notre cas de décourager les visiteurs se connectant au matériel réseau. Pour pouvoir mettre en place une bannière nous devons nous rendre sur les matériels qui devront en bénéficier, à savoir les commutateurs de couche 2 et 3 ainsi que le routeur. Une fois sur le matériel, nous devons entrer les commandes suivantes :

```
enable
configure terminal
banner motd "###"
L'Acces a cet equipement est strictement restreint aux seules personnes
Autorisees. Cet equipement est la propriete de TiersLieux86
Deconnectez-vous immediatement si vous n'etes pas une personne -----
autorisee-----"

Unauthorized access prohibited
Authorized access only
This system is the property of TiersLieux86 Disconnect IMMEDIATELY if
you are not an authorized user!
###" #Pour pouvoir délimiter la commande du texte nous séparons via " " ou "
```

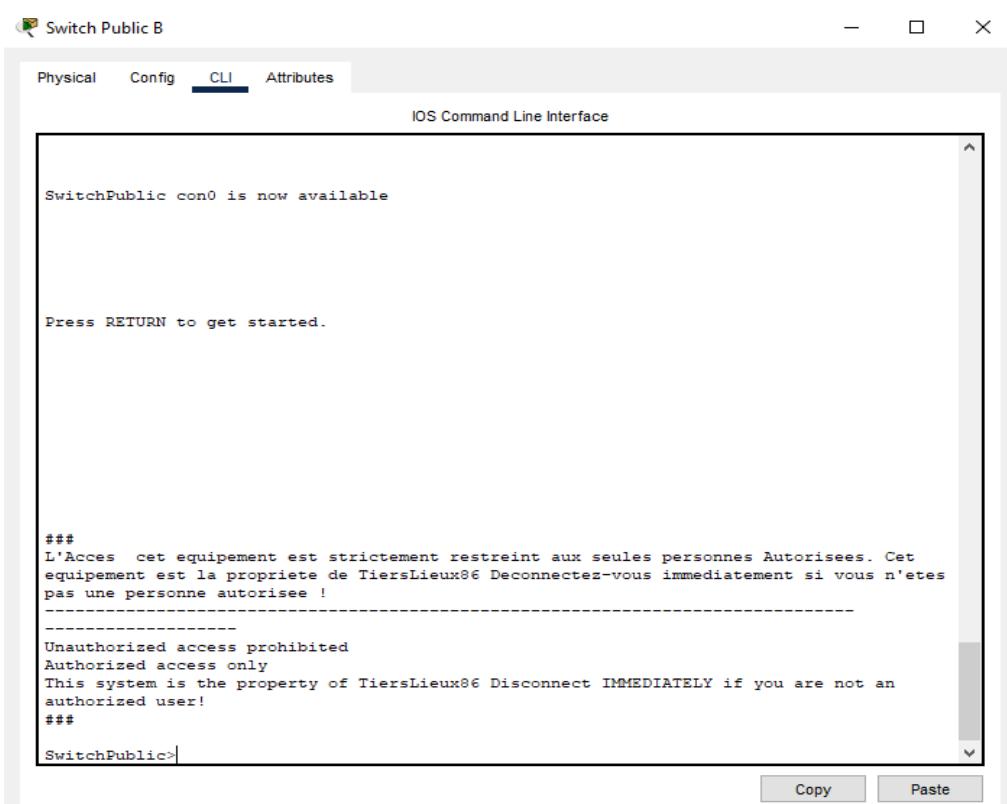


Figure 11 : Bannière Cisco Packet Tracer

Une bannière doit être mise en place

Mots de passe console et privilégié

L'objectif est désormais de mettre en place un mot de passe console qui sera demandé lors de l'accès à la console. Pour cela nous devons faire les commandes suivantes :

```
enable  
configure terminal  
line console 0  
login  
password Cisco #Cisco est le mot de passe
```

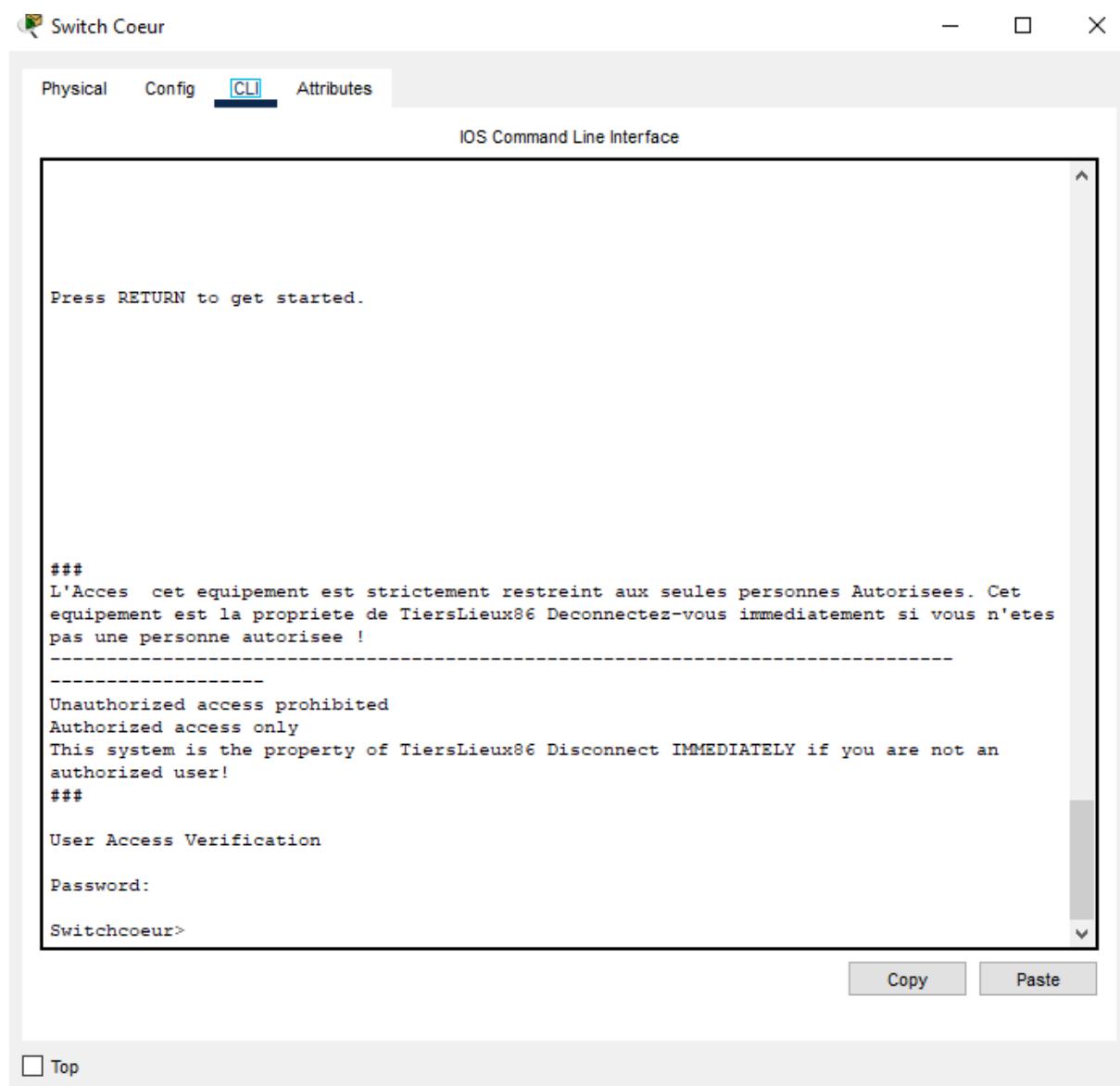


Figure 12 : Mise en place du mot de passe console

Le mot de passe console sera « **Cisco** »;

Nous devons ensuite mettre en place le mot de passe du mode privilégié qui est accessible grâce à la commande enable. Pour cela nous devons faire les commandes suivantes :

```
enable  
configure terminal  
enable password ENP@ssw0rd #ENP@ssw0rd est le mot de passe
```

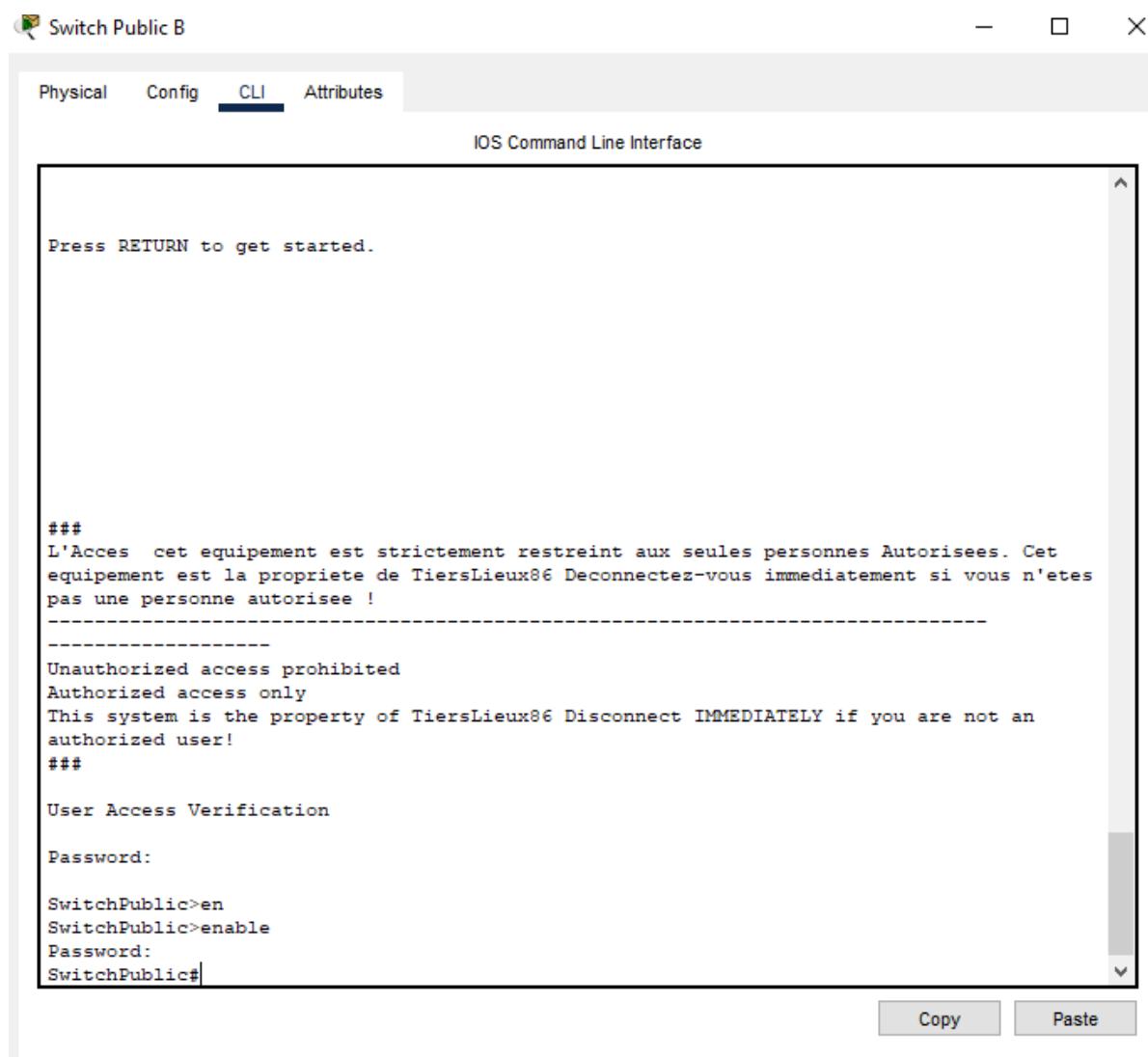


Figure 13 : Mise en place du mot de passe sur enable

~~Le mot de passe privilégié sera « ENP@ssw0rd »;~~

SSH

SSH permet d'administrer à distance le matériel, au même titre que l'interface web de celui- ci. L'interface web propose l'avantage de la facilité, plus simple d'utilisation mais moins adapté dans certaines situations, voire moins stable. Nous nous tournons donc vers l'accès à distance via un protocole. Reste le choix entre Telnet et SSH. Telnet n'étant pas sécurisé nous utiliserons en priorité SSH.

Nous verrons premièrement SSH pour les équipements sur Cisco Packet Tracer et ensuite SSH pour notre serveur Windows 2019.

Cisco Packet Tracer

Pour activer SSH nous devons d'abord vérifier si celui-ci est activé, pour cela nous devons faire la commande :

```
enable  
show ip ssh
```

Cette commande nous retourne un message dans lequel nous pouvons constater que SSH est activé ou non.

```
SSH Disabled - version 1.99  
%Please create RSA keys (of atleast 768 bits size) to enable SSH  
v2.  
Authentication timeout: 120 secs; Authentication retries: 3
```

Pour pouvoir activer SSH nous devons configurer le nom de notre switch...

```
enable  
configure terminal  
hostname SwitchBureaux  
exit
```

et son domaine.

```
enable  
configure terminal  
ip domain-name 10.2.0.1  
exit  
wr #permet de sauvegarder la configuration
```

Nous pouvons ensuite procéder à la configuration de notre service SSH sur l'appareil. Pour cela, nous devons faire les commandes suivantes :

```
enable
configure terminal
crypto key generate rsa general-keys modulus 1024
```

Ce qui nous retournera

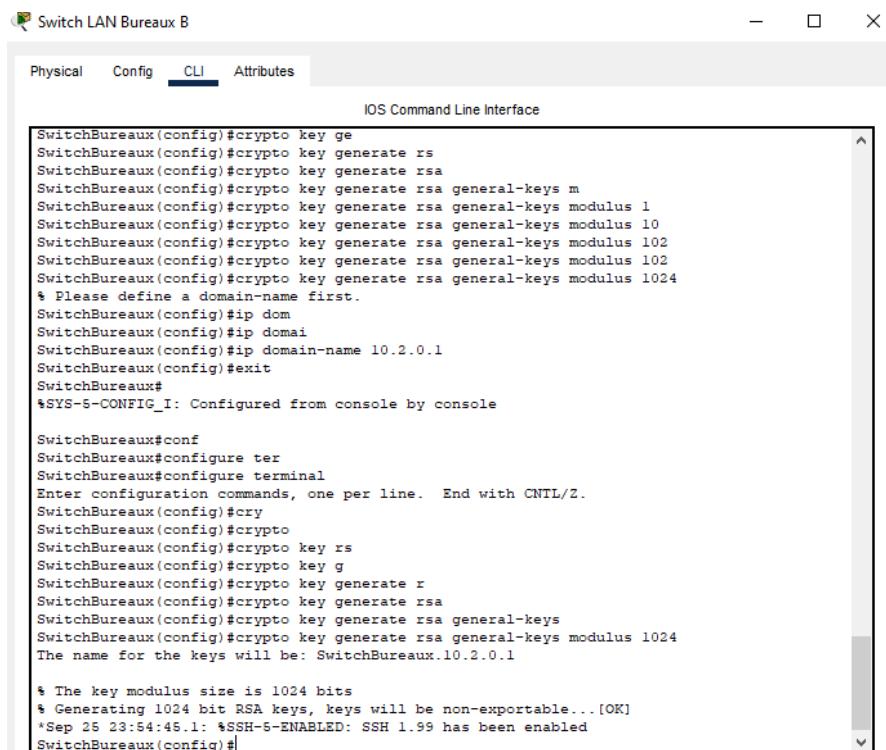
```
The name for the keys will be: SwitchBureaux.10.2.0.1
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Sep 25 23:54:45.1: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Nous pouvons désormais activer SSH2, pour cela nous faisons la commande suivante :

```
enable
configure terminal
ip ssh version 2
```

Et nous pouvons vérifier si la configuration a bien été prise avec :

```
enable
show ip ssh
```



The screenshot shows a window titled "Switch LAN Bureaux B" with the "CLI" tab selected. Below the tabs, it says "IOS Command Line Interface". The main area displays the following CLI session:

```
SwitchBureaux(config)#crypto key ge
SwitchBureaux(config)#crypto key generate rs
SwitchBureaux(config)#crypto key generate rsa
SwitchBureaux(config)#crypto key generate rsa general-keys m
SwitchBureaux(config)#crypto key generate rsa general-keys modulus 1
SwitchBureaux(config)#crypto key generate rsa general-keys modulus 10
SwitchBureaux(config)#crypto key generate rsa general-keys modulus 102
SwitchBureaux(config)#crypto key generate rsa general-keys modulus 102
SwitchBureaux(config)#crypto key generate rsa general-keys modulus 1024
% Please define a domain-name first.
SwitchBureaux(config)#ip dom
SwitchBureaux(config)#ip domai
SwitchBureaux(config)#ip domain-name 10.2.0.1
SwitchBureaux(config)#exit
SwitchBureaux#
*SYS-5-CONFIG_I: Configured from console by console

SwitchBureaux#conf
SwitchBureaux#configure ter
SwitchBureaux#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchBureaux(config)#cry
SwitchBureaux(config)#crypto
SwitchBureaux(config)#crypto key rs
SwitchBureaux(config)#crypto key g
SwitchBureaux(config)#crypto key generate r
SwitchBureaux(config)#crypto key generate rsa
SwitchBureaux(config)#crypto key generate rsa general-keys
SwitchBureaux(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: SwitchBureaux.10.2.0.1

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Sep 25 23:54:45.1: %SSH-5-ENABLED: SSH 1.99 has been enabled
SwitchBureaux(config)#+
```

Figure 14 : Création de la clé rsa pour SSH

The screenshot shows the Cisco IOS Command Line Interface (CLI) running on a device named 'SwitchBureaux'. The user is in configuration mode, specifically under the 'crypto' command. They are generating RSA keys with a modulus of 1024 bits. The session also includes configuration of IP addresses and domain names, and ends with a check of the current SSH configuration.

```
Physical Config CLI Attributes

IOS Command Line Interface

SwitchBureaux(config)#crypto key generate rsa general-keys modulus 1024
* Please define a domain-name first.
SwitchBureaux(config)#ip dom
SwitchBureaux(config)#ip domai
SwitchBureaux(config)#ip domain-name 10.2.0.1
SwitchBureaux(config)#exit
SwitchBureaux#
*SYS-5-CONFIG_I: Configured from console by console

SwitchBureaux#conf
SwitchBureaux#configure ter
SwitchBureaux#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchBureaux(config)#cry
SwitchBureaux(config)#crypto
SwitchBureaux(config)#crypto key rs
SwitchBureaux(config)#crypto key g
SwitchBureaux(config)#crypto key generate r
SwitchBureaux(config)#crypto key generate rsa
SwitchBureaux(config)#crypto key generate rsa general-keys
SwitchBureaux(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: SwitchBureaux.10.2.0.1

* The key modulus size is 1024 bits
* Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Sep 25 23:54:45.1: *SSH-5-ENABLED: SSH 1.99 has been enabled
SwitchBureaux(config)#ip ssh version 2
SwitchBureaux(config)#exit
SwitchBureaux#
*SYS-5-CONFIG_I: Configured from console by console

SwitchBureaux#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
SwitchBureaux#
```

Figure 15 : Vérification de la configuration de SSH

SSH est donc activé, il nous reste à créer un compte admin et lui associer le mot de passe SSHP@ssw0rd qui permettra l'administration. Pour cela nous devons faire les commandes suivantes :

```
enable
configure terminal
aaa new-model
aaa authentication login default local
aaa authorization exec default local
username admin password SSHP@ssw0rd
line vty 0 4 #permet d'activer les lignes virtuelles
transport input ssh #défini quel protocole est utilisé
login local #précise où se trouve la base des comptes utilisateurs
exit
exit
```

Switch Public B

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Press RETURN to get started!

###  
L'Acces cet equipement est strictement restreint aux seules personnes Autorisees. Cet  
equipement est la propriete de TiersLieux86 Deconnectez-vous immediatement si vous n'etes  
pas une personne autorisee !  
-----  
-----  
Unauthorized access prohibited  
Authorized access only  
This system is the property of TiersLieux86 Disconnect IMMEDIATELY if you are not an  
authorized user!  
###  
User Access Verification  
  
Username: admin  
Password:  
SwitchPublic>
```

Copy Paste

Figure 16 : Utilisation de l'identifiant récemment créé pour se connecter au switch

Nous pouvons ainsi nous connecter au matériel via SSH2, le compte “admin” doit-être renseigné ainsi que le mot de passe SSHP@ssw0rd ce qui donne :

```
C:\>ssh -l admin
Password: SSHP@ssw0rd
```

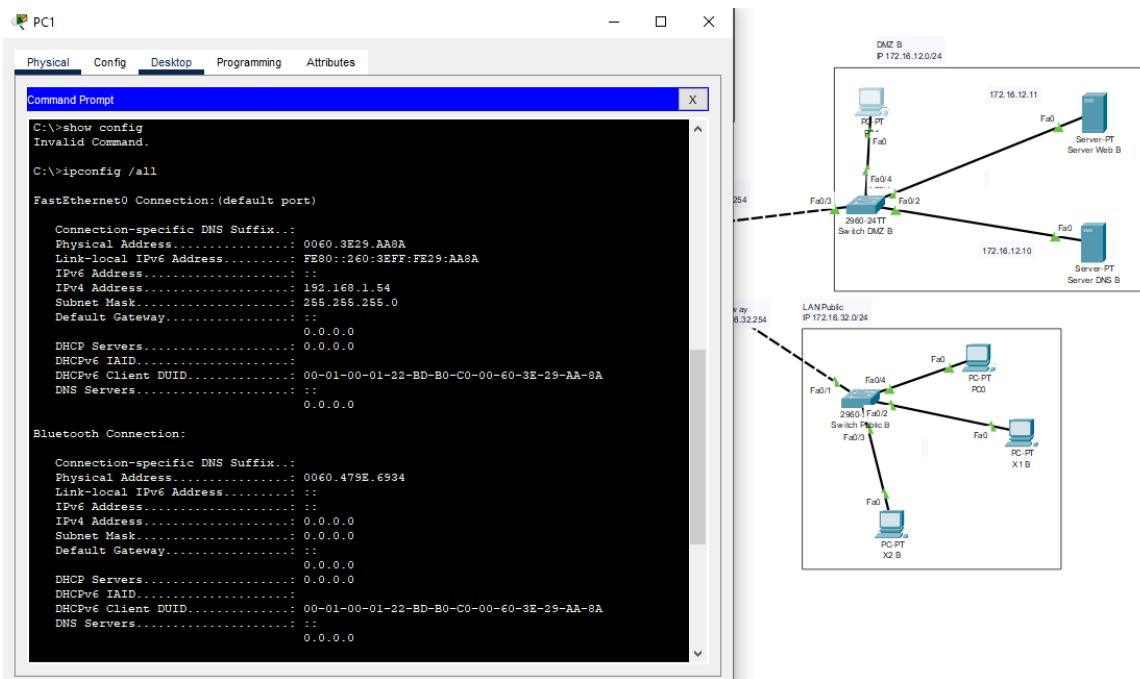


Figure 17 : Connexion via ssh de Pc01 sur le switch DMZ via l'IP 192.168.1.12

Nous pouvons ainsi via un pc adresser statiquement en 192.168.1.X manager les outils réseau à distance, cela peut se voir via la situation suivante.

Je me connecte sur le PC01 placé dans la DMZ (mais il pourrait être placé dans le LAN bureau ou encore dans le LAN public c'est à titre d'exemple), je me rend dans le “command prompt” et je vais me connecter en ssh sur le switch LANPublic adresser en 192.168.1.32 (cette adresse est mise en rapport avec le vlan pour éviter de trop se perdre).

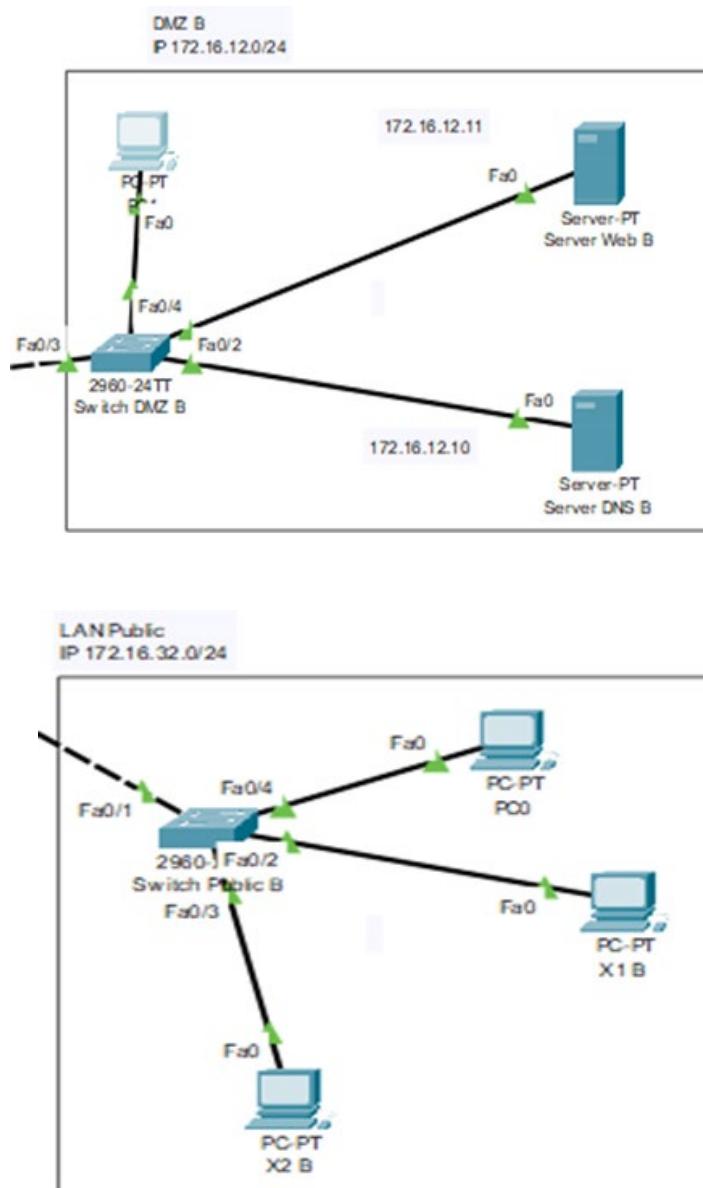
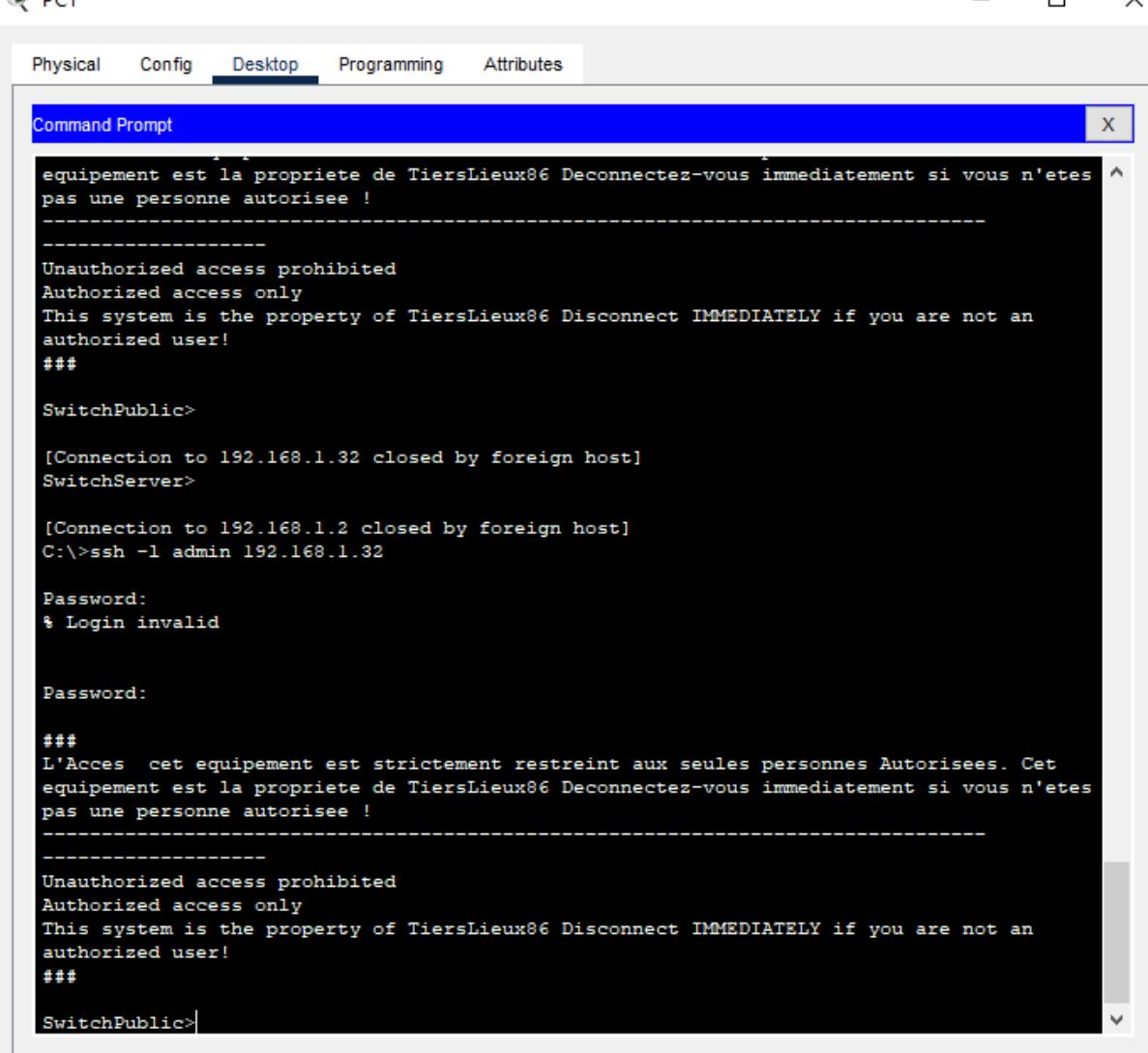


Figure 18 : PC01

Je fais donc la commande ssh -l admin 192.168.1.32 et un mot de passe m'est demandé. Je rentre donc le mot de passe que j'ai renseigné lors de la configuration du SSH à savoir SSHP@ssw0rd et je peux ainsi manager mon matériel bien que je ne sois pas dans le même bâtiment ou encore dans la même pièce.



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window has a blue header bar with the title and standard window controls (minimize, maximize, close). Below the header is a menu bar with tabs: Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is currently selected. The main area of the window is a black terminal-like interface displaying the following text:

```
equipement est la propriete de TiersLieux86 Deconnectez-vous immediatement si vous n'etes pas une personne autorisee !
-----
Unauthorized access prohibited
Authorized access only
This system is the property of TiersLieux86 Disconnect IMMEDIATELY if you are not an authorized user!
###

SwitchPublic>

[Connection to 192.168.1.32 closed by foreign host]
SwitchServer>

[Connection to 192.168.1.2 closed by foreign host]
C:\>ssh -l admin 192.168.1.32

Password:
% Login invalid

Password:

###
L'Acces cet equipement est strictement restreint aux seules personnes Autorisees. Cet equipement est la proprieté de TiersLieux86 Deconnectez-vous immediatement si vous n'etes pas une personne autorisee !
-----
Unauthorized access prohibited
Authorized access only
This system is the property of TiersLieux86 Disconnect IMMEDIATELY if you are not an authorized user!
###

SwitchPublic>
```

Figure 20 : Connexion au switch du LANPublic 192.168.1.32

Environnement Virtuel

Le but de cette mise en place est de pouvoir se connecter en SSH sur notre serveur. La première difficulté résidait dans l'installation du service serveur Open SSH. En effet, il est possible de l'installer via PowerShell mais aussi via l'interface graphique des fonctionnalités facultatives. La commande suivante permet l'installation du service :

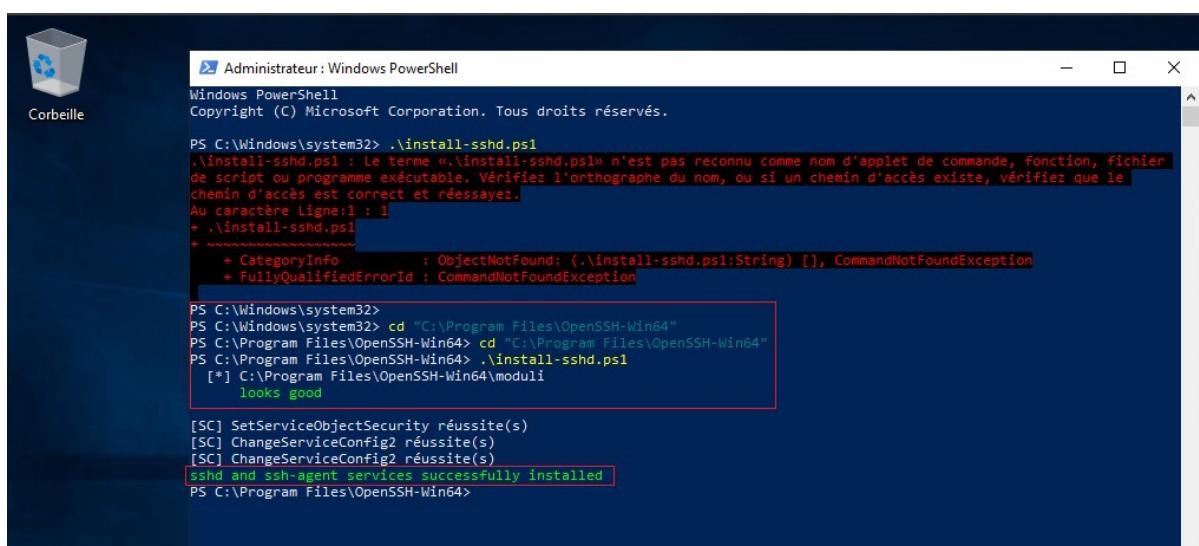
```
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
```

Or rien ne se passait lors de l'exécution de la commande en question, j'ai donc opté pour une Installation graphique, mais un message d'erreur m'était retourné, me signalant que le compte administrateur local ne possédait pas les droits nécessaires.

Je me suis donc rendu dans le secpol.msc via win+r et stratégie locale> Option de sécurité> Contrôle de compte utilisateur : utiliser le mode Approbation administrateur pour le compte Administrateur intégré. Je me suis déconnecté et reconnecté et le message d'erreur ne m'est plus retourné.

Un autre problème est survenu, le téléchargement se lançait sans se finir, j'ai donc dû télécharger le fichier via GitHub ([lien du fichier](#)), j'ai ensuite décompresser le fichier dans mon dossier Programme Files ait fait les commandes suivantes dans PowerShell en mode administrateur dans le but de recevoir le retour de commande témoignant de la bonne installation du service:

```
cd "C:\Program Files\OpenSSH-Win64" #se placer dans le répertoire  
.\\install-sshd.ps1 #installation du fichier
```



```
Administrator : Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. Tous droits réservés.  
  
PS C:\Windows\system32> .\\install-sshd.ps1  
.\\install-sshd.ps1 : Le terme «.\install-sshd.ps1» n'est pas reconnu comme nom d'applet de commande, fonction, fichier  
de script ou programme exécutable. Vérifiez l'orthographe du nom, ou si un chemin d'accès existe, vérifiez que le  
chemin d'accès est correct et réessayez.  
Au caractère Ligne:1 : 1  
+ .\\install-sshd.ps1  
+ ~~~~~  
+ CategoryInfo          : ObjectNotFound: (.\Install-sshd.ps1:String) [], CommandNotFoundException  
+ FullyQualifiedErrorId : CommandNotFoundException  
  
PS C:\Windows\system32>  
PS C:\Windows\system32> cd "C:\Program Files\OpenSSH-Win64"  
PS C:\Program Files\OpenSSH-Win64> cd "C:\Program Files\OpenSSH-Win64"  
PS C:\Program Files\OpenSSH-Win64> .\\install-sshd.ps1  
[*] C:\Program Files\OpenSSH-Win64\modules  
    looks good  
  
[SC] SetServiceObjectSecurity réussite(s)  
[SC] ChangeServiceConfig2 réussite(s)  
[SC] ChangeServiceConfig2 réussite(s)  
sshd and ssh-agent services successfully installed  
PS C:\Program Files\OpenSSH-Win64>
```

Figure 21 : Installation du fichier OpenSSH Server

J'ai ensuite modifié la configuration en tant que démarrage automatique pour ne pas avoir à démarrer le service manuellement à chaque redémarrage du serveur.

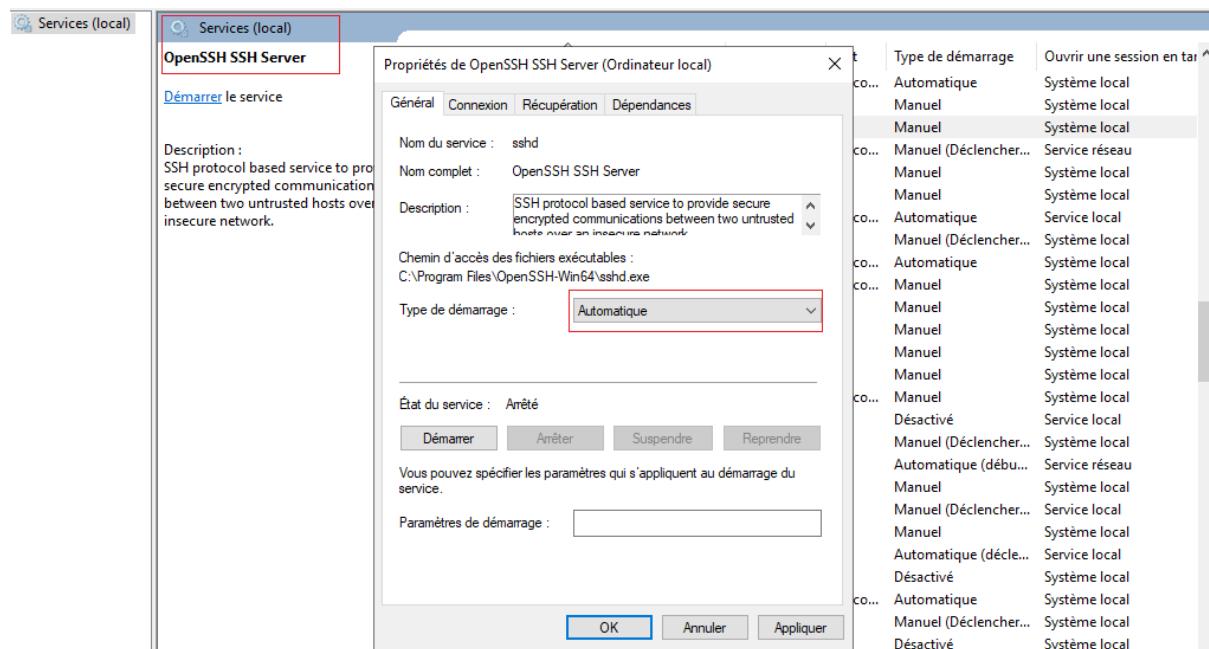


Figure 22 : Configuration SSH n°1

Nous devons ensuite continuer les configurations. En effet, nous devons premièrement redémarrer le serveur pour avoir tous les dossiers. Nous nous rendons ensuite dans le disque local C nous rendons les éléments masqués visibles et allons dans ProgramData puis dans le dossier ssh. Nous cherchons le sshd_config qui nous permet de modifier notre connexion ssh. Nous modifions ensuite la ligne port 22, j'ai décidé de changer de port pour augmenter la sécurité, une nouvelle règle de pare-feu devra donc être créée pour autoriser les flux par le port 222 qui sera le port pour la connexion OpenSSH.

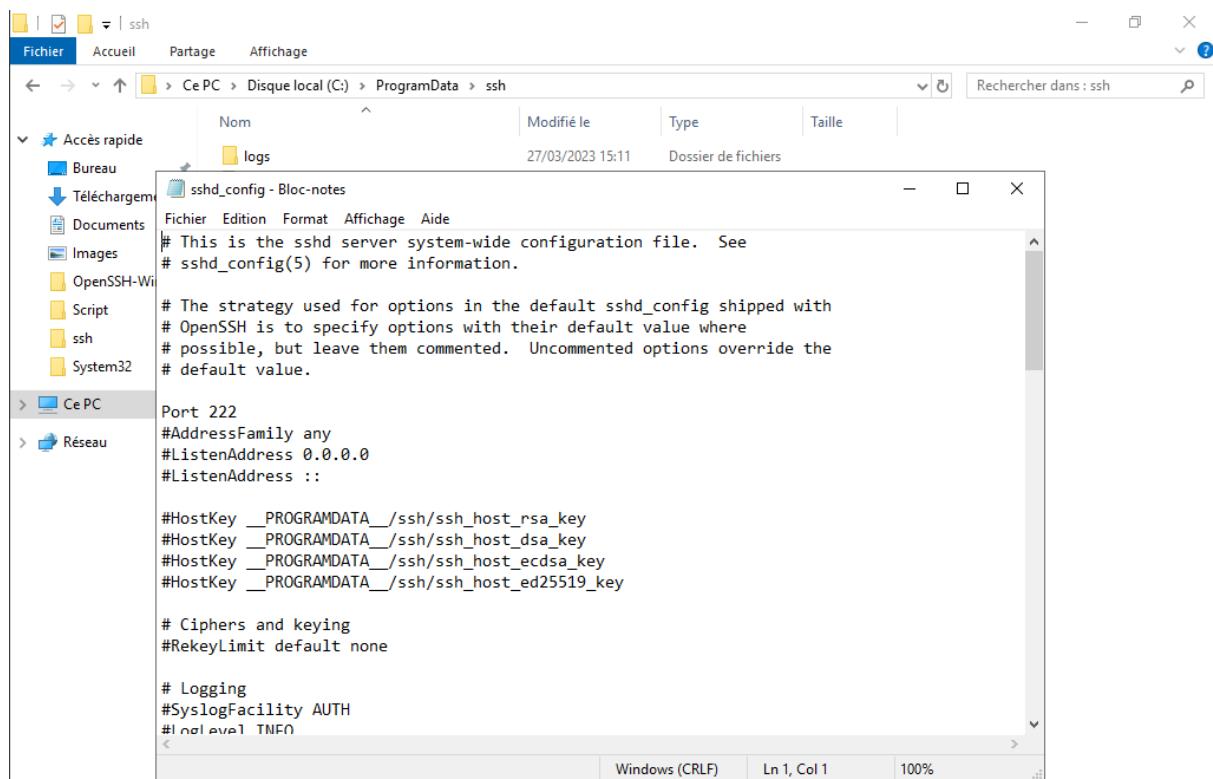
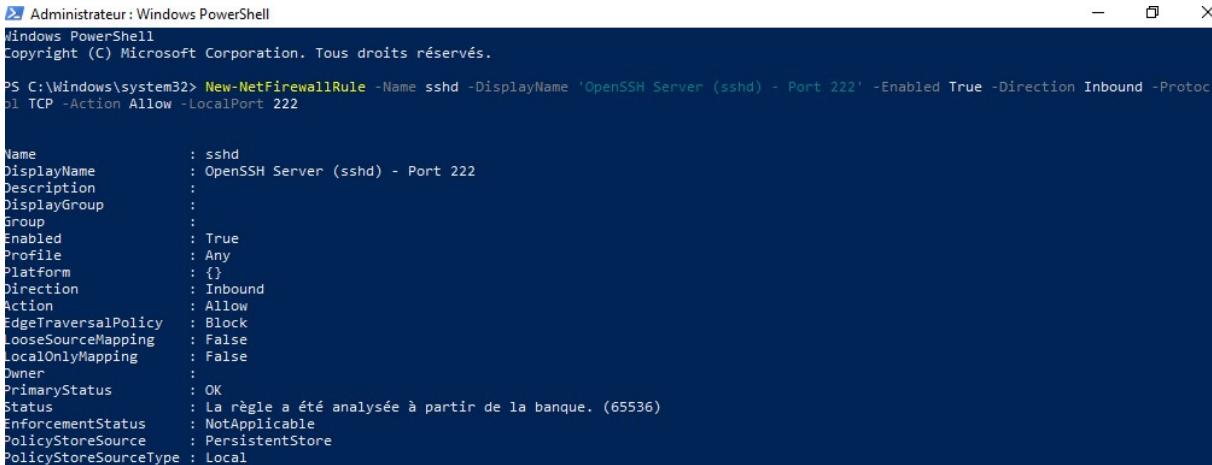


Figure 23 : Configuration SSH n°2

La création de cette règle de pare-feu peut se faire via PowerShell et la commande suivante : cette règle accepte le trafic entrant sur le port 222 avec le protocole TCP.

```
New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd) - Port 222' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 222
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

PS C:\Windows\system32> New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd) - Port 222' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 222

Name          : sshd
DisplayName   : OpenSSH Server (sshd) - Port 222
Description   :
DisplayGroup :
Group         :
Enabled       : True
Profile       : Any
Platform      : {}
Direction    : Inbound
Action        : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner         :
PrimaryStatus : OK
Status        : La règle a été analysée à partir de la banque. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
```

Figure 24 : Commande PowerShell

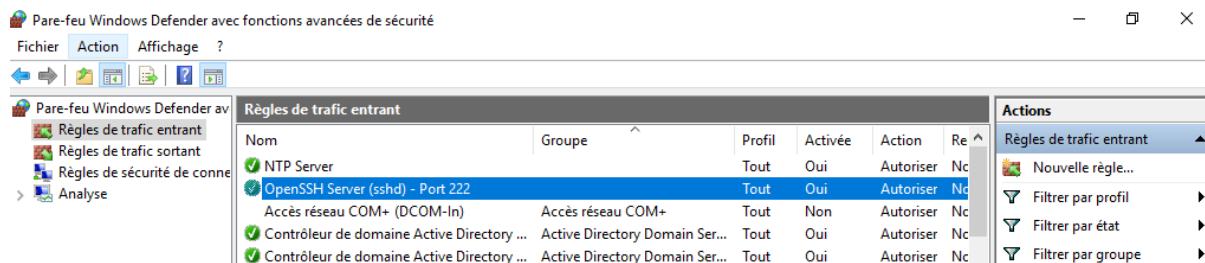


Figure 25 : Règle de pare-feu sur l'interface graphique

Nous pouvons donc ensuite désactiver la règle par défaut sur le port 22 puisque nous ne l'utiliserons pas. Cela apporte donc un gain de sécurité. Nous redémarrons notre service OpenSSH Server via le gestionnaire de service et la connexion peut être tentée. Nous pouvons donc ensuite nous rendre sur un client Windows 10, ouvrir PowerShell et taper la commande suivante :

```
ssh administrateur@10.2.0.1 -p222 #ne pas oublier de préciser le port
```



```
Windows PowerShell
Microsoft Windows [version 10.0.17763.737]
(c) 2018 Microsoft Corporation. Tous droits réservés.

chasseneuil\administrateur@DC-01 C:\Users\Administrateur>exit
Connection to 10.2.0.1 closed.

PS C:\Users\retd> ssh administrateur@10.2.0.1 -p 222
```

Figure 26 : Résultat de la connexion SSH

Nous pouvons donc constater que la connexion SSH est paramétrée sur et sur le matériel et sur le serveur. La tâche est complétée avec succès.

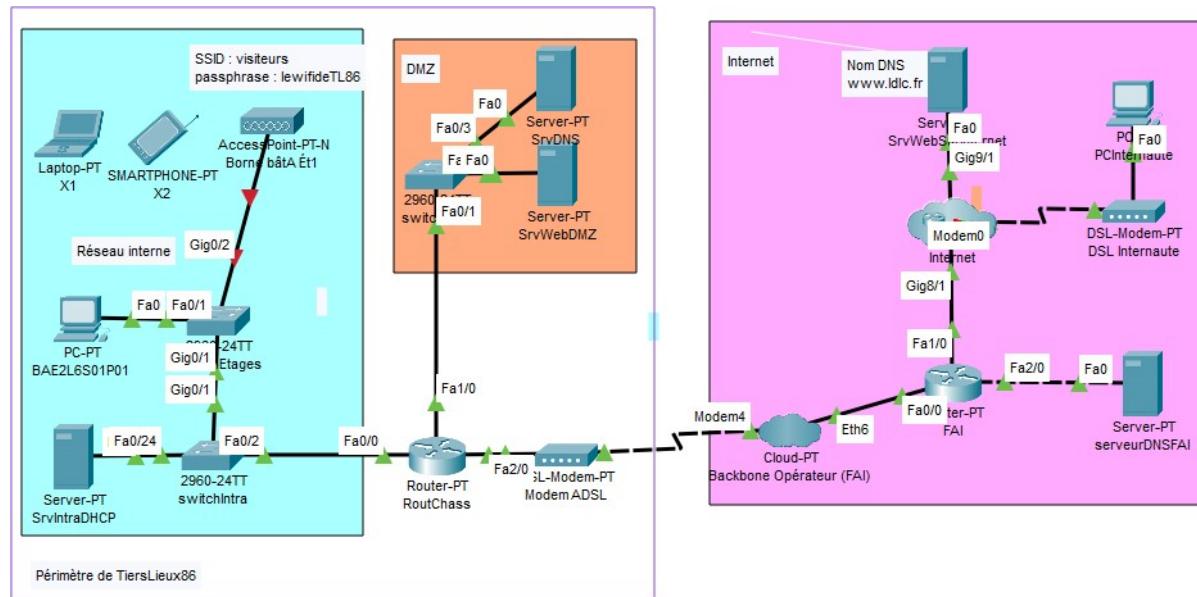
Point sur cette tâche

Pas de réelle complexité pour la partie sur Cisco. Il faut simplement veiller à ne pas oublier de rentrer les commandes “line vty 0 4”, “transport input ssh” ainsi que “login local”. Sans lesquelles il sera impossible de s’identifier. Pour ce qui est de la partie sur l’environnement virtuel, l’indisponibilité du paquet via PowerShell et les problèmes lors de l’installation ont donné un peu de fil à retordre, mais cela m’a permis de découvrir un autre moyen de faire ce qui reste toujours très intéressant.

~~Les équipements devront pouvoir être administrés par SSH2 avec le user « admin » et le mot de passe « SSHP@ssw0rd »~~

Tâche 2

Cette tâche consiste en la mise en place d'internet sur notre maquette. Cela doit se faire via un routeur de FAI, soit un routeur de Fournisseur d'Accès Internet. C'est un matériel fourni par un prestataire pour avoir accès à internet. Une maquette dédiée à cela est fournie, je vais donc faire les configurations sur celle-ci.



Tâche 3

Cette tâche consiste en la synchronisation des clients NTP au serveur NTP. Or des problèmes persistent, il est impossible de connecter le switch cœur au serveur NTP qui pourtant avait pris la configuration. Le NTP n'est pas stable. Les switches l2 quant à eux peuvent se synchroniser sur le switch cœur mais des problèmes sont aussi visibles car un des switches prend la stratum 17 ce qui n'est pas possible en étant synchronisé car à partir de 16 la mention unsynchronized est renvoyée.

Figure 27 : Service NTP

```
Switch Public B
Physical Config CLI Attributes
IOS Command Line Interface

#####
L'Accès à cet équipement est strictement restreint aux seules personnes Autorisées. Cet
équipement est la propriété de TiersLieux86. Déconnectez-vous immédiatement si vous n'êtes
pas une personne autorisée !
-----
Unauthorized access prohibited
Authorized access only
This system is the property of TiersLieux86. Disconnect IMMEDIATELY if you are not an
authorized user!
#####

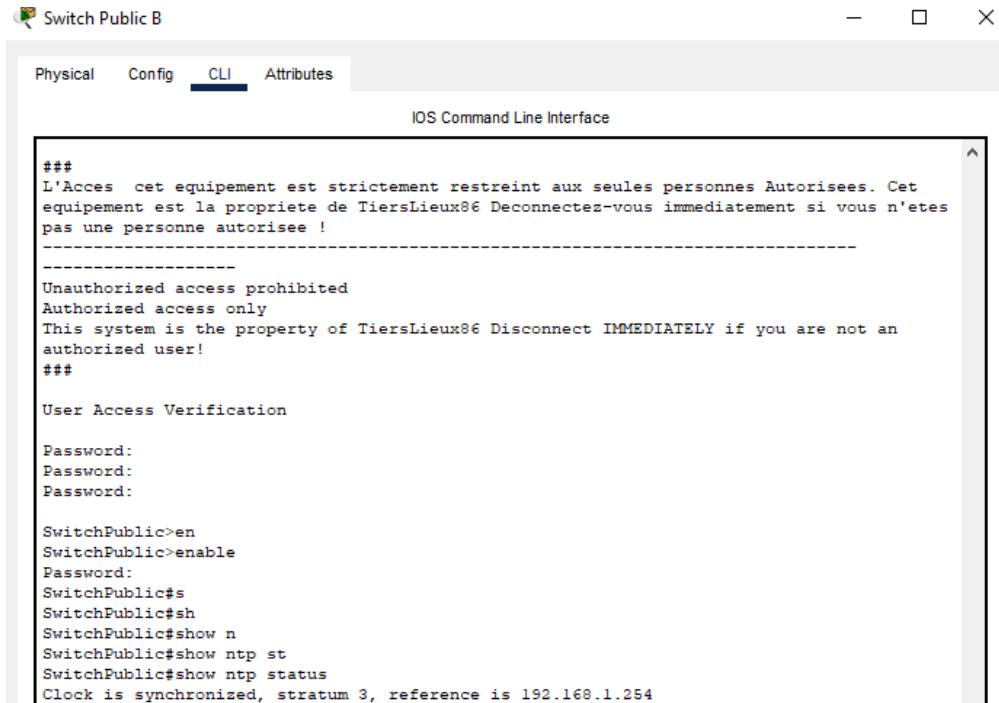
User Access Verification

Password:

SwitchPublic>en
SwitchPublic>enable
Password:
SwitchPublic#show ntp statu
SwitchPublic#show ntp status
Clock is synchronized, stratum 17, reference is 192.168.1.254
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E79D1B6E.00000037 (22:43:05 UTC Mon Mar 20 2023)
clock offset is -10504999.00 msec, root delay is 0.00 msec
root dispersion is 10.18 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 3 sec ago.
SwitchPublic#
```

Copy Paste

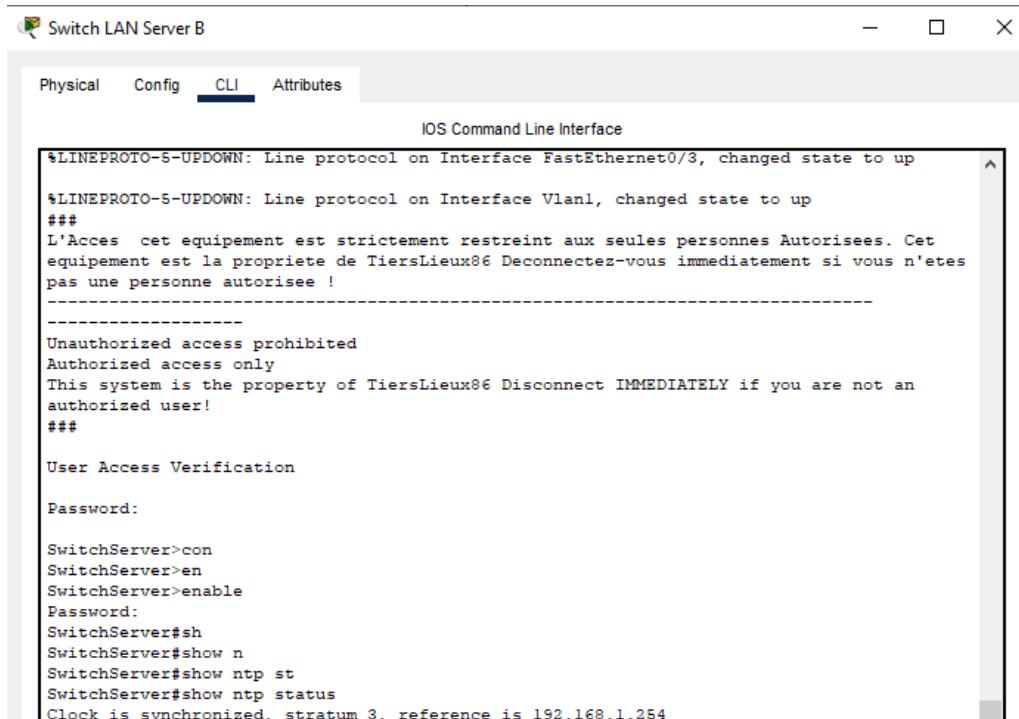
Le problème vient donc de la liaison entre le switch I3 et notre serveur de temps. En soit, bien qu'il ne soit plus synchronisé, nous pouvons configurer le I3 pour qu'il fasse autorité et remplace le serveur de temps ainsi les autres clients se connecteront sur lui et seront synchronisés. Nous pouvons voir que l'IP de référence est désormais 10.2.0.1 comme demandé.



The screenshot shows the Cisco Switch Public B interface. The 'CLI' tab is selected. The terminal window displays the following output:

```
###  
L'Acces cet equipement est strictement restreint aux seules personnes Autorisees. Cet  
equipement est la propriete de TiersLieux86 Deconnectez-vous immediatement si vous n'etes  
pas une personne autorisee !  
-----  
Unauthorized access prohibited  
Authorized access only  
This system is the property of TiersLieux86 Disconnect IMMEDIATELY if you are not an  
authorized user!  
###  
User Access Verification  
Password:  
Password:  
Password:  
  
SwitchPublic>en  
SwitchPublic>enable  
Password:  
SwitchPublic$  
SwitchPublic$sh  
SwitchPublic$show n  
SwitchPublic$show ntp st  
SwitchPublic$show ntp status  
Clock is synchronized, stratum 3, reference is 192.168.1.254
```

Figure 28 : Service NTP 1



The screenshot shows the Cisco Switch LAN Server B interface. The 'CLI' tab is selected. The terminal window displays the following output:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up  
###  
L'Acces cet equipement est strictement restreint aux seules personnes Autorisees. Cet  
equipement est la propriete de TiersLieux86 Deconnectez-vous immediatement si vous n'etes  
pas une personne autorisee !  
-----  
Unauthorized access prohibited  
Authorized access only  
This system is the property of TiersLieux86 Disconnect IMMEDIATELY if you are not an  
authorized user!  
###  
User Access Verification  
Password:  
  
SwitchServer>con  
SwitchServer>en  
SwitchServer>enable  
Password:  
SwitchServer$  
SwitchServer$show n  
SwitchServer$show ntp st  
SwitchServer$show ntp status  
Clock is synchronized, stratum 3, reference is 192.168.1.254
```

Figure 29 : Service NTP 2

The screenshot shows a CLI interface with the following text:

```
Switchcoeur#show clock detail
20:29:6.186 UTC Mon Mar 20 2023
Time source is NTP
Switchcoeur#show ntp status
Clock is synchronized, stratum 2, reference is 10.2.0.1
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E79D050B.000000F5 (20:28:59.245 UTC Mon Mar 20 2023)
clock offset is 0.00 msec, root delay is 1.00 msec
root dispersion is 15.52 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 11 sec ago.
Switchcoeur#configure
Switchcoeur#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Switchcoeur(config)#wr
^
% Invalid input detected at '^' marker.

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

Switchcoeur#show ntp status
Clock is synchronized, stratum 2, reference is 10.2.0.1
```

Figure 30 : Service NTP 3

Nous pouvons constater que la configuration revient comme demander. Ce qui est plutôt étrange.
Nous pouvons constater que les configurations sont bonnes et que le serveur qui fait autorité sur le
l3 est le 10.2.0.1 et que les autres clients connectés reçoivent une configuration correcte.

Nous pouvons de plus vérifier par la commande :

```
enable
show clock detail
```

```
----- -----
reference time is E79D04D4.0000039D (20:28:4.925 UTC Mon Mar 20 2023)
clock offset is 23001.00 msec, root delay is 0.00 msec
root dispersion is 28.88 msec, peer dispersion is 0.24 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 5, last update was 25 sec ago.
SwitchBureaux#show ntp
% Incomplete command.
SwitchBureaux#show clock
20:36:6.467 UTC Mon Mar 20 2023
SwitchBureaux#show clock detail
20:36:11.648 UTC Mon Mar 20 2023
Time source is NTP
SwitchBureaux#
```

Figure 31 : Service NTP 4

Les détails de la création d'un serveur se trouvent plus haut, cliquer sur le titre suivant pour y accéder rapidement “*Protocole NTP Environnement Virtuel*”.

Le serveur NTP Windows est quant à lui stable et fonctionnel, nous pouvons le voir via les screenshot suivants :

```
Administrator : Invite de commandes
Microsoft Windows [version 10.0.17763.737]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>w32tm /status
Indicateur de dérive : 0(Aucun avertissement)
Couche : 1 (Référence principale, synchronisée par l'horloge du réveil)
Précision : -23 (119.209ns par battement)
Délai de racine : 0.0000000s
Dispersion de racine : 10.000000s
ID de référence : 0x4C4F434C (Nom de la source : "LOCL")
Heure de la dernière synchronisation réussie : 19/03/2023 17:45:18
Source : Local CMOS Clock
Intervalle d'interrogation : 6 (64s)

C:\Users\Administrateur>w32tm /resync
Envoi de la commande de resynchronisation à l'ordinateur local
^C
C:\Users\Administrateur>
```

Figure 32 : Serveur NTP

```
Sélection Invite de commandes
Microsoft Windows [version 10.0.19045.2006]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\retd>tm /query /status
'tm' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\retd>win32tm /query /status
'win32tm' n'est pas reconnu en tant que commande interne
ou externe, un programme exécutable ou un fichier de commandes.

C:\Users\retd>w32tm /query /status
Indicateur de dérive : 0(Aucun avertissement)
Couche : 2 (Référence secondaire, synchronisée par (S)NTP)
Précision : -23 (119.209ns par battement)
Délai de racine : 0.0052290s
Dispersion de racine : 21.5166735s
ID de référence : 0x0A020001 (IP de la source : 10.2.0.1)
Heure de la dernière synchronisation réussie : 27/03/2023 09:34:03
Source : DC-01.chasseneuil.fr
Intervalle d'interrogation : 10 (1024s)

C:\Users\retd>
```

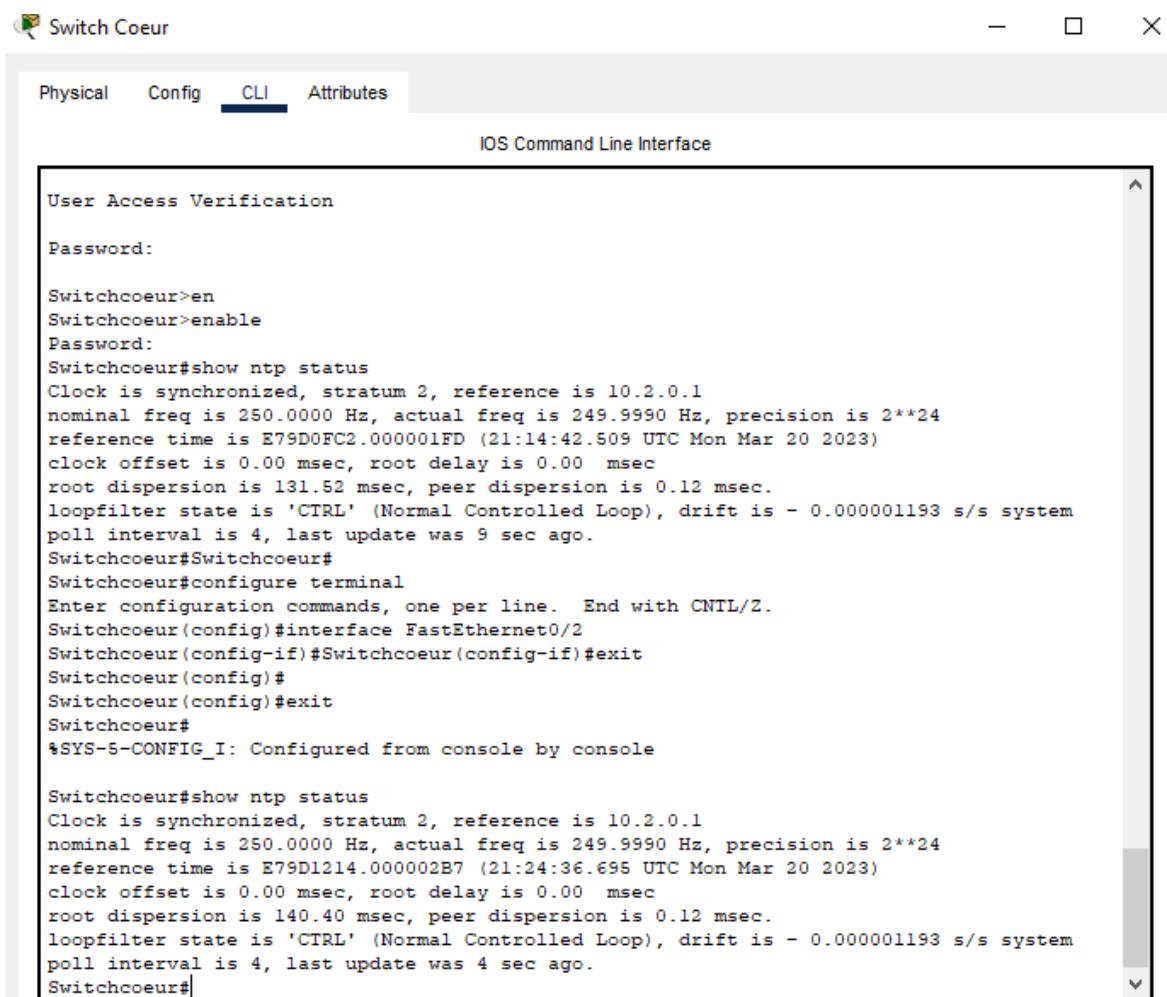
Figure 33 : Client NTP

Le service NTP est donc paramétré sur la maquette ainsi que sur le serveur de l'environnement virtuel.

Tâche 4

Cette dernière tâche sert de conclusion à la mission n°1 qui était portée sur la mise en place d'un service NTP sur la maquette réseau, ainsi que de différentes restrictions et fonctionnalités. Certaines de ses fonctionnalités pouvaient-être paramétrées sur l'environnement virtuel, je pense notamment au NTP ainsi qu'à l'accès SSH. Cette tâche se résumera donc via des captures d'écran témoignant de la bonne configuration faite lors des précédentes tâches ainsi que d'une fiche récapitulative récapitulant les interconnexions, vlan et plages d'adressage IP qui sera une annexe.

Protocole NTP :



```
User Access Verification

Password:

Switchcoeur>en
Switchcoeur>enable
Password:
Switchcoeur#show ntp status
Clock is synchronized, stratum 2, reference is 10.2.0.1
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E79D0FC2.000001FD (21:14:42.509 UTC Mon Mar 20 2023)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 131.52 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 9 sec ago.
Switchcoeur#Switchcoeur#
Switchcoeur#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switchcoeur(config)#interface FastEthernet0/2
Switchcoeur(config-if)#Switchcoeur(config-if)#exit
Switchcoeur(config)#
Switchcoeur(config)#exit
Switchcoeur#
%SYS-5-CONFIG_I: Configured from console by console

Switchcoeur#show ntp status
Clock is synchronized, stratum 2, reference is 10.2.0.1
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E79D1214.000002B7 (21:24:36.695 UTC Mon Mar 20 2023)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 140.40 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 4 sec ago.
Switchcoeur#
```

Figure 34 : Protocole NTP

The screenshot shows the Cisco IOS CLI interface for a device named "Switch LAN Server B". The "CLI" tab is selected. The command-line window displays the following output:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
###  
L'Acces cet equipement est strictement restreint aux seules personnes Autorisees. Cet  
equipement est la propriete de TiersLieux86 Deconnectez-vous immediatement si vous n'etes  
pas une personne autorisee !  
-----  
Unauthorized access prohibited  
Authorized access only  
This system is the property of TiersLieux86 Disconnect IMMEDIATELY if you are not an  
authorized user!  
###  
User Access Verification  
Password:  
SwitchServer>con  
SwitchServer>en  
SwitchServer>enable  
Password:  
SwitchServer#sh  
SwitchServer#show n  
SwitchServer#show ntp st  
SwitchServer#show ntp status  
Clock is synchronized, stratum 3, reference is 192.168.1.254
```

Figure 35 : Protocole NTP 1

Bannière et mots de passe :

The screenshot shows the Cisco IOS CLI interface for a device named "Switch Public B". The "CLI" tab is selected. The command-line window displays the following output:

```
###  
L'Acces cet equipement est strictement restreint aux seules personnes Autorisees. Cet  
equipement est la proprietee de TiersLieux86 Deconnectez-vous immediatement si vous n'etes  
pas une personne autorisee !  
-----  
Unauthorized access prohibited  
Authorized access only  
This system is the property of TiersLieux86 Disconnect IMMEDIATELY if you are not an  
authorized user!  
###  
User Access Verification  
Password:  
Password:  
Password:  
SwitchPublic>en  
SwitchPublic>enable  
Password:
```

Figure 36 : Mot de passe

SSH 2 :

```

PC1

Physical Config Desktop Programming Attributes

Command Prompt

equipement est la propriété de TiersLieux86 Deconnectez-vous immédiatement si vous n'êtes
pas une personne autorisée !
-----
Unauthorized access prohibited
Authorized access only
This system is the property of TiersLieux86 Disconnect IMMEDIATELY if you are not an
authorized user!
###

SwitchPublic>

[Connection to 192.168.1.32 closed by foreign host]
SwitchServer>

[Connection to 192.168.1.2 closed by foreign host]
C:\>ssh -l admin 192.168.1.32

Password:
% Login invalid

Password:

###
L'Accès cet équipement est strictement restreint aux seules personnes Autorisées. Cet
équipement est la propriété de TiersLieux86 Deconnectez-vous immédiatement si vous n'êtes
pas une personne autorisée !
-----
Unauthorized access prohibited
Authorized access only
This system is the property of TiersLieux86 Disconnect IMMEDIATELY if you are not an
authorized user!
###

```

Figure 37 : Connexion SSH

Résultat du ping confortant l'annexe du plan d'adressage :

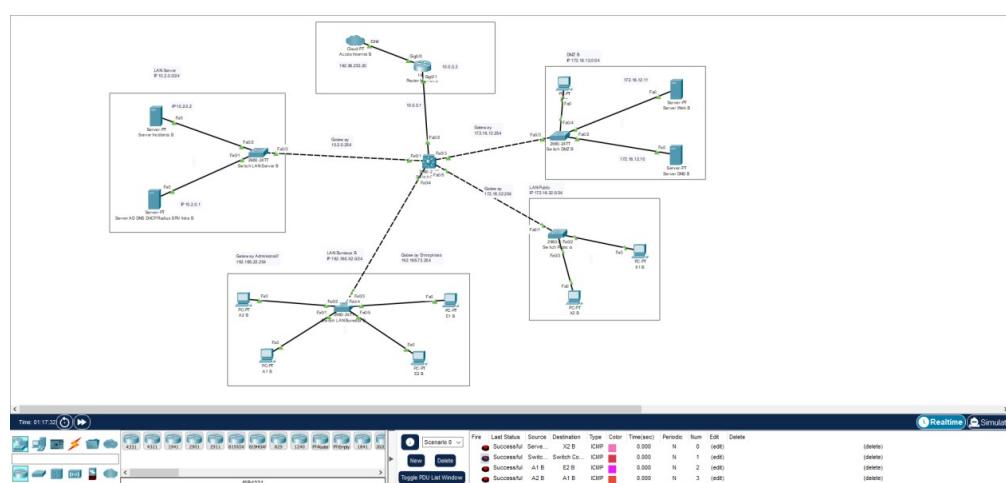


Figure 38 : Maquette

Server AD DNS DHCP Radius SRV Intra B

Physical Config Services Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 172.12.
Ping request could not find host 172.12.. Please check the name and try again.
C:\>ping 172.16.12.11

Pinging 172.16.12.11 with 32 bytes of data:

Reply from 172.16.12.11: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.12.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 39 : Ping 1

A1 B

Physical Config Desktop Programming Attributes

Command Prompt X

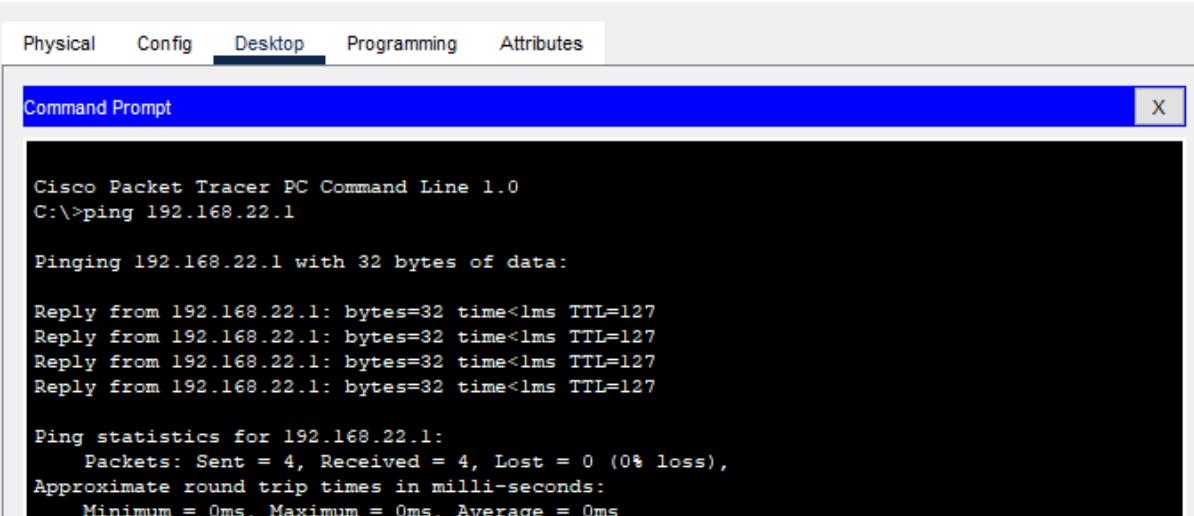
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.72.1

Pinging 192.168.72.1 with 32 bytes of data:

Reply from 192.168.72.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.72.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 40 : Ping 2



The screenshot shows a Cisco Packet Tracer interface titled 'X1 B'. The top menu bar includes 'Physical', 'Config', 'Desktop' (which is selected), 'Programming', and 'Attributes'. Below the menu is a blue header bar with the text 'Command Prompt' and a close button ('X'). The main window displays the output of a 'ping' command:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.22.1

Pinging 192.168.22.1 with 32 bytes of data:

Reply from 192.168.22.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.22.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 41 : Ping 3

Mission 2 : sauvegarde des équipements réseaux

Cette mission se décompose en 5 tâches et à comme sujet le tftp. L'objectif final de celle-ci est de mettre en place une solution de sauvegarde et donc de restauration des configurations et des IOS via TFTP.

Premièrement, qu'est-ce que le TFTP ?

Le TFTP pour Trivial File Transfer Protocol est un protocole de transfert de fichiers. Il est simple et fonctionne sous la forme client/serveur et permet de gérer le transfert de fichiers au sein de réseaux composés d'ordinateurs.

Qu'est qu'une sauvegarde ?

Elle consiste en la duplication de données, donc dans notre cas les données de configuration de nos appareils réseaux, celle-ci permet une fois faite de restaurer les configurations dupliquées si un problème, une réinitialisation ou un changement de matériel devaient arriver.

Qu'est-ce l'IOS ?

L'IOS ou Internetwork Operating System est le système d'exploitation produit par Cisco et qui équipe la grande majorité de ses équipements à l'image des routeurs, commutateurs ou encore des points d'accès wifi. Il permet la configuration par interface graphique ou bien par la CLI (Command Line Interface).

Tâche 1

Le principe de cette tâche est la mise en place d'un serveur TFTP sur l'environnement virtuel. L'installation se fera sur le serveur Windows Server 2019 mais elle aurait pu se faire sur la machine cliente. Nous devons dans un premier temps télécharger l'installateur, puis l'exécuter. Ensuite, nous lançons le programme et nous rendons dans settings, cela ouvre une fenêtre qui nous permet dans l'onglet GLOBAL de configurer les services que nous voulons utiliser.

Sachant que nous voulons créer un serveur TFTP nous ne laissons cocher que TFTP Server. Nous pouvons nous rendre dans l'onglet TFTP et changer les configurations que nous voulons. Nous pouvons ensuite préciser un dossier où stocker les données via browse, j'ai créé au préalable un dossier TFTP Files qui me servira de répertoire pour stocker les données de configuration. Nous donnons ensuite une adresse IP à notre serveur TFTP dans celle que le logiciel nous propose dans le menu déroulant à côté de "Bind TFTP to this address", pour moi ce sera la 127.0.0.1. Nous devons ensuite redémarrer le logiciel. Nous pouvons constater que la configuration a été sauvegardée, ce qui veut dire que le serveur est bien paramétré.

Les screenshot suivants donnent la configuration de mon serveur TFTP :

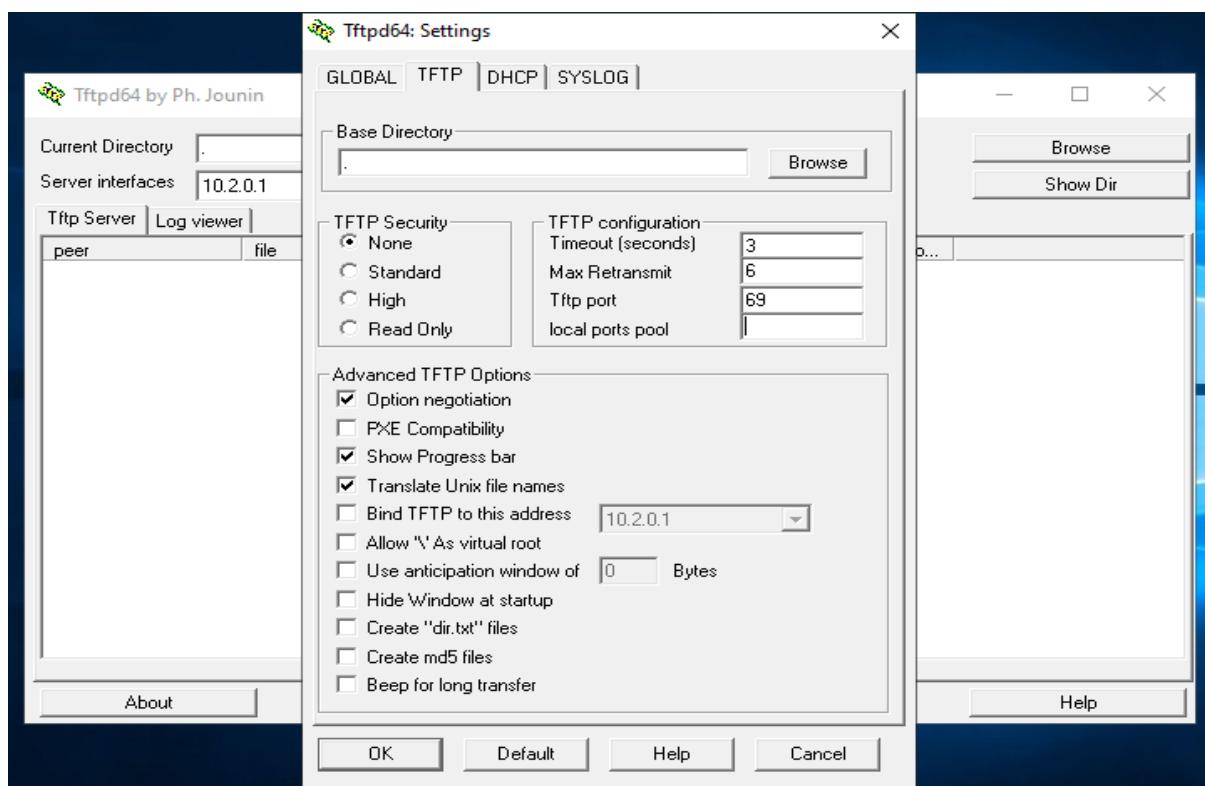


Figure 42 : Server TFTP Configuration TFTP

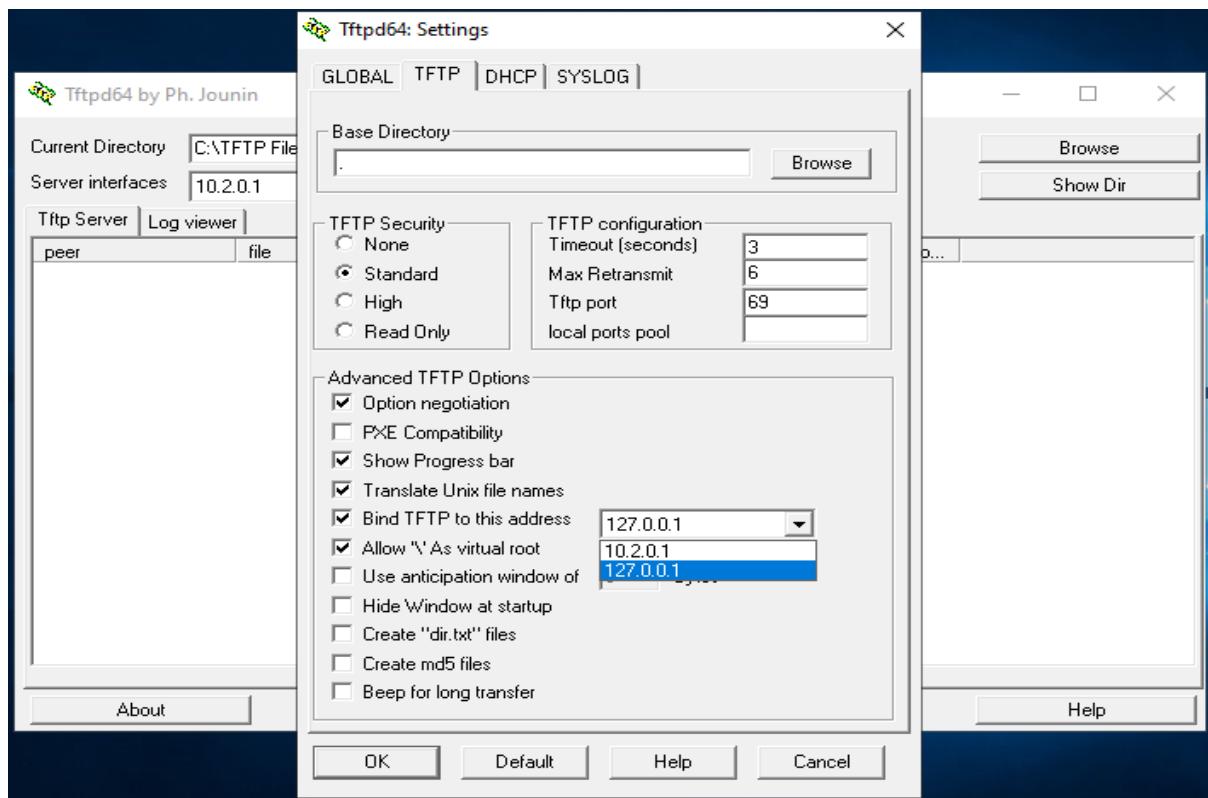


Figure 43 : Server TFTP Configuration IP

Tâche 2

L'objectif de cette tâche est d'écrire une procédure expliquant comment sauvegarder et restaurer la configuration d'équipements Cisco via le serveur TFTP ainsi que l'IOS de l'équipement.

Sauvegarder/restaurer la configuration

Premièrement, nous devons veiller à ce que notre serveur TFTP soit en fonctionnement. Par la suite nous nous dirigeons sur l'appareil dont nous voulons sauvegarder la configuration. En effet, sans sauvegarde au préalable, il sera impossible de restaurer une configuration.

Nous savons que le matériel Cisco possède deux mémoire pour les configurations, l'une stocke la configuration en cours, celle qui est modifiée en live et qui n'est pas forcément enregistrer. C'est la mémoire RAM pour Random Access Memory, c'est une mémoire dite volatile qui efface les données stockées lors de l'extinction de l'appareil, de la fermeture d'une application, du nettoyage du cache et bien d'autres. Le problème avec ce type de mémoire c'est que lorsque l'appareil est éteint volontairement ou non les données sont perdues et la configuration aussi. Vient alors la notion de NVRAM pour Non Volatile Random Access Memory, qui elle lors de l'extinction de la machine ne supprime pas les données. C'est sur celle-ci que les configurations sont donc sauvegardées. Nous distinguons donc le fichier running-config associé à la RAM et le fichier startup-config qui lui est associé à la NVRAM.

Tout d'abord nous créons notre configuration, nous souhaitons ensuite la sauvegarder en tant que startup-configuration, nous devons donc faire la commande suivante :

```
copy running-config startup-config  
Destination filename [startup-config]? #Nous appuyons sur Entrée
```

Nous avons donc notre configuration initiale. Nous devons ensuite l'exporter via le protocole TFTP sur notre serveur TFTP qui utilise l'udp sur le port 69. Nous devons donc faire les commandes suivantes :

```
copy startup-config tftp  
Address or name of remote host [ ]? 127.0.0.1 #Nous renseignons  
l'IP de notre serveur  
Destination filename [ConfigurationMatériel]? #Nous appuyons sur Entrée  
!!  
[OK - X bytes]  
  
X bytes copied in 0.X secs (XXXX bytes/sec)
```

Nous avons copié notre configuration de démarrage sur le serveur TFTP avec l'adresse IP 127.0.0.1. Désormais nous devons récupérer cette sauvegarde et procéder à la restauration de celle-ci. Cela peut être dû à différentes raisons telles que la mise hors tensions non désirés lors de la configuration du matériel ce qui à amener à la suppression de la configuration en cours, un reset de la configuration non voulut où voulut etc...

Nous devons donc premièrement être sûr de posséder la configuration du matériel que nous souhaitons restaurer avant tout. Si c'est le cas, nous pouvons alors effacer la configuration en cours de manière à faire les choses proprement et éviter tous problèmes lors de la restauration. Nous devons pour cela utiliser les commandes suivantes :

```
erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue ? [Confirm] #Enter
[OK]
Erase of the nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

Nous rechargeons ensuite la configuration d'usine de notre appareil via les commandes :

```
reload
Proceed with reload? [Confirm] #Enter
<output omitted>
      - system Configuration Dialog -
Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!
```

Puisqu'aucune interface n'est paramétrée, nous devons au moins créer celle qui devra communiquer avec le serveur TFTP.

Nous pouvons ensuite passer à la restauration de notre sauvegarde, pour cela nous faisons les commandes suivantes :

```
copy tftp running-config
Address or name of remote host [ ]? 127.0.0.1
Source filename [ConfigurationMatériel ]?
Accessing tftp://127.0.0.1/ConfigurationMatériel...
Loading ConfigurationMatériel from 127.0.0.1: !
[OK - x bytes]

x bytes copied in 0.x secs (x bytes/sec)
```

Et nous sauvegardons la configuration dans la startup-config donc la NVRAM via les commandes :

```
copy running-config startup-config
Destination filename [startup-config]? #Enter
```

Sauvegarder/restaurer l'IOS

L'IOS est le système d'exploitation de notre appareil. Nous devons premièrement prendre connaissance de quel IOS est présent et du nom de fichier que celui-ci utilise sur la machine via la commande :

```
show boot
```

Et nous recherchons sur la ligne BOOT path-list le nom du fichier celui-ci peut ressembler à "c2960-lanlitek9-mz.122-58.SE2.bin"

Nous souhaitons ensuite copier notre fichier sur le serveur TFTP, pour cela nous devons utiliser les commandes suivantes :

```
copy flash tftp 127.0.0.1 <nom du fichier>
```

Nous souhaitons ensuite restaurer notre IOS nous devons donc copier l'IOS depuis notre serveur TFTP, nous devons faire la commande suivante :

```
copy tftp flash:
Address or name of remote host [ ] ? 127.0.0.1
Source filename [ ]? <Nom du fichier trouvé sur BOOT Path-list>
Destination filename [Nom du fichier trouvé sur BOOT Path-list]? 
```

Nous avons ensuite 2 images disques sur notre matériel, il faut donc choisir lequel va être celui que nous voulons utiliser. Nous pouvons faire la commande suivante pour lister ces images :

```
dir flash
```

Cette commande montre différents fichiers appartenant à un numéro, le plus proche de 0 est prioritaire sur les autres. Nous devons donc modifier la séquence de boot pour paramétrer le démarrage sur le bon IOS. Pour cela nous pouvons utiliser la commande suivante :

```
boot system flash: <nom du fichier>
```

Ainsi, le bon IOS est sauvegardé/restaurer et paramétrer.

Tache 3

Le but de cette tâche est de réaliser une procédure concernant la réinitialisation des mots de passe des switches et routeurs Cisco. Pourquoi faire ? Le matériel réseau n'est pas voué à être manipulé régulièrement et nous pouvons oublier les mots de passe. Le matériel peut aussi avoir été utilisé par une autre personne auparavant et avoir été configuré avec des mots de passe. Il peut donc être nécessaire de savoir comment réinitialiser ceux-ci.

Switch

Pour les switches nous devons suivre les étapes suivantes :

“Redémarrer le switch et appuyer sur le bouton mode

*On débranche le switch, on appuie sur le bouton **mode** sur la face avant du switch en bas à gauche, et on rebranche le switch.*

*En théorie d'après la doc la led du haut, qui correspond à **SYST** va clignoter orange puis passer au vert fixe, mais en pratique sur mon switch, ça a clignoté vert puis c'est passé à l'orange fixe, et c'est là que j'ai lâché le bouton **mode**. Maintenant la led clignote vert.”*

Un prompt est retourner :

```
Base ethernet MAC Address: 00:19:2f:ac:4f:60
Xmodem file system is available.
The password-recovery mechanism is enabled.
```

```
The system has been interrupted prior to initializing the
flash filesystem. The following commands will initialize
the flash filesystem, and finish loading the operating
system software:
```

```
flash_init
load_helper
boot
```

```
switch:
```

Nous utilisons la commande `flash_init` qui permet d'initialiser le flash. Nous devons ensuite utiliser la commande `load_helper` qui permet d'avoir accès à un assistant de démarrage. Nous devons ensuite afficher le contenu de la mémoire flash via la commande `dir flash`, un fichier `config.text` doit-être présent. Nous devons renommer ce fichier en `config.bak` via la commande `rename flash:config.text flash:config.bak` puis nous faisons un boot pour redémarrer le switch.

```
switch: flash_init
Initializing Flash...
flashfs[0]: 363 files, 5 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 5987840
flashfs[0]: Bytes available: 26526208
flashfs[0]: flashfs fsck took 10 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs) installed, fsid: 3
Setting console baud rate to 9600...

switch:
```

```
switch: load_helper
switch:
```

```
2 -rwx    5          private-config.text
4 -rwx    1230       config.text
5 drwx   192         c2960-lanbase-mz.122-25.FX
```

```
switch: dir flash:
Directory of flash:/

26526208 bytes available (5987840 bytes used)
```

```
switch:
switch: rename flash:config.text flash:config.bak
switch: boot
```

Nous faisons ensuite un yespuis nopard l'auto install et pour le dialogue de configuration initial.

```
Would you like to terminate autoinstall? [yes]: yes
--- System Configuration Dialog ---
```

```
Would you like to enter the initial configuration dialog?
[yes/no]: no
```

Nous repassons en mode enable et nous remettons le fichier config.bakà sa place avec son nom d'origine

```
enable
rename flash:config.bak flash:config.text
```

Nous replaçons le fichier config.textdans la running-config via la commande :

```
copy flash:config.text system:running-config
Destination filename [runnin-config]? #Enter
```

Nous pouvons ensuite entrer les commandes suivantes pour enlever les mots de passe :

```
no enable password
no enable secret
```

Et nous pouvons ainsi faire une sauvegarde via :

```
copy running-config startup-config
```

Routeur

Nous devons d'abord éteindre puis rallumer le routeur, pendant le démarrage nous devons appuyer sur Ctrl+Pause(Attn). Nous entrons ensuite la commande confreg 0x2142 puis la commande reset, au démarrage nous entrons deux fois no, nous passons ensuite en mode enable et faisons les commandes no enable secret et no enable password nous faisons ensuite les commandes confreg 0x2102 et copy run start.

Tâche 4

Cette tâche a pour but de rédiger une procédure expliquant comment mettre à jour les IOS de nos appareils. Ayant un serveur TFTP à disposition, nous allons placer les images dessus et les uploader directement sur le matériel via les commandes qui ont été vues précédemment. Pour récupérer l'image de notre produit nous pouvons nous rendre sur le site de [Cisco Product Support and Downloads](#), nous entrons le nom de notre produit et les différents IOS nous serons proposés.

The screenshot shows the Cisco Product Support and Downloads website. At the top, there is a search bar with the placeholder "Product Name e.g. 2911" and a "LOG IN NOW" button. Below the search bar, a sidebar titled "Most Popular" lists several Catalyst 2960-S Series Switches models. The main content area has a heading "Select a Product". On the left, a sidebar menu includes categories like "IOS and NX-OS Software", "Optical Networking", "Routers", "Security", "Servers - Unified Computing", "Storage Networking", and "Switches". The "Switches" category is currently selected. In the main content area, a list of Catalyst 2960-S Series Switches is shown, with "Catalyst 2960-S Series Switches" highlighted. To the right, a list of specific switch models is displayed, including Catalyst 2960S-24PD-L Switch, Catalyst 2960S-24PS-L Switch, Catalyst 2960S-24TD-L Switch, Catalyst 2960S-24TS-L Switch, Catalyst 2960S-24TS-S Switch, Catalyst 2960S-48FPS-L Switch, and Catalyst 2960S-48LPS-L Switch.

Figure 44 Cisco Product Support and Downloads n°1

File Information	Release Date	DRAM/FLASH	
UNIVERSAL	11-Sep-2018	64/32	
c2960s-universalk9-mz.152-2.E9.bin Advisories			
UNIVERSAL WITH WEB BASED DEV MGR	11-Sep-2018	64/32	
c2960s-universalk9-tar.152-2.E9.tar			

Figure 45 : Cisco Product Support and Downloads n°2

Nous copions ensuite le fichier sur notre serveur TFTP et utilisons la commande suivante dans le but de récupérer sur le matériel notre IOS :

```
copy tftp flash:  
Address or name of remote host [ ] ? 127.0.0.1  
Source filename [ ]? <Nom du fichier trouvé sur BOOT Path-list>  
Destination filename [Nom du fichier trouvé sur BOOT Path-list]?
```

Nous ne devons pas oublier que le fichier ne sera peut-être pas celui choisi pour boot, nous devons alors faire les commandes suivantes pour changer l'ordre de démarrage :

```
dir flash
```

```
boot system flash: <nom du fichier>  
write #sauvegarde dans la startup-config
```

Ainsi l'IOS de notre matériel est installé et l'ordre de démarrage est le bon permettant de garder le matériel à jour d'une manière simple mais efficace.

Tâche 5

Cette dernière tâche a pour objectif la mise en place d'un serveur TFTP sur Cisco Packet Tracer et une démonstration des fonctionnalités vue précédemment. Premièrement, voici à quoi ressemble la maquette, configurer conformément à un réseaux type « ETP de Poitiers ». Le serveur TFTP sera ici le serveur dédié aux incidents avec l'adresse IP en 10.2.0.2.

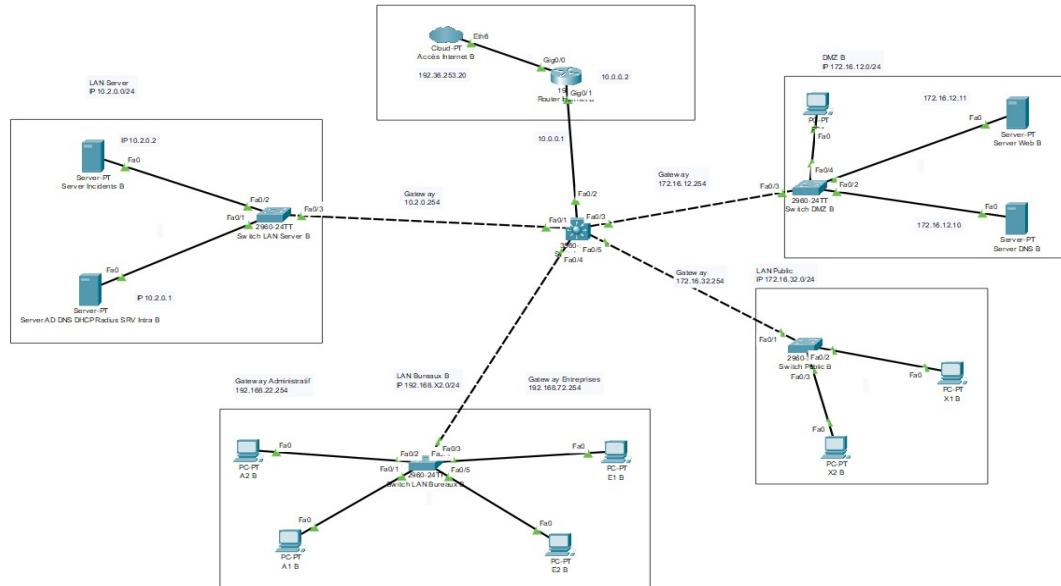


Figure 46 : Maquette du réseau

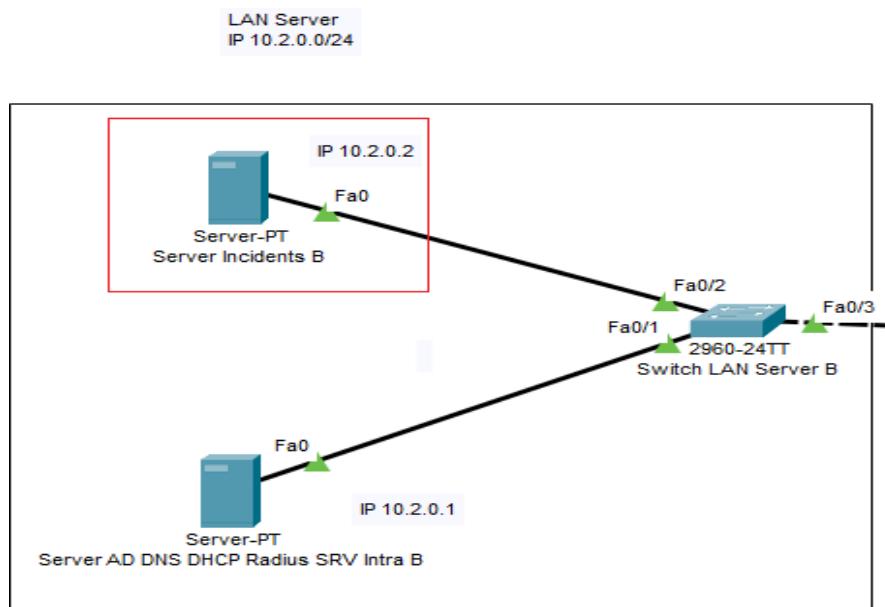


Figure 47 : Server d'incidents

Sauvegarder/restaurer la configuration

La sauvegarde de configuration

Le serveur fait partie du vlan Serveur associé au numéro 52 avec une plage d'IP en 10.2.0.X/24. Nous devons donc assigner à l'interface vlan 52 de notre matériel une IP sur cette plage pour que la sauvegarde puisse se faire. Pour cela nous devons faire les commandes suivantes :

```
enable
configure terminal
interface vlan 52
ip address 10.2.0.100
```

Write

Nous pouvons ensuite faire la commande suivante pour sauvegarder la configuration :

Et nous pouvons passer au test des commandes pour sauvegarder notre configuration sur le serveur TFTP :

```
copy startup-config tftp
10.2.0.2
```

Ce qui donne le résultat suivant :

```
Switch LAN Server B
Physical Config CLI Attributes
IOS Command Line Interface
*Error opening tftp://10.2.0.2/SwitchServer-config (Timed out)
SwitchServer#conf
SwitchServer#configure ter
SwitchServer#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchServer(config)#interf
SwitchServer(config)#interface vlan 52
SwitchServer(config-if)#ip add
SwitchServer(config-if)#ip address 10.2.0.100
% Incomplete command.
SwitchServer(config-if)#ip address 10.2.0.100 255.255.255.0
SwitchServer(config-if)#no shut
SwitchServer(config-if)#exit
SwitchServer(config)#
SwitchServer(config)#exit
SwitchServer#
*SYS-5-CONFIG_I: Configured from console by console

SwitchServer#wr
Building configuration...
[OK]
SwitchServer#copy startup-config tftp
Address or name of remote host []?
?Host name or address not specified

SwitchServer#
SwitchServer#copy startup-config tftp
Address or name of remote host []? 10.2.0.2
Destination filename [SwitchServer-config]?

Writing startup-config....!!
[OK - 1943 bytes]

1943 bytes copied in 3.012 secs (645 bytes/sec)
SwitchServer#
```

Figure 48 : Résultat n°1

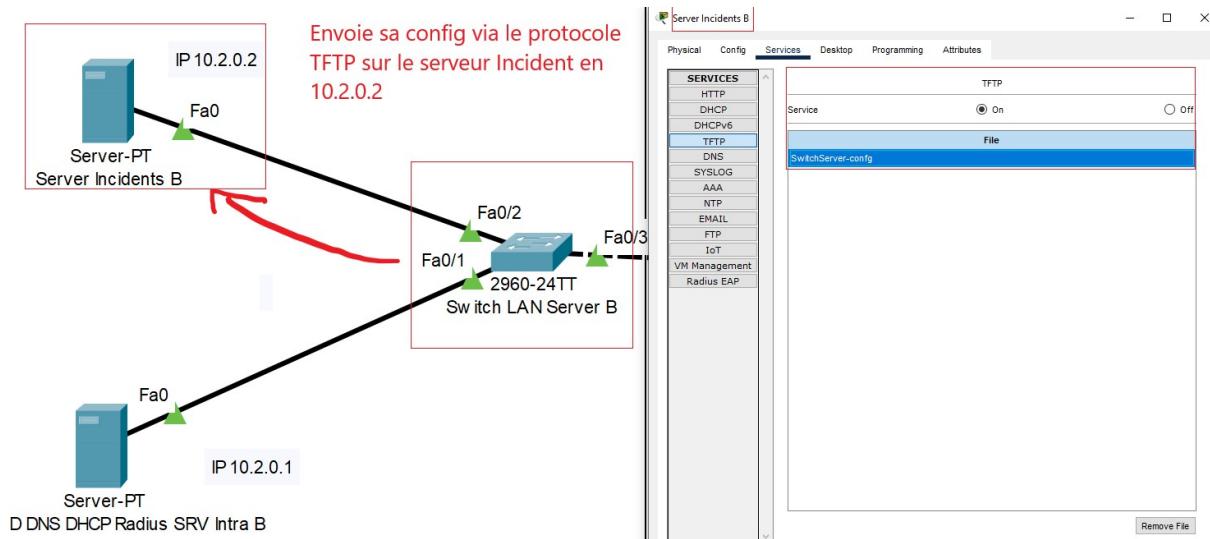


Figure 49 : Résultat n°2

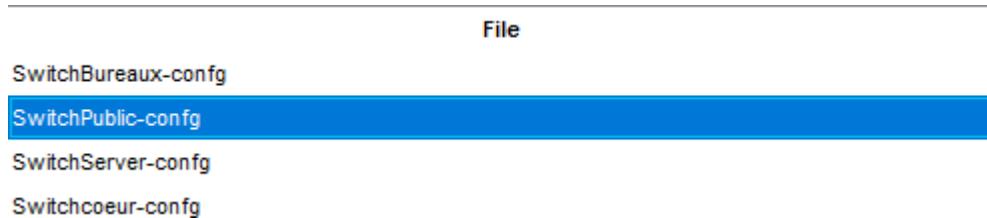
La restauration de configuration

La sauvegarde fonctionne, nous passons donc désormais à la restauration de celle-ci, pour cela nous allons mettre la configuration d'usine sur le switch Public. Pour cela nous devons faire les commandes suivantes :

```
enable
erase startup-config
yes
```

Figure 50 : Fichier de configuration sauvegarder sur le TFTP

Nous pouvons ensuite copier depuis le serveur TFTP la configuration du switch public que nous avons au préalable sauvegarder :



via les commandes :

```
copy running-config tftp #commande de copie sur la mémoire RAM  
10.2.0.2 #IP du serveur TFTP  
SwitchPublic-config #Nom du fichier de configuration
```

Nous pouvons constater que la copie se fait bien depuis le serveur TFTP et qu'il n'y a pas d'échec.

The screenshot shows the CLI interface of a Cisco switch named "Switch Public B". The terminal window displays the following session:

```
Writing startup-config....!  
[OK - 1950 bytes]  
  
1950 bytes copied in 3.021 secs (645 bytes/sec)  
SwitchPublic#era  
SwitchPublic#erase st  
SwitchPublic#erase startup-config  
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]  
[OK]  
Erase of nvram: complete  
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram  
SwitchPublic#  
SwitchPublic#  
SwitchPublic#copy tf  
SwitchPublic#copy tftp runn  
SwitchPublic#copy tftp running-config  
Address or name of remote host []? 10.2.0.2  
Source filename []? SwitchPublic-config  
Destination filename [running-config]?  
  
Accessing tftp://10.2.0.2/SwitchPublic-config...  
Loading SwitchPublic-config from 10.2.0.2: !  
[OK - 1950 bytes]  
  
1950 bytes copied in 0 secs  
SwitchPublic#  
%SYS-5-CONFIG_I: Configured from console by console  
  
SwitchPublic#show run  
SwitchPublic#show running-config  
Building configuration...  
  
Current configuration : 1950 bytes  
!  
version 15.0
```

At the bottom right of the terminal window, there are "Copy" and "Paste" buttons.

Figure 51 : Résultat du test de copie depuis le serveur TFTP vers switch public

Il ne faut pas oublier de sauvegarder cette configuration dans la mémoire NVRAM donc dans la startup-config de l'appareil via la commande :

```
copy running-config startup-config
```

Sauvegarder/restaurer l'IOS

Nous devons désormais tester la sauvegarde de notre IOS et sa restauration.

La sauvegarde de l'IOS

Nous devons tout d'abord prendre connaissance du fichier que le matériel utilise en tant que système d'exploitation. Pour cela nous pouvons faire la commande suivante :

```
show flash
```

Un prompt ressemblant au suivant nous sera retourné, nous regarderons alors le fichier encadré en rouge ci-dessous :

```
SwitchPublic#show flash
Directory of flash:/
  1  -rw-      4670455      <no date>| 2960-lanbasek9-mz.150-2.SE4.bin
  5  -rw-          1950      <no date>  config.text
  2  -rw-          916      <no date>  vlan.dat

64016384 bytes total (59343063 bytes free)
SwitchPublic#
```

Figure 52 : Fichier IOS

Une fois que nous avons localiser ce fichier nous pouvons passer à la sauvegarde, via les commandes suivantes :

```
copy flash tftp  
2960-lanbasek9-mz.150-2.SE4.bin  
10.2.0.2  
Enter
```

```
1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin  
5 -rw- 1950 <no date> config.text  
2 -rw- 916 <no date> vlan.dat  
  
64016384 bytes total (59343063 bytes free)  
SwitchPublic#copy flash tftp 2960-lanbasek9-mz.150-2.SE4.bin  
^  
* Invalid input detected at '^' marker.  
  
SwitchPublic#copy flash tftp  
Source filename []? 2960-lanbasek9-mz.150-2.SE4.bin  
Address or name of remote host []? 10.2.0.2  
Destination filename [2960-lanbasek9-mz.150-2.SE4.bin]?  
  
Writing 2960-lanbasek9-mz.  
150-2.SE4.bin...!!!!!!  
[OK - 4670455 bytes]  
  
4670455 bytes copied in 0.143 secs (2625788 bytes/sec)  
SwitchPublic#
```

Figure 53 : Résultat de la sauvegarde

La restauration de l'IOS

Nous devons désormais faire le test d'une restauration de l'IOS, ce test sera une fois de plus sur le switch public. Pour pouvoir copier le fichier du serveur TFTP au flash de notre switch nous devons faire les commandes suivantes :

```
copy tftp flash
10.2.0.2
2960-lanbasek9-mz.150-2.SE4.bin #Nom du fichier à copier
Enter #Demande si nous voulons réécrire sur le fichier car il est déjà existant
Enter
```

The screenshot shows the CLI interface for a Cisco switch named "Switch Public B". The "CLI" tab is selected. The terminal window displays the following command sequence:

```
copy tftp flash
10.2.0.2
2960-lanbasek9-mz.150-2.SE4.bin #Nom du fichier à copier
Enter #Demande si nous voulons réécrire sur le fichier car il est déjà existant
Enter
```

Below this, the terminal shows the system's response to the copy command, including a warning about overwriting an existing file and the progress of the file transfer.

Figure 54 : Résultat du test de restauration

Bilan

Nous pouvons donc conclure que le serveur TFTP est bien paramétré ainsi que ses clients. Tant au niveau de notre environnement virtuel que de la maquette Cisco. Le protocole est en soi facile à prendre en main puisqu'il réside sur le principe client/serveur, un simple paramétrage des IP et des interfaces vlan est à faire pour assurer la bonne communication du matériel avec le serveur. Quant aux sauvegardes et aux restaurations, le principe reste simple à comprendre.

Mission 3 : segmentation du réseau

Cette mission a pour but la mise en place de VLAN de niveau 1 et du protocole VTP.

Premièrement, qu'est-ce qu'un VLAN ?

Un VLAN pour Virtual Local Area Network est un réseau local virtuel. Ceux-ci sont créés sur un équipement réseau tel qu'un switch pour cloisonner les flux. Ainsi, un VLAN ne peut par défaut pas communiquer avec un autre VLAN. C'est donc une manipulation faite dans une optique de sécurité du réseau. En effet un VLAN peut permettre de ne pas faire circuler un malware sur le réseau.

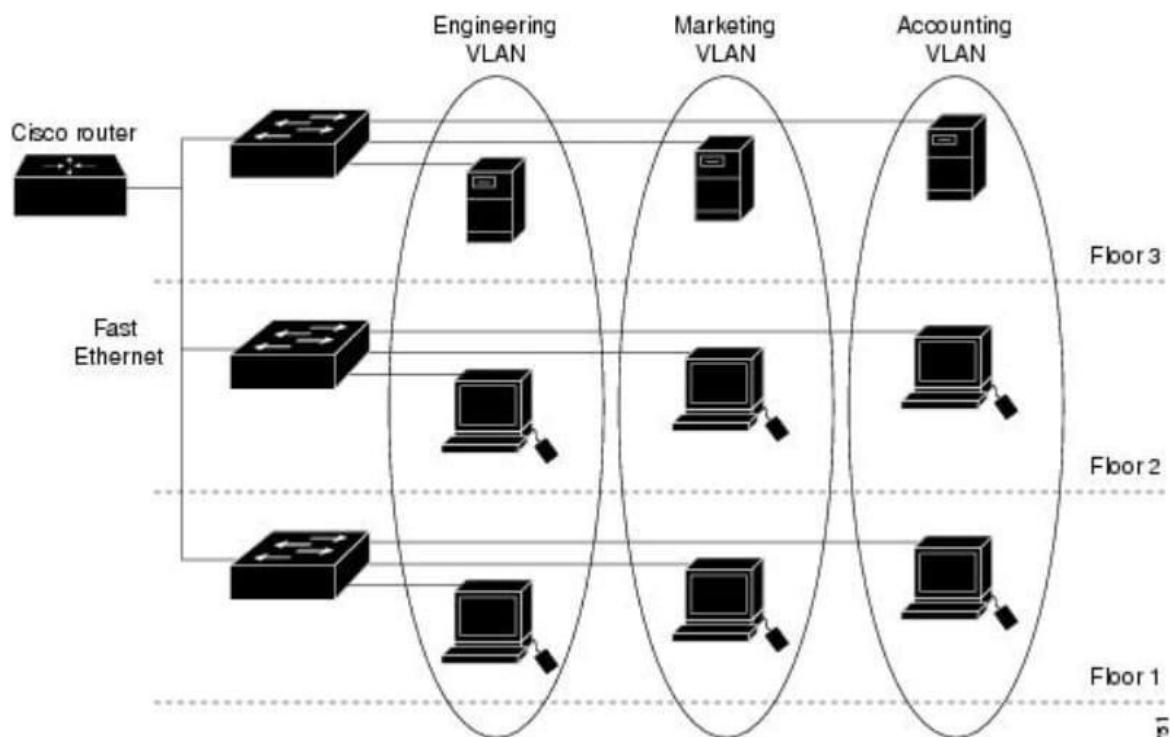


Figure 55 : Schéma du fonctionnement de VLAN

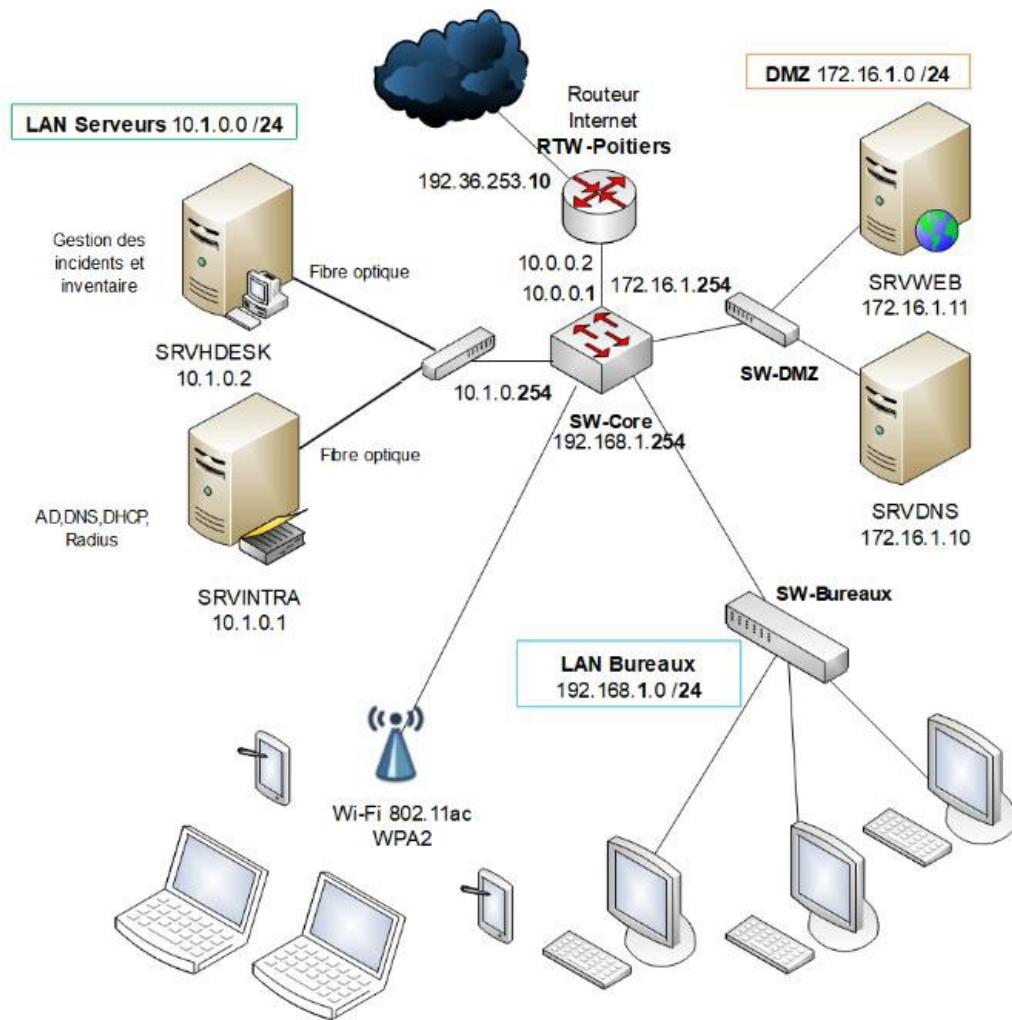
Qu'est-ce que le VTP ? Le VTP pour VLAN Trunking Protocol est un protocole présent sur les équipements Cisco. Il permet de créer un switch référent qui distribue à tous les autres switches sa base de données comprenant les VLAN. Il permet donc de limiter les configurations à faire sur le matériel puisque seulement un switch peut être paramétré. Cette mission est donc orientée sur les VLANs, ceux-ci délimiteront les services et entreprises du site de Chasseneuil.

Tâche 1

Cette tâche a pour objectif la mise en place de VLAN pour des entreprises juniors et pour les salles de réunion. Nous devrons donc mettre en place un vlan par entreprise et un vlan par salle de réunion.

Nom du VLAN	Numéro du VLAN	Pool d'IP DHCP	Gateway
Esporting	2	127.17.2.X /24	127.17.2.254 /24
ValorElec	3	127.17.3.X /24	127.17.3.254 /24
Réunion A	4	127.17.4.X /24	127.17.4.254 /24
Réunion B	5	127.17.5.X /24	127.17.5.254 /24

Figure 56 : Tableau des VLANs



Pour cela nous devons suivre le plan suivant tout en respectant le schéma de l'ETP.

Figure 57 : Schéma de l'ETP de Poitiers Centre

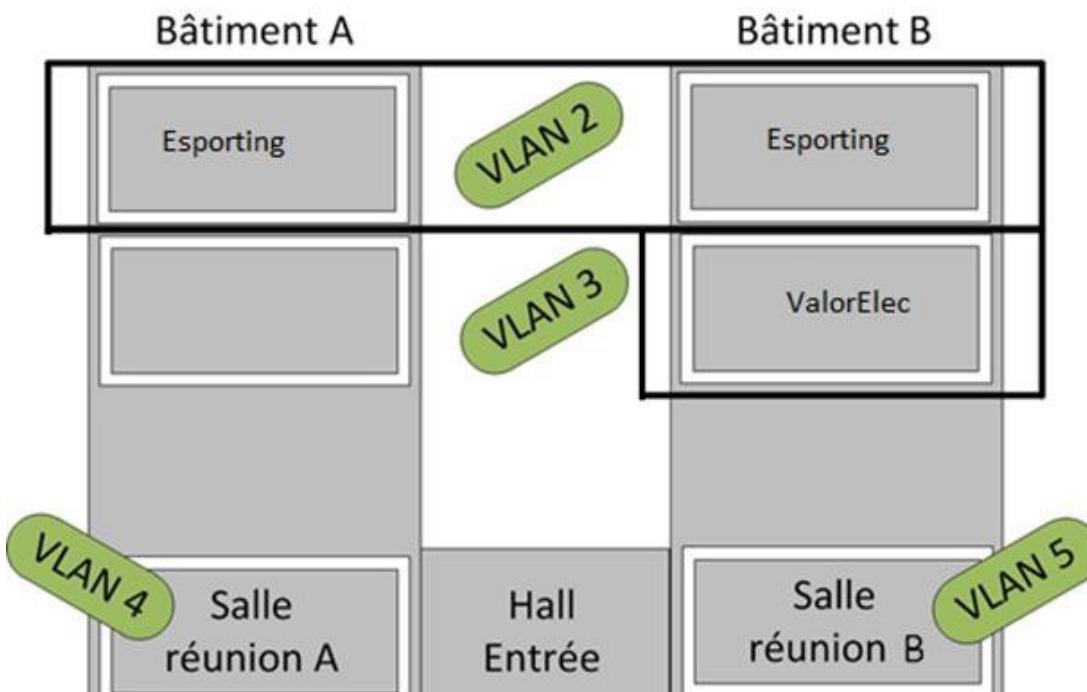


Figure 58 : Plan des services et de leurs VLAN

Nous devons donc créer les vlan sur le réseau des entreprises junior qui sera en 172.17.X.0/24

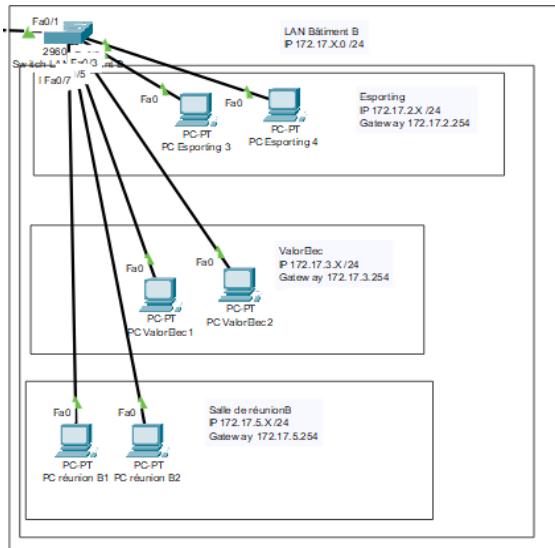
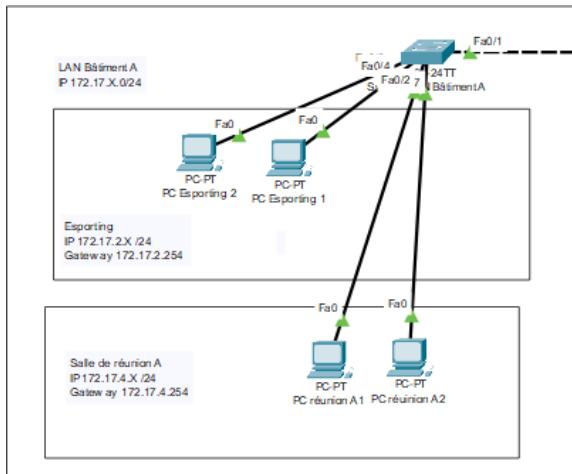


Figure 59 : Bâtiment A

Figure 60 : Bâtiment B

Premièrement, créons nos VLAN, ceux-ci vont être créer sur le switch cœur de notre réseau car des VLAN ont déjà été créer auparavant. Nous devons faire les commandes suivantes pour créer un vlan et lui attribuer un nom.

```
enable
configure terminal
vlan <numéro de notre vlan>
name <nom de notre vlan>
```

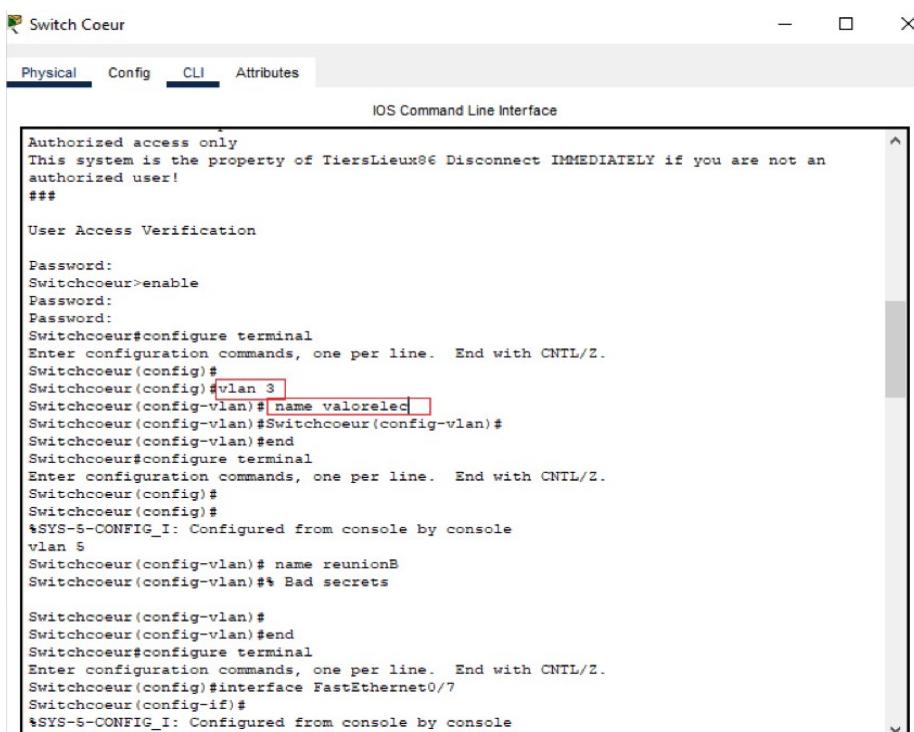


Figure 61 : Configuration du VLAN 3 ValorElec

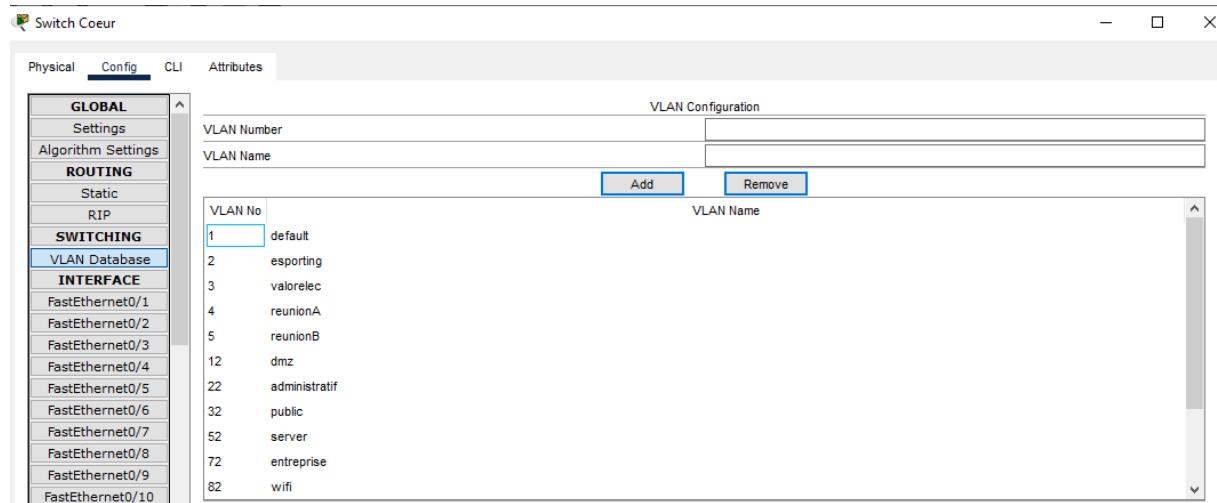


Figure 62 : Liste des VLAN créés

Nous devons reproduire cette action pour chaque VLAN, ce qui devient laborieux quand nous avons différents switches à paramétriser.

Tâche 2

Cette tâche consiste à mettre en place le protocole VTP sur les VLAN. Le protocole permet de diffuser la base de données contenant les vlan d'un de nos switch (le switch Serveur) pour que les autres switch (Client) puissent les récupérer. Ce qui pallie au problème de configuration énoncé plus haut, ainsi la configuration est ainsi facilitée. Puisque les vlan sont configurés sur notre switch cœur, c'est celui-ci qui va faire office de serveur VTP. Pour cela nous devons faire les commandes suivantes :

```
enable
configure terminal
vtp domain Chasseneuil
vtp mode server
vtp password cisco123
vtp version 2
```

Nous pouvons vérifier la bonne configuration de notre serveur VTP via la commande suivante :

```
enable
show vtp status
```

Figure 63 : Résultat de la commande

```
Switch Coeur
Physical Config CLI Attributes

IOS Command Line Interface

Password:
Password:

Switchcoeur>en
Switchcoeur>enable
Password:
Switchcoeur#show ntp status
Clock is synchronized, stratum 2, reference is 10.2.0.1
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E79D2404.0000022F (22:41:8.559 UTC Mon Mar 20 2023)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 423.46 msec, peer dispersion is -137269716642109.13 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 7 sec ago.

Switchcoeur#show vtp st
Switchcoeur#show vtp status
VTP Version capable      : 1 to 2
VTP version running      : 2
VTP Domain Name          : Chasseneuil
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : 0001.C9BA.3900
Configuration last modified by 192.168.1.254 at 3-21-23 03:19:51
Local updater ID is 192.168.1.254 on interface V11 (lowest numbered VLAN interface found)

Feature VLAN :
-----
VTP Operating Mode        : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 15
Configuration Revision    : 63
MD5 digest                : 0x50 0x9A 0x96 0xE3 0xE3 0x71 0xBD 0x7D
                           0x90 0xC6 0xB2 0x13 0xA0 0x5A 0x1A 0xF9
```

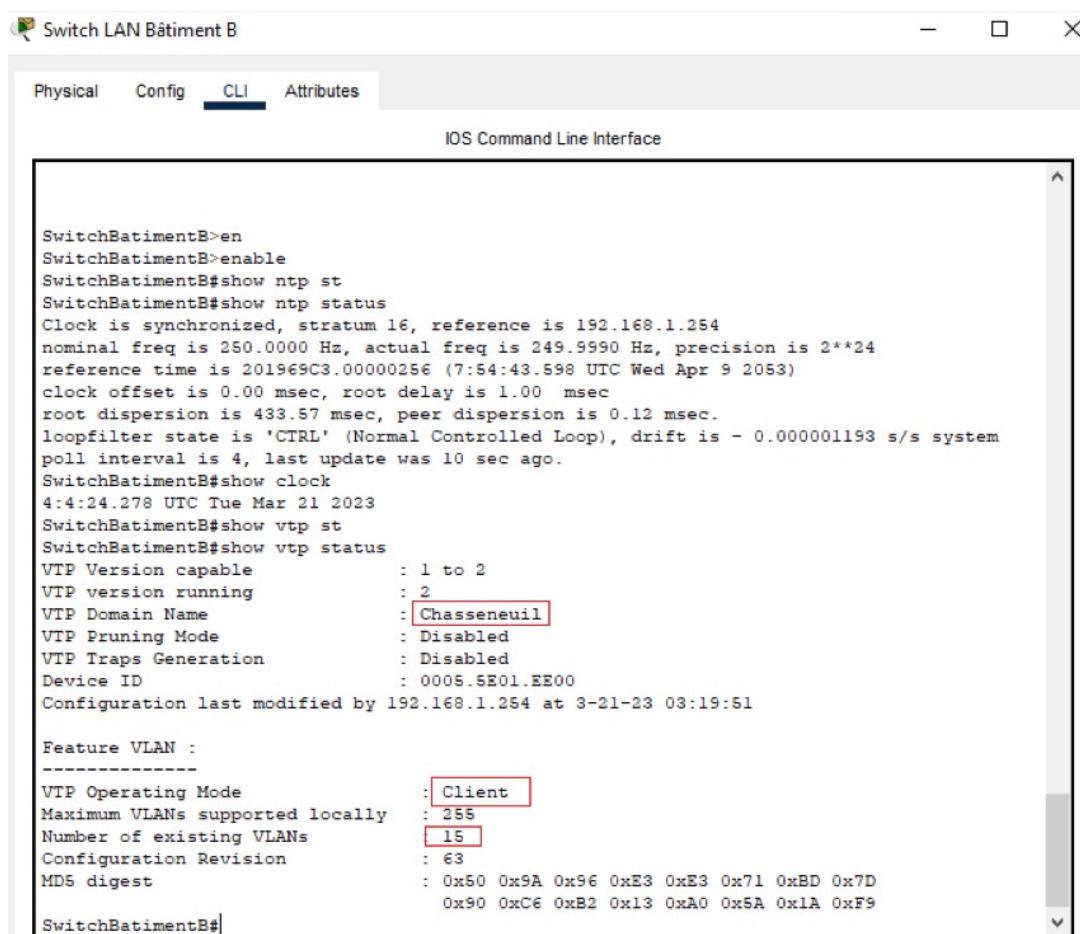
Ainsi notre switch est configuré en tant que serveur et il va pouvoir communiquer ses vlan aux autres switch. Or cette communication ne peut avoir lieu qu'avec un port configuré en trunk, Il faut donc veiller à ce que les deux interfaces soient en trunk.

Nous devons désormais configurer les clients, pour cela nous devons faire les commandes suivantes :

```
enable
configure terminal
vtp mode client
vtp version 2
vtp domain Chasseneuil
vtp password cisco123
```

Nous pouvons vérifier la configuration en nous rendant dans la base de données des vlan ou en faisant la commande suivante :

```
enable
show vtp status
```



```
SwitchBâtimentB>en
SwitchBâtimentB>enable
SwitchBâtimentB>show ntp st
SwitchBâtimentB>show ntp status
Clock is synchronized, stratum 16, reference is 192.168.1.254
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 201969C3.00000256 (7:54:43.598 UTC Wed Apr 9 2053)
clock offset is 0.00 msec, root delay is 1.00 msec
root dispersion is 433.57 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 10 sec ago.
SwitchBâtimentB#show clock
4:4:24.278 UTC Tue Mar 21 2023
SwitchBâtimentB#show vtp st
SwitchBâtimentB#show vtp status
VTP Version capable : 1 to 2
VTP version running : 2
VTP Domain Name : Chasseneuil
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0005.5E01.EE00
Configuration last modified by 192.168.1.254 at 3-21-23 03:19:51

Feature VLAN :
-----
VTP Operating Mode : Client
Maximum VLANs supported locally : 255
Number of existing VLANs : 15
Configuration Revision : 63
MD5 digest : 0x50 0x9A 0x96 0xE3 0xE3 0x71 0xBD 0x7D
              0x90 0xC6 0xB2 0x13 0xA0 0x5A 0x1A 0xF9
SwitchBâtimentB#
```

Figure 64 : Résultat de la commande

Tâche 3

Cette tâche vise à la mise en place d'un routage inter-vlan au sein de notre réseau. Le principe du routage inter-vlan est de pouvoir faire communiquer entre eux deux appareils n'étant pas présents dans le même vlan. Le routage inter-vlan peut se faire via un routeur ou bien un switch de couche 3, c'est cette solution qui a été retenue dans notre cas.

Pour faire du routage inter-vlan, nous devons paramétriser une ip par VLAN qui servira de passerelle par défaut. Cela se fait via les commandes suivantes :

```
enable
configure terminal
interface vlan 2
ip address 172.17.2.254 255.255.255.0
exit
```

Nous devons faire cela pour tous les vlan présents sur nos switch en adaptant bien sur l'IP donnée à l'interface du vlan avec un numéro adapté. Enfin, nous devons activer le routage via la commande :

```
ip routing
```

Le routage inter-vlan est donc opérationnel mais les machines ne peuvent pas communiquer puisqu'elles sont dépourvues d'adresses IP pour le moment. Nous pouvons donc configurer les IP de manière statique, une par une en respectant le plan d'adressage, mais nous pouvons aussi les allouer dynamiquement via un serveur DHCP. C'est le choix qui a été retenu. Tous les vlan non pas besoin d'un adressage dynamique à l'image du vlan DMZ qui est constitué de serveurs qui ne doivent pas être en DHCP ou encore du vlan Serveur pour les mêmes raisons, nous créons donc un pool d'adresse IP sur mesure au vlan avec un plan d'adressage adapter.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
Réunion B	172.17.5.254	10.2.0.1	172.17.5.1	255.255.255.0	255	10.2.0.2
ValorElec	172.17.3.254	10.2.0.1	172.17.3.1	255.255.255.0	255	10.2.0.2
Réunion A	172.17.4.254	10.2.0.1	172.17.4.1	255.255.255.0	255	10.2.0.2
Réunion B	172.17.5.254	10.2.0.1	172.17.5.1	255.255.255.0	255	10.2.0.2
serverPool	0.0.0.0	0.0.0.0	10.2.0.0	255.255.255.0	255	10.2.0.2
Administratif	192.168.22.254	10.2.0.1	192.168.22.1	255.255.255.0	255	10.2.0.2
Entreprise	192.168.72.254	10.2.0.1	192.168.72.1	255.255.255.0	255	10.2.0.2
Public	172.16.32.254	10.2.0.1	172.16.32.1	255.255.255.0	255	10.2.0.2
Esporting	172.17.2.254	10.2.0.1	172.17.2.1	255.255.255.0	255	10.2.0.2

Figure 65 : Pool DHCP

Nous devons ensuite activer le relai DHCP sur notre switch de couche 3 pour chaque vlan via la commande :

```
enable
configure terminal
interface vlan 2
ip helper-address 10.2.0.1
exit
write
```

Ainsi, nos appareils sont en mesure de recevoir une adresse IP dynamiquement et ainsi de communiquer avec notre réseau.

Tâche 4

Cette tâche consiste en la création de tests sur la maquette simulée pour vérifier le fonctionnement du routage inter-vlan. Cela se fera via des ping d'une machine à une autre via la commande prompte. Ces tests ne seront pas exhaustifs puisque le nombre d'appareils est important.

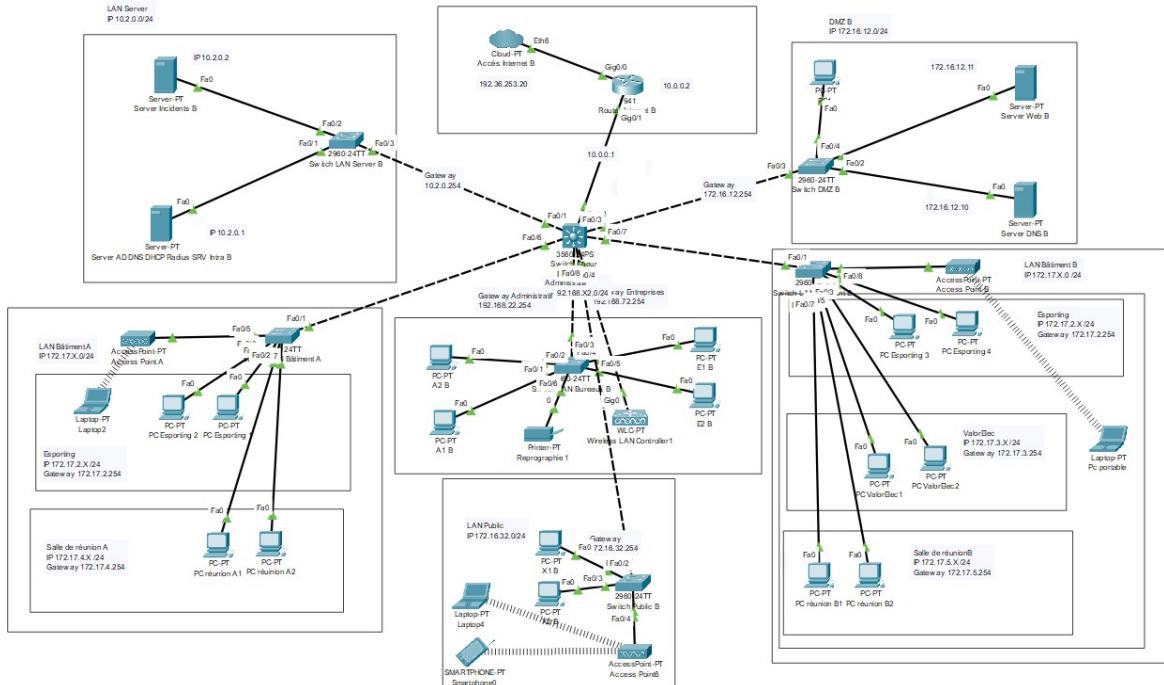


Figure 66 : Maquette Cisco mission 3

```
ping 172.17.5.1
Pinging 172.17.5.1 with 32 bytes of data:
Request timed out.
Reply from 172.17.5.1: bytes=32 time=7ms TTL=127
Reply from 172.17.5.1: bytes=32 time=35ms TTL=127
Reply from 172.17.5.1: bytes=32 time=39ms TTL=127

Ping statistics for 172.17.5.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 39ms, Average = 27ms

C:\>ipconfig

Bluetooth Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....:::
    IPv6 Address.....:::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....:
                           0.0.0.0

Wireless0 Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: FE80::203:E4FF:FE4E:CA58
    IPv6 Address.....:::
    IPv4 Address.....: 10.0.82.2
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....:
                           10.0.82.254
```

Figure 67 : Ping 1

```
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.22.254: Destination host unreachable.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ip config
Invalid Command.

C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: FE80::20A:F3FF:FE4B:87EA
    IPv6 Address.....:::
    IPv4 Address.....: 192.168.22.2|
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....:
                           192.168.22.254
```

Figure 68 : Ping 2

```
C:\>ping 172.17.3.1

Pinging 172.17.3.1 with 32 bytes of data:

Request timed out.
Reply from 172.17.3.1: bytes=32 time<1ms TTL=127
Reply from 172.17.3.1: bytes=32 time<1ms TTL=127
Reply from 172.17.3.1: bytes=32 time<1ms TTL=127

Ping statistics for 172.17.3.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: FE80::202:17FF:FE75:B7E2
    IPv6 Address.....: :::
    IPv4 Address.....: 172.17.2.4
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: :::
                           172.17.2.254
```

Figure 69 : Ping 3

Nous pouvons donc constater que le routage inter-vlan est bien en place. Les vlan sont configurés et les plans d'adressage correspondent. Pour pouvoir constater par vous-même, la maquette sera disponible en téléchargement.

Mission 4 : centralisation des journaux

Cette mission consiste en la configuration de la centralisation des journaux via Syslog. Cette tâche se fera sur l'environnement virtuel avec un serveur Ubuntu adressé en 10.2.0.2 et sur Cisco Packet Tracer.

Premièrement, qu'est-ce que Syslog ?

Syslog est un protocole qui définit un service de journaux d'événements d'un système informatique. Syslog est aussi le nom du format qui permet ces échanges. Le serveur Syslog a donc pour fonction de collecter et de centraliser les messages Syslog provenant des périphériques réseau à l'image des switch, routeurs pare-feu ou encore serveurs.

Tâche 1

Le principe de cette tâche est de paramétrier un serveur Syslog, nous verrons premièrement comment le paramétrier sous Cisco Packet Tracer puis deuxièmement comment le paramétrier sur un serveur Ubuntu.

Syslog sous Cisco

Nous souhaitons donc créer un serveur Syslog qui centralisera les logs de nos appareils sur notre maquette. Pour cela nous allons utiliser le serveur de gestion des incidents et inventaires adressé en 10.2.0.2.

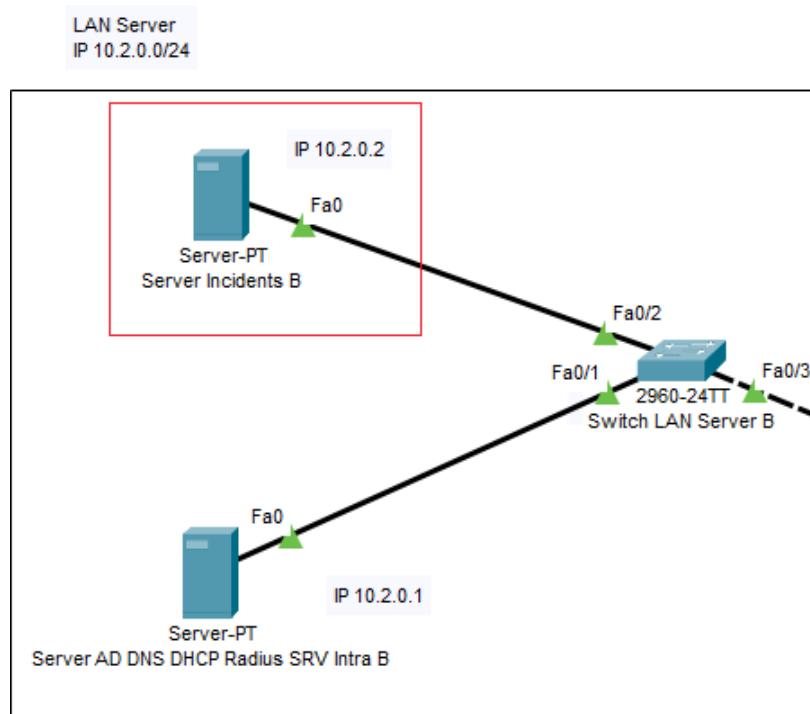


Figure 70 : Serveur d'incidents

Nous devons premièrement configurer notre serveur avec le service syslog activer. Nous devons nous rendre sur le serveur et cliquer sur On.

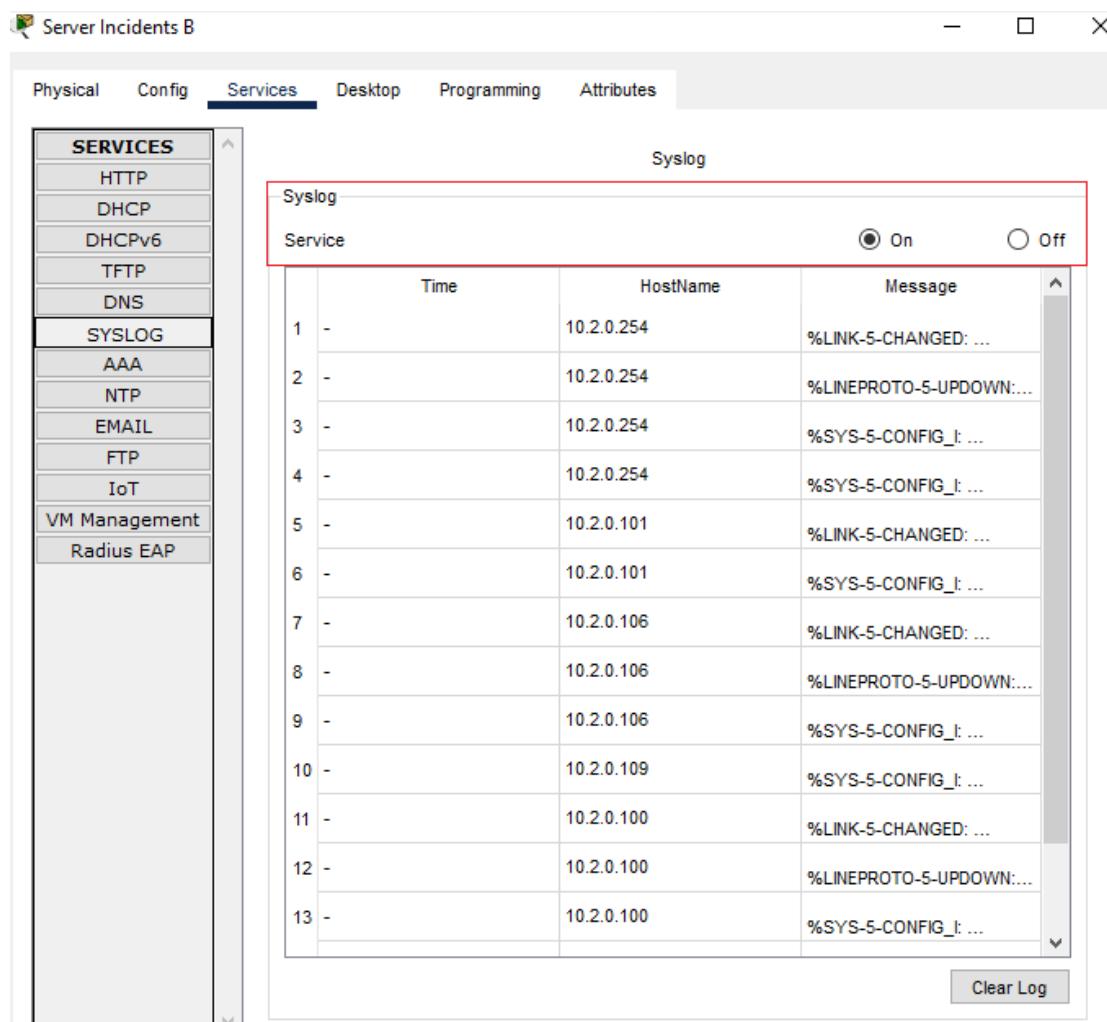


Figure 71 : Mise en route du service Syslog

Nous pouvons constater la présence de logs, c'est suite à la configuration de certains appareils pour m'assurer que les commandes que j'utilisai étaient adaptées. Le serveur syslog est donc mis en place, nous pouvons ensuite configurer les clients qui lui enverront leurs logs via le protocole syslog. Via cette manipulation, nous aurons un accès au logs de tous nos appareils réseaux sur le serveur.

Pour pouvoir envoyer nos logs sur le serveur Syslog, nous devons faire la commande suivante sur le matériel :

```
enable
configure terminal
logging 10.2.0.2
exit
exit
write
```

Syslog sous Ubuntu

Un serveur Ubuntu peut faire office de serveur Syslog, or pour cela il faut déjà disposer d'un serveur Ubuntu. Nous devons donc nous rendre sur le site [Ubuntu](#) qui est l'une des distributions basée sous linux et télécharger l'ISO de notre serveur. Nous installons ensuite notre serveur via VirtualBox et devons paramétriser son adressage. Premièrement, notre serveur doit être adressé en 10.2.0.2 pour être fidèle à l'adresse Cisco, deuxièmement, il doit se trouver dans le LAN Serveur donc doit avoir comme passerelle par défaut 10.2.0.254. Nous devons donc modifier le fichier de configuration du réseau de notre serveur pour cela nous devons faire les manipulations suivantes. Nous devons nous rendre sur le serveur puis entrer nos identifiants :

```
login: administrateur
password: Eragone123
```

Nous devons ensuite nous rendre dans le dossier suivant via les commandes suivantes :

```
sudo vi /etc/netplan/00-installer-config.yaml
```

Ce qui donne le fichier que nous devons modifier comme dans la configuration que j'ai réalisée sur l'image suivante :

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses:
        - 10.2.0.2/24
      routes:
        - to: default
          via: 10.2.0.254
      nameservers:
        addresses:
          - 10.2.0.1
  version: 2
```

Figure 72 : Configuration IP du serveur

Pour quitter le mode VIM nous faisons échap et :wq (write and quit) entrer. Enfin, pour nous assurer que la configuration est bonne et qu'avec cela nous pouvons communiquer avec notre routeur Vyos, nous pouvons faire des pings. Un ping de la passerelle LAN Serveur en 10.2.0.254 et un sur la passerelle LAN Bureaux en 192.168.2.254. Nous devons utiliser les commandes suivantes :

```
ping 10.2.0.254
ping 192.168.2.254
```

```
administrateur@ubuntu:~$ ping 10.2.0.254
PING 10.2.0.254 (10.2.0.254) 56(84) bytes of data.
64 bytes from 10.2.0.254: icmp_seq=1 ttl=64 time=1.37 ms
64 bytes from 10.2.0.254: icmp_seq=2 ttl=64 time=1.22 ms
64 bytes from 10.2.0.254: icmp_seq=3 ttl=64 time=1.38 ms
64 bytes from 10.2.0.254: icmp_seq=4 ttl=64 time=1.15 ms
^C
--- 10.2.0.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3201ms
rtt min/avg/max/mdev = 1.150/1.280/1.382/0.098 ms
administrateur@ubuntu:~$ ping 192.168.2.254
PING 192.168.2.254 (192.168.2.254) 56(84) bytes of data.
64 bytes from 192.168.2.254: icmp_seq=1 ttl=64 time=1.28 ms
64 bytes from 192.168.2.254: icmp_seq=2 ttl=64 time=1.21 ms
64 bytes from 192.168.2.254: icmp_seq=3 ttl=64 time=2.20 ms
64 bytes from 192.168.2.254: icmp_seq=4 ttl=64 time=1.28 ms
^C
--- 192.168.2.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3171ms
rtt min/avg/max/mdev = 1.208/1.493/2.203/0.410 ms
```

Figure 73 : Résultats des ping

Nous devons ensuite procéder à l'installation du service rsyslog qui est une évolution de Syslog. Pour cela nous faisons les commandes suivantes :

```
sudo apt update && apt install rsyslog
```

Nous devons ensuite configurer notre serveur pour qu'il soit actif, pour cela nous devons éditer le fichier /etc/rsyslog.conf, nous devons éditer les lignes suivantes :

```
# provides UDP syslog reception
modules(load="imudp")
input(type="imudp" port="514")
```

Enfin, nous pouvons redémarrez notre service via la commande :

```
sudo systemctl restart rsyslog
```

Nous pouvons ensuite constater le bon fonctionnement de notre serveur syslog via la commande suivante :

```
sudo systemctl status rsyslog
```

```
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
"/etc/rsyslog.conf" 59L, 1380B écrit(s)
administrateur@ubuntu:~$ sudo systemctl restart rsyslog
administrateur@ubuntu:~$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-03-29 18:13:08 UTC; 19s ago
TriggeredBy: • syslog.socket
    Docs: man:rsyslogd(8)
          man:rsyslog.conf(5)
          https://www.rsyslog.com/doc/
   Main PID: 1575 (rsyslogd)
      Tasks: 5 (limit: 2237)
     Memory: 1.1M
        CPU: 8ms
      CGroup: /system.slice/rsyslog.service
              └─1575 /usr/sbin/rsyslogd -n -iNONE
```

Figure 74 : Résultat de la configuration active (running)

Nous pouvons ensuite configurer notre routeur Vyos en tant que client du serveur Syslog par exemple en nous rendant sur son interface et en faisant la commande :

```
set system syslog host 10.2.0.2 facility local7 level debug
```

```
Configuration path: system [ntpexit] is not valid
Set failed

[edit]
vyos@vyos#
[edit]
vyos@vyos# show interfaces
 ethernet eth0 {
     address 10.2.0.254/24
     hw-id 08:00:27:28:04:48
 }
 ethernet eth1 {
     address 192.168.2.254/24
     hw-id 08:00:27:42:44:bf
 }
 loopback lo {
 }
[edit]
vyos@vyos# exit
exit
vyos@vyos:~$ configure
[sledit]
vyos@vyos# set system syslog host 10.2.0.2 facility local7 level debug
[edit]
vyos@vyos#
```

Figure 75 : Résultat de la commande sur Vyos

Tâche 2

Cette tâche consiste en la configuration des équipements Cisco pour que ceux-ci envoient leurs logs sur le serveur dédié à cela donc le serveur 10.2.0.2. Pour configurer un client et donc un appareil, que ce soit routeur, switch L2 ou switch L3, nous devons faire la commande suivante :

```
enable
configure terminal
logging 10.2.0.2
exit
```

Ce qui donnera le résultat suivant :

```
Password:
RouterInternet>en
RouterInternet>enable
Password:
RouterInternet#conf
RouterInternet#configure ter
RouterInternet#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RouterInternet(config)#logging 10.2.0.2
RouterInternet(config)#exit
RouterInternet#
%SYS-5-CONFIG_I: Configured from console by console
%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.2.0.2 port 514 started - CLI initiated
```

Figure 76 : Résultat de logging 10.2.0.2

Nous devons ensuite configurer tous nos appareils de la même manière pour pouvoir centraliser les logs.

Une fois le matériel configuré, nous pouvons nous rendre sur le serveur Syslog et constater que les logs lui sont bien retournés.

Time	HostName	Message
1 -	10.2.0.101	%SYS-5-CONFIG_I: Configured from console by console
2 -	10.2.0.101	%LINK-5-CHANGED: Interface Vlan1, changed state to up
3 -	10.2.0.101	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, ...

Figure 77 : Logs

Retour de logs de l'appareil adresser en 10.2.0.101 qui est l'interface vlan 52 du switch LAN bureau B.

Nous pouvons constater que l'horodatage n'est pas affiché, nous devons donc rajouter cela en paramètre via la commande :

```
enable  
configure terminal  
service timestamps log datetime msec
```

Tâche 3

Cette tâche a pour objectif le test du bon fonctionnement du service mis en place, nous allons procéder à quelques tests dans le but de générer des logs et voir s'ils sont bien retournés sur le serveur Syslog. Je vais faire un shutdown puis un no shutdown sur le vlan 1 du switch du bâtiment A adressé en 10.2.0.105 sur l'interface vlan52, cela générera des logs qui seront transmis via le protocole syslog.

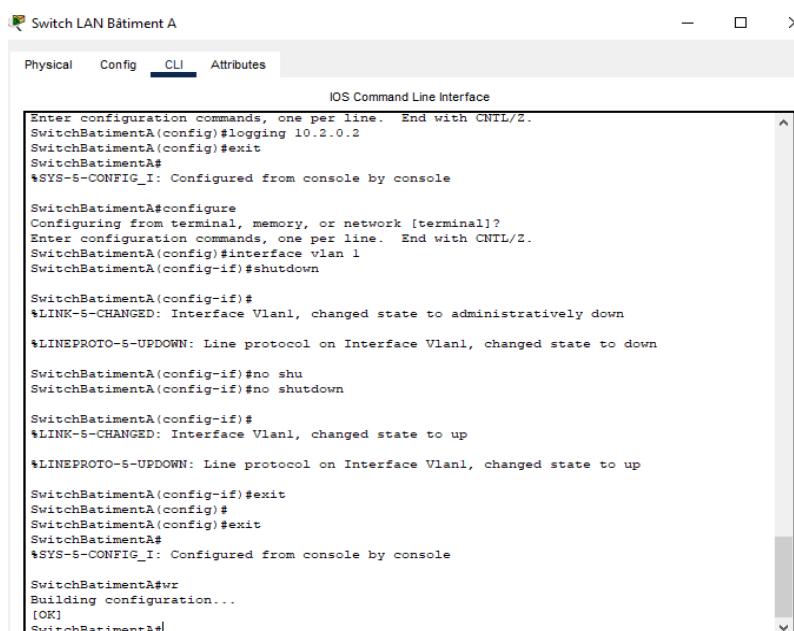


Figure 78 : test n°1

9	03.20.2023 09:27:17.365 PM	10.2.0.102	%SYS-5-CONFIG_I Configured from console by console
10	03.20.2023 09:29:32.006 PM	10.2.0.254	%LINK-5-CHANGED: Interface Vlan1, changed state to ...
11	03.20.2023 09:29:32.006 PM	10.2.0.254	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, ...
12	03.20.2023 09:29:36.432 PM	10.2.0.254	%LINK-5-CHANGED: Interface Vlan1, changed state to up
13	03.20.2023 09:29:36.432 PM	10.2.0.254	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, ...
14	03.20.2023 09:29:39.283 PM	10.2.0.254	%SYS-5-CONFIG_I Configured from console by console
15	03.20.2023 09:30:37.580 PM	10.2.0.101	%SYS-5-CONFIG_I Configured from console by console

Figure 79 : Résultat n°1

Le test numéro 2 consistera en la configuration du vlan 3 sur le switch public du bâtiment B adresser en 10.2.0.102 sur le vlan52.

```
SwitchPublic>en
SwitchPublic>enable
Password:
SwitchPublic#show clock
21:28:32.232 UTC Mon Mar 20 2023
SwitchPublic#show nt
SwitchPublic#show ntp st
SwitchPublic#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1990)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec.
loopfilter state is 'FSET' (Drift set from file), drift is - 0.000001193 s/s system poll
interval is 4, never updated.
SwitchPublic#show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.254
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E79D142D.00000353 (21:33:33.051 UTC Mon Mar 20 2023)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 81.19 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 15 sec ago.
SwitchPublic#conf
SwitchPublic#configure ter
SwitchPublic#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchPublic(config)#inter
SwitchPublic(config)#interface vla
SwitchPublic(config)#interface vlan 3
SwitchPublic(config-if)#
*Mar 20, 21:34:03.3434: %LINK-5-CHANGED: Interface Vlan3, changed state to up
*Mar 20, 21:34:03.3434: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed
state to up
SwitchPublic(config-if)#$
```

Figure 80 : Test n°2

15	03.20.2023 09:30:37.580 PM	10.2.0.101	%SYS-5-CONFIG_I: Configured from console by console
16	03.20.2023 09:34:03.205 PM	10.2.0.102	%LINK-5-CHANGED: Interface Vlan3, changed st...
17	03.20.2023 09:34:03.205 PM	10.2.0.102	%LINEPROTO-5-UPDOWN: Line protocol on ...
18	03.20.2023 09:36:55.620 PM	10.2.0.102	%SYS-5-CONFIG_I: Configured from console by console

Figure 81 : Résultat n°2

Nous pouvons voir que l'horodatage est correct, que les logs parviennent bien au serveur Syslog, la configuration est donc bonne.

Bilan :

Le fait de voir tous ces protocoles et principes en théorie est très intéressant mais lors de la mise en place sur un serveur Ubuntu par exemple, le manque d'expérience se fait ressentir au niveau du temps de réalisation des tâches mais aussi au niveau de la logique.

Sources

Article Windows NTP Windows Server Site complet Cisco

Mot de passe Cisco

Comment installer OpenSSH (correctif) Liste A-Z commande Cisco Réinitialiser mdp

VTP Cisco

Configurer l'IP d'un serveur Ubuntu Syslog Linux

Enregistrer ses logs Windows dans Rsyslog

Partie 2 : Mettre en place la haute-disponibilité et la sécurisation des équipements d'interconnexion

Mission 5 : tolérance aux pannes

Cette mission a pour objectif de recenser les différents points sensibles physique mais aussi logiciel pouvant entraîner une interruption du service ou des pertes de données et proposer des solutions permettant la tolérance de pannes. Celle-ci se décompose en 3 tâches.

Premièrement, qu'est-ce que la haute disponibilité ?

La haute disponibilité est le principe d'avoir un système informatique fonctionnel et d'avoir une disponibilité de celui-ci auprès des utilisateurs. Pour cela des moyens sont mis en œuvre pour y parvenir car dans une ère où tout est de plus en plus informatisé, les réseaux se doivent d'être disponibles et performants. Nous pouvons alors mettre en place de la redondance matérielle, vient alors le terme de cluster de haute disponibilité et la mise en place de processus, de règles à suivre permettant de réduire les erreurs et d'accélérer la reprise d'activité en cas d'erreurs ou de dysfonctionnements avec notamment la démarche ITIL.

Tâche 1

Cette tâche a pour but de recenser les problèmes physiques possibles et les propositions de solutions.

Problème physique	Solution
Panne de disques durs	-RéPLICATION DES DONNÉES SUR PLUSIEURS DISQUES DURS VIA L'UTILISATION DU RAID + DISQUE SPARE -UTILISATION DE LOGICIELS DE SURVEILLANCE DE DISQUES (CRYSTALDISKINFO GRATUIT OU HDTUNE PAYANT) -REMPLACEMENT DES DISQUES PRÉSENTANT DES PROBLÈMES, FAIBLESSES OU EN PANNE
Panne d'alimentation électrique	-UTILISATION D'ONDULEUR PERMETTANT LA CONTINUITÉ DE L'ALIMENTATION ÉLECTRIQUE DU MATERIEL ET LA STABILITÉ DU COURANT ÉLECTRIQUE (SURTENSION, SOUSTENSION)
Défaillance matériel	-MISE EN PLACE DE REDONDANCE POUR LE MATERIEL TEL QUE LES ROUTEURS, SERVEURS, SWITCHES -HSRP OU GLBP (CLUSTER DE ROUTEUR AYANT LA MÊME IP VIRTUELLE CE QUI APporte UNE REDONDANCE ET UNE RÉPARTITION DES RESSOURCES)
Aléa (Inondations, incendies, tremblement de terre...)	-MISE EN SÛRETÉ DES ÉQUIPEMENTS (ARMOIRES, SALLES CLIMATISÉES, RANGEMENT ET BRASSAGE PROPRE/ORGANISÉ)

Figure 82

Ces solutions permettent donc de mettre, d'installer et d'utiliser le matériel réseau de manière sécurisée et optimale. Permettant une tolérance aux pannes et donc une certaine pérennité du système d'information et donc de l'entreprise. Or tout ne réside pas dans l'installation et la sécurisation du matériel.

Tâche 2

En effet, cette liste orientée au niveau des problèmes et solutions pouvant être mises en place au niveau du système et/ou logiciels, complète la première.

Problème système et/ou logiciel	Solution
Perte de connexion réseau/saturation réseau	-Redondance des chemins et des routes alternatives -Mise en place du routage dynamique (les équipements adaptent leurs route) Switch -Mise en place de l'Etherchannel (augmente la bande passante et la redondance de liens) -Mise en place du Spanning Tree Protocol (évite les boucles)
Compatibilité du matériel et des logiciels utiliser	-Utiliser du matériel compatible avec les logiciels (firmware, pilotes) et protocoles utilisés (SNMP)
Erreurs lors de la configuration	-Utilisation des ressources pour faciliter la gestion des configurations (VTP) et sauvegarde régulière des configurations (TFTP)
Sécurité des équipements réseaux	-Mise en place de pare-feu, antivirus, système de détection d'intrusion et de prévention de celles-ci -Mise en place d'ACL des équipements Cisco

Figure 83 : Tableau de synthèse des problèmes logiciels/systèmes et les solutions envisageables

La bonne configuration de nos appareils réseaux et l'optimisation des communications permet de répartir la charge et ainsi d'accroître le phénomène de tolérance aux pannes.

Tâche 3

Cette tâche consiste en la création d'une maquette permettant la mise en place de différents procédés créés pour la tolérance aux pannes à l'image de l'Etherchannel ou encore du Spanning Tree Protocol. Le schéma suivant nous servira de base pour cela.

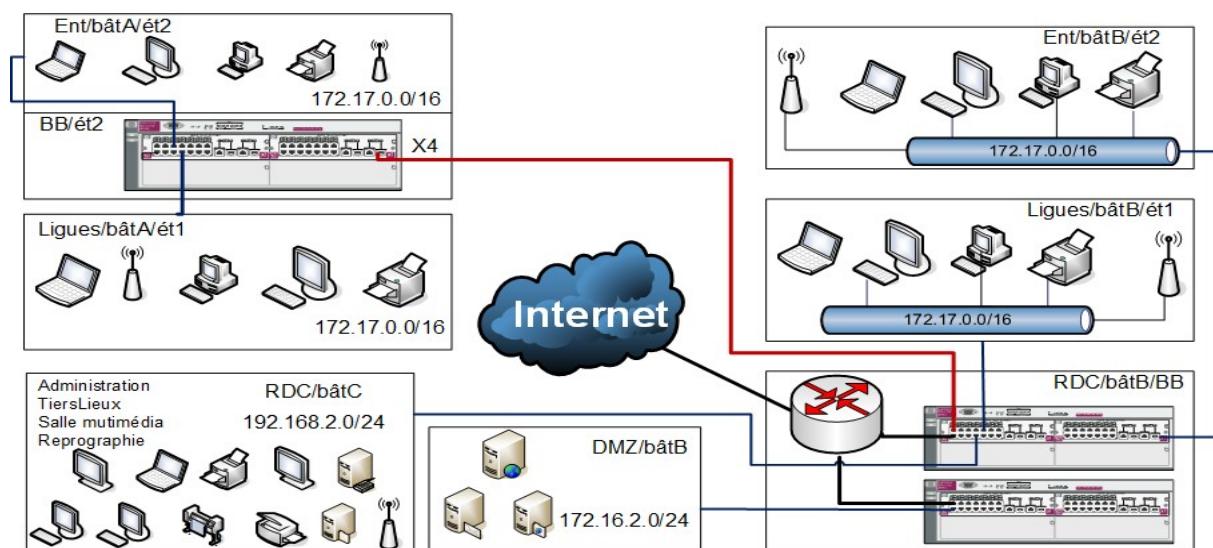


Figure 84 : Schéma réseau Chasseneuil

Celui-ci reprend le réseau de Chasseneuil fait au cours des missions précédentes de manière synthétique sans tous les services. Cette maquette servira de test pour la mise en place des protocole et services à l'image de l'Etherchannel, du Rapid Spanning Tree ainsi que de HSRP ou GLPB.

Figure 85 : Maquette test

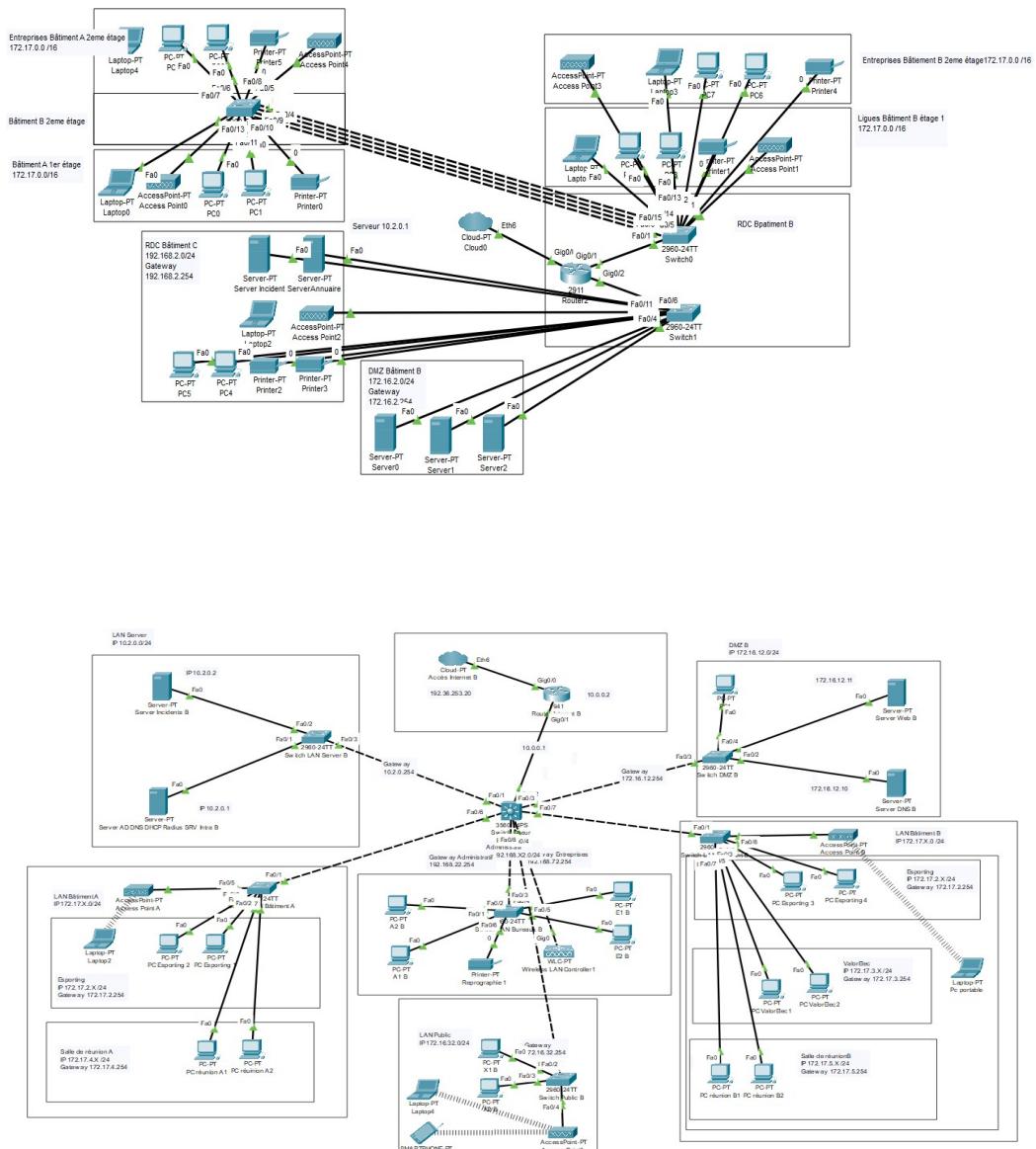


Figure 86 : Maquette originelle

Mission 6 : amélioration de la bande passante

Cette mission porte sur l'amélioration de la bande passante via la mise en place de liens Etherchannel. Cette installation doit se faire entre les deux commutateurs qui nous ont servi à mettre en place les VLAN 2, 3, 4 et 5 pour nos entreprises et salles de réunions.

Premièrement, qu'est-ce que l'Etherchannel ?

L'Etherchannel ou agrégation de lien permet de réunir plusieurs port réseau et donc plusieurs câbles physiques pour ne créer qu'un seul lien logique. Cela permet d'améliorer la bande passante car les ressources sont réparties sur les différents ports physiques mais aussi de garantir une disponibilité du lien logique car si l'un des ports tombe en panne alors l'un de ceux qui constituent cette agrégation prendra le relais. Deux protocoles sont disponibles pour créer un Etherchannel.

D'un côté, LACP pour Link Aggregation Control Protocol, celui-ci incorpore des règles vitesse, vlan, mode duplex, pour que la configuration se fasse bien. Nous retrouvons ensuite le PAgP, pour Port Aggregation Protocol qui fonctionne de la même manière que LACP mais il appartient à Cisco.

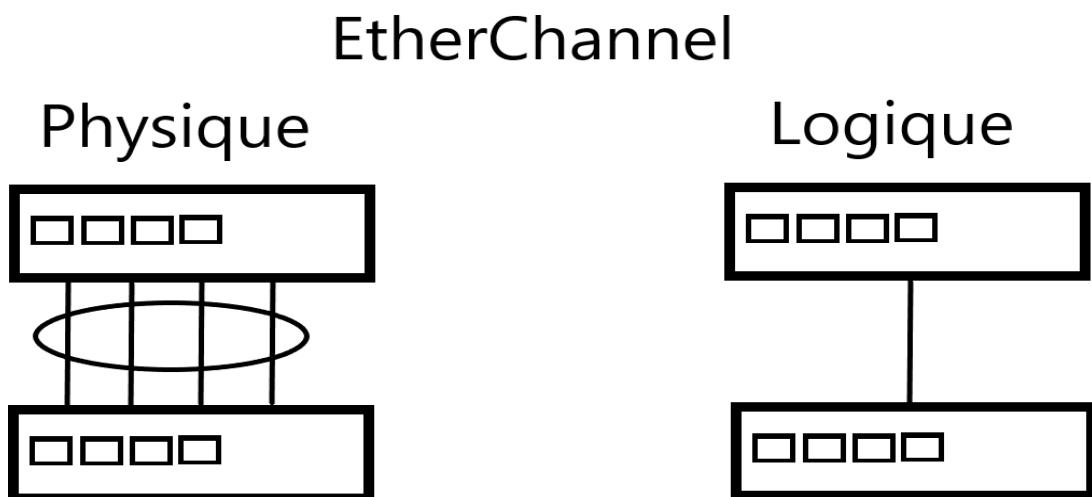


Figure 87 : Représentation de l'Etherchannel

Tâche 1

Le but de cette tâche est l'implémentation de l'agrégation de liens via Etherchannel entre les deux routeurs qui on servit de tests pour mettre en place les vlan.

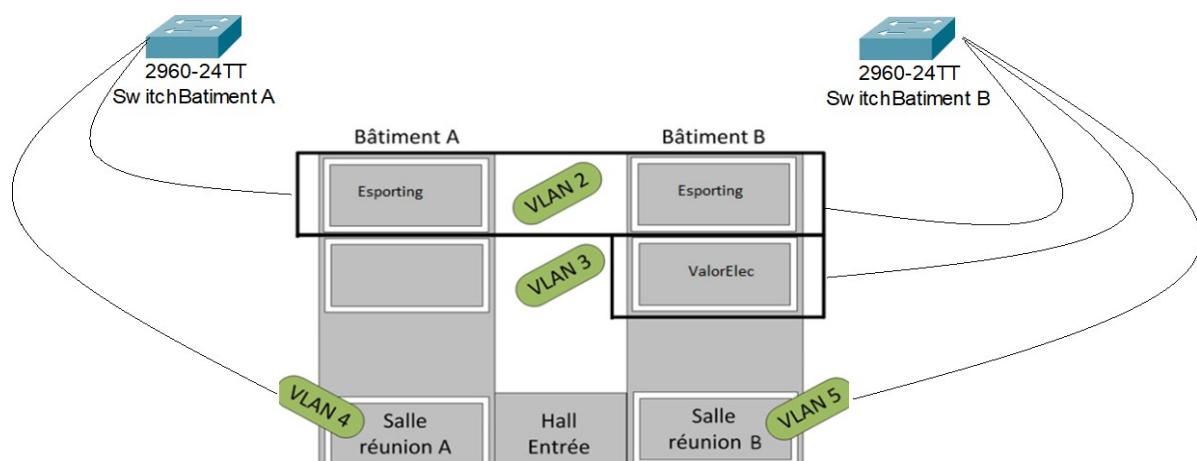


Figure 88 : Implantation des switches

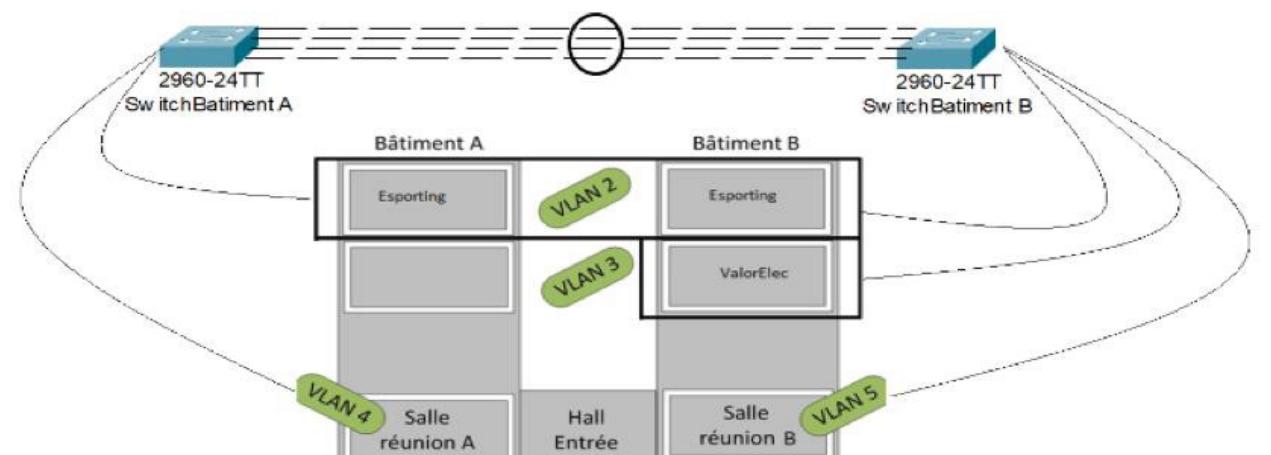


Figure 89 : Implémentation des switches avec Etherchannel

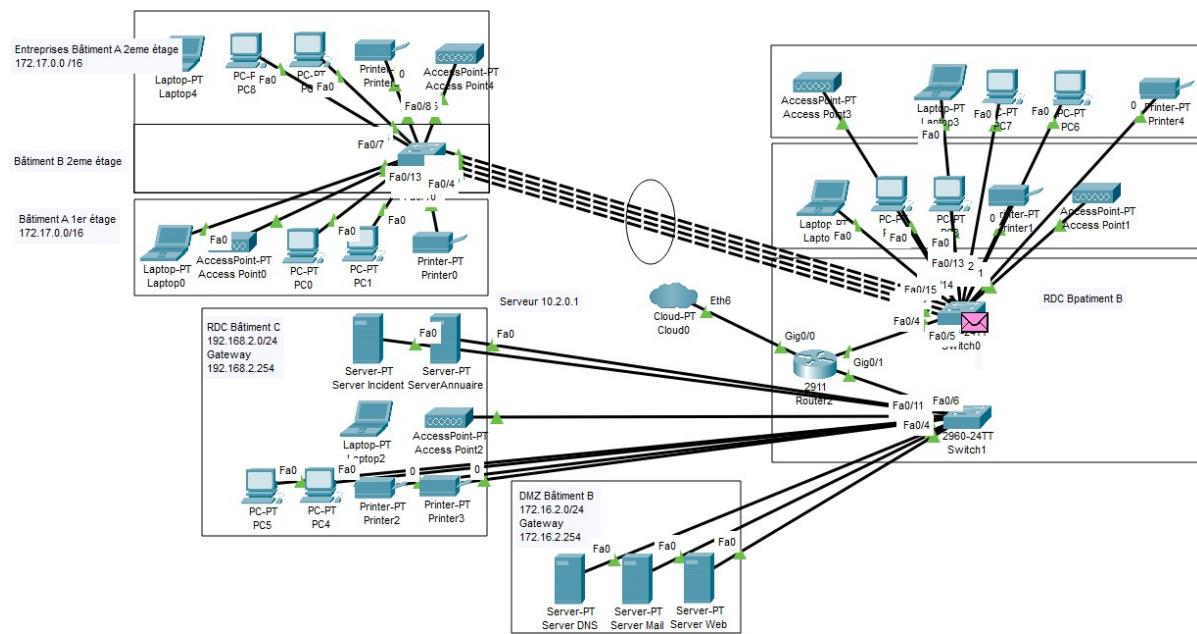


Figure 90 : Etherchannel sur la maquette test n°1

```

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol      Ports
-----+-----+-----+
      1          PAgP        Fa0/1 (P)  Fa0/2 (P)  Fa0/3 (P)  Fa0/4 (P)

```

Figure 91 : Etherchannel sur la maquette test n°2

Nous devons donc désormais procéder à la configuration de l'Etherchannel sur la maquette comportant le réseau complet.

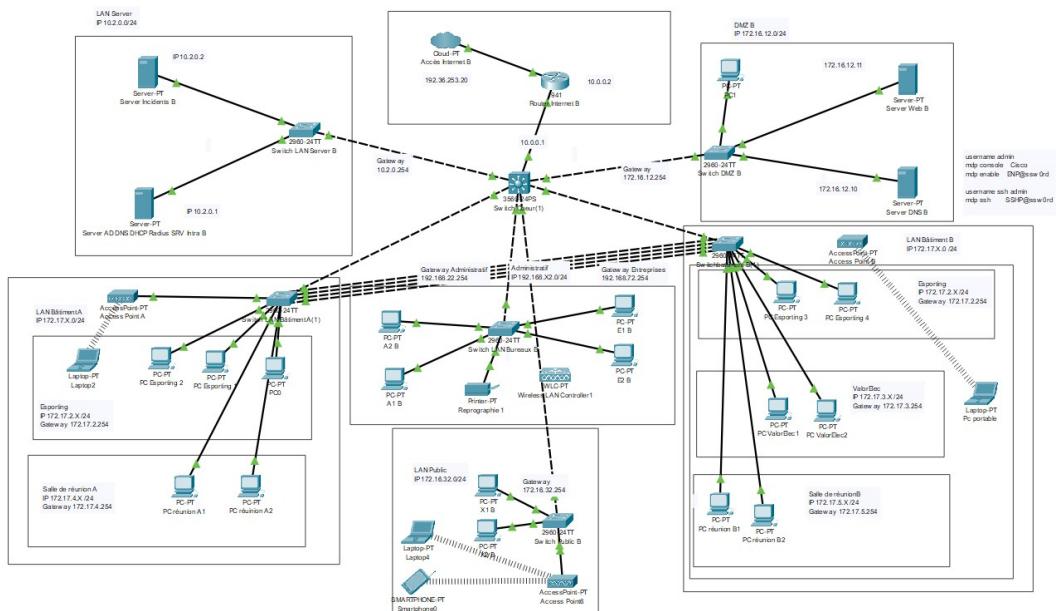


Figure 92 : Etherchannel sur la maquette réseau complète n°1

```

SwitchBatiementB#show e
SwitchBatiementB#show etherchannel s
SwitchBatiementB#show etherchannel summary
Flags: D - down      P - in port-channel
      I - stand-alone  S - suspended
      H - Hot-standby (LACP only)
      R - Layer3       S - Layer2
      U - in use        f - failed to allocate aggregator
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
-----+-----+-----+
      1  Pol(SU)      -          Fa0/13(P)  Fa0/14(P)  Fa0/15(P)  Fa0/16(P)
SwitchBatiementB#

```

Figure 93 : Résultat de la configuration n°2

```
[OK]
SwitchBâtimentA#show e
SwitchBâtimentA#show etherchannel su
SwitchBâtimentA#show etherchannel summary
Flags: D - down      P - in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3       S - Layer2
      U - in use       f - failed to allocate aggregator
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
-----+-----+-----+
1      Po1(SU)      -          Fa0/13(P) Fa0/14(P) Fa0/15(P) Fa0/16(P)
SwitchBâtimentA#
```

Figure 94 : Résultat de la configuration n°3

Tâche 2

L'objectif est de tester le bon fonctionnement sur le réseau simulé sous Packet Tracer et enfin de rédiger la procédure de mise en place de l'Etherchannel.

Test

Dans un premier temps, nous pouvons constater notamment via les screenshot plus haut que les deux appareils ont bien été configurés et que l'agrégation de liens est active. Nous pouvons le voir via Po1 (SU) qui signifie "Layer 2" (couche 2) pour S et "in use" pour U et cela pour nos deux machines. De plus, nous pouvons voir via la lettre P que nos ports allant de Fa0/13 à Fa0/16 sont bien pris en compte. Par ailleurs, les liens sont bien verts, témoignant du bon fonctionnement de l'Etherchannel, qui, s'il ne fonctionnait pas nous donnerai 3 ports du switch Bâtiment B en orange fixe, montrant que le Protocol Spanning Tree bloque 3 portssur 4 pour éviter les boucles. Il faut faire la commande suivante pour que spanning tree ne bloque pas le Po1.

```

enable
configure terminal
spanning-tree vlan 1 root primary

```

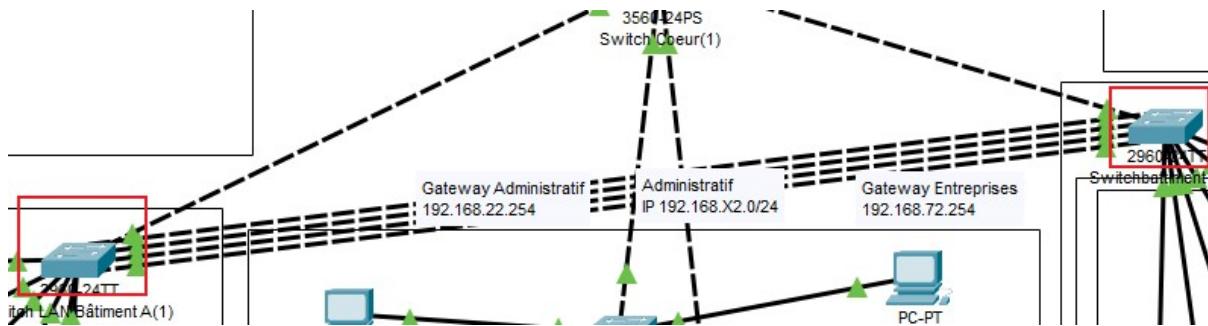


Figure 95 Liens logique actif

Nous pouvons vérifier que nos portchannel fonctionnent et sont connectés via les commandes :

```
show interface port-channel 1
```

```

Switchbattiment B(1)
Physical Config CLI Attributes
IOS Command Line Interface
 0 input packets with dribble condition detected
--More--
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
 2357 packets output, 263570 bytes, 0 underruns

SwitchBatiementB#show interfaces port-channel 1
Port-channell is up, line protocol is up (connected)
Hardware is EtherChannel, address is 0007.ec04.8c85 (bia 0007.ec04.8c85)
MTU 1500 bytes, BW 500000 Kbit, DLY 1000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 500Mb/s
input flow-control is off, output flow-control is off
Members in this channel: Fa0/13 ,Fa0/14 ,Fa0/15 ,Fa0/16 ,
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, 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
  956 packets input, 193351 bytes, 0 no buffer
  Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 watchdog, 0 multicast, 0 pause input
  0 input packets with dribble condition detected
--More--
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to up

```

Figure 96 : résultats de la commande n°1

The screenshot shows a window titled "Switch LAN Bâtiment A(1)" with the "CLI" tab selected. The title bar includes standard window controls: minimize, maximize, and close. Below the title bar is a menu bar with "Physical", "Config", "CLI" (which is underlined), and "Attributes". The main area is labeled "IOS Command Line Interface". The output of the command "show interfaces p" is displayed, with the first few lines of the output highlighted by a red rectangle:

```
Index Load Port EC state No of bits
-----+-----+-----+-----+
 0    00 Fa0/13 On      0
 0    00 Fa0/14 On      0
 0    00 Fa0/15 On      0
 0    00 Fa0/16 On      0
Time since last port bundled: 00d:00h:04m:06s Fa0/16
SwitchBatemtA#
SwitchBatemtA#show int
SwitchBatemtA#show interfaces p
SwitchBatemtA#show interfaces port-channel 1
Port-channell is up, line protocol is up (connected)
Hardware is EtherChannel, address is 0060.47ea.bbcc (bia 0060.47ea.bbcc)
MTU 1500 bytes, BW 500000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 500Mb/s
input flow-control is off, output flow-control is off
Members in this channel: Fa0/13 ,Fa0/14 ,Fa0/15 ,Fa0/16 ,
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, 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
 956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 watchdog, 0 multicast, 0 pause input
 0 input packets with dribble condition detected
--More-- |
```

Figure 97 : Résultats de la commande n°2

Procédure

Premièrement, nous devons choisir les ports qui nous permettront la mise en place des liens. Pour notre maquette, se seront les ports fastethernet 0/13 à 0/16. Nous plaçons des liens pour Trunk sur ces ports et entrons en mode configuration sur nos deux switches. Nous devons ensuite faire les commandes suivantes :

```
interface range fastethernet 0/13-16
channel-group 1 mode on
```

Nous devons configurer le mode trunk sur le Po1 via:

```
interface port-channel 1
switchport mode trunk
```

Nous pouvons ensuite configurer le load balancing via la commande :

```
configure terminal
port-channel load-balance src-mac #config le load balancing sur l'adresse MAC
source
```

Nous pouvons ensuite vérifier la bonne configuration de nos port-channel via les commandes suivantes:

```
enable
show etherchannel summary
```

```
SwitchBatimentA#show etherchannel summary
Flags: D - down      P - in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3       S - Layer2
      U - in use        f - failed to allocate aggregator
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+
1      Po1(SU)       -          Fa0/13(P)  Fa0/14(P)  Fa0/15(P)  Fa0/16(P)
SwitchBatimentA#
```

Figure 98 : Résultat de la commande

```
enable
show interface port-channel 1
```

```
SwitchBatimentA#show interfaces port-channel 1
Port-channell is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0060.47ea.bbcc (bia 0060.47ea.bbcc)
  MTU 1500 bytes, BW 500000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 500Mb/s
  input flow-control is off, output flow-control is off
  Members in this channel: Fa0/13 ,Fa0/14 ,Fa0/15 ,Fa0/16 ,
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, 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
```

Figure 99 : Résultat de la commande 1

```
enable
show etherchannel port-channel
```

```
Ports in the Port-channel:
Index Load  Port      EC state      No of bits
-----+-----+-----+
  0   00   Fa0/13   On           0
  0   00   Fa0/14   On           0
  0   00   Fa0/15   On           0
  0   00   Fa0/16   On           0
Time since last port bundled: 00d:00h:44m:38s Fa0/16
SwitchBatimentA#
```

Figure 100 : Résultat de la commande 2

Nous pouvons donc constater que les paquets passent bien sur notre lien logique via la simulation de packet tracer, une démonstration vidéo sera disponible.

Mission 7 : tolérance aux pannes des commutateurs

L'objectif de cette mission est de mettre en place le protocole Rapid Spanning Tree et de faire une série de tests visant à simuler des pannes à différents endroits. Cette mission se décompose en 2 tâches, l'une orientée sur la mise en place et l'autre sur la réalisation des tests.

Premièrement, qu'est-ce que le protocole Rapid Spanning Tree ?

Spanning Tree est un protocole de couche 2 permettant d'éviter les boucles dans un réseau. Celles-ci peuvent générer des tempêtes de diffusion (tempête de broadcast) qui est une saturation du réseau pouvant aller jusqu'au déni de services, paralysant ainsi complètement le réseau. Il est donc important d'activer Spanning Tree s'il ne l'est pas déjà d'usine.

Nous avons une topologie constituée de VLAN, Spanning Tree doit donc être configuré pour prendre en compte les VLAN. Pour cela, différents protocoles existent, à l'image de MSTP pour Multiple Spanning Tree Protocol ou encore de PVST pour Per-VLAN Spanning Tree qui est propriétaire à Cisco. Cela permet d'adapter le protocole spanning tree pour chaque VLAN ainsi, une boucle sur le VLAN 12 ne sera pas forcément une boucle sur le VLAN 22.

Tâche 1

Cette tâche consiste donc en la mise en place du Rapid-PVST pour Rapid Per-Vlan Spanning Tree sur les switchs de notre réseau. Pour cela, nous devons nous rendre sur nos différents switches et faire la commande suivante:

```
enable  
configure terminal  
spanning-tree mode rapid-pvst
```

Lors des choix du mode, deux protocoles sont proposés. Le PVST et le Rapide PVST. Rapid PVST est une amélioration de PVST. Il est plus rapide et permet lors d'un problème de converger le flux par un autre port. La transition d'un port à l'état *blocking* (port causant une boucle) à l'état de *forwarding* est plus rapide. Le lien perdu est donc rapidement récupéré.

Nous devons ensuite déclarer un switch en tant que root, celui-ci fait office de référence de la topologie réseau. Pour le repérer nous pouvons faire la commande suivante:

```
enable  
show spanning-tree
```

```

Switchcoeur#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID  Priority  24577
    Address  000D.BD57.092B
    This bridge is the root
    Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority  24577 (priority 24576 sys-id-ext 1)
    Address  000D.BD57.092B
    Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
    Aging Time 20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/1          Desg FWD 19        128.1    P2p
  Fa0/3          Desg FWD 19        128.3    P2p
  Fa0/4          Desg FWD 19        128.4    P2p
  Fa0/5          Desg FWD 19        128.5    P2p
  Fa0/6          Desg FWD 19        128.6    P2p
  Fa0/7          Desg FWD 19        128.7    P2p
  Fa0/2          Desg FWD 19        128.2    P2p

```

Figure 101 : Résultat de la commande

Nous pouvons constater que notre switch cœur est le root du réseau. Enfin pour constater l'état du spanning tree sur une machine nous pouvons faire la commande suivante :

```

enable
show spanning-tree

```

```

SwitchBatiementB#show spanning
SwitchBatiementB#show spanning-tree
VLAN001
  Spanning tree enabled protocol rstp
  Root ID  Priority  24577
    Address  000D.BD57.092B
    Cost     19
    Port     1(FastEthernet0/1)
    Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority  28673 (priority 28672 sys-id-ext 1)
    Address  00D0.D3A8.BC99
    Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
    Aging Time 20

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Fa0/1          Root FWD 19        128.1    P2p
  Fa0/8          Desg FWD 19        128.8    P2p
  Po1           Desg FWD 7         128.27   Shr
  Fa0/15         Desg FWD 19        128.15   P2p
  Fa0/14         Desg FWD 19        128.14   P2p
  Fa0/13         Desg FWD 19        128.13   P2p
  Fa0/16         Desg FWD 19        128.16   P2p

VLAN002
  Spanning tree enabled protocol rstp
  Root ID  Priority  24578
    Address  000D.BD57.092B
    Cost     19
    Port     1(FastEthernet0/1)
    Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

```

Figure 102 : Résultat de la commande sur Switch Bat B

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Fa0/3	Root	FWD	19	128.3		P2p
Fa0/4	Desg	FWD	19	128.4		P2p
Fa0/5	Altn	BLK	19	128.5		P2p

Figure 103 : Résultat de la commande sur Switch DMZ

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Fa0/1	Root	FWD	19	128.1		P2p
Fa0/2	Desg	FWD	19	128.2		P2p
Pol	Altn	BLK	7	128.27		Shr
Fa0/13	Desg	FWD	19	128.13		P2p
Fa0/15	Desg	FWD	19	128.15		P2p
Fa0/8	Altn	BLK	19	128.8		P2p
Fa0/14	Desg	FWD	19	128.14		P2p
Fa0/16	Desg	FWD	19	128.16		P2p

Figure 104 : Résultat de la commande sur Switch Bat A

Nous pouvons constater que le spanning tree est bien paramétré, puisque les ports générateurs de boucles sont en état bloqués.

Tâche 2

Cette tâche a pour but de tester la solution proposée via la simulation de pannes. Pour simuler celle-ci je vais faire un shutdown sur des ports dans le but de voir si les flux sont redirigés via le protocole spanning tree sur un autre port, passant donc par un autre chemin.

Tout d'abord un rappel de la maquette actuelle :

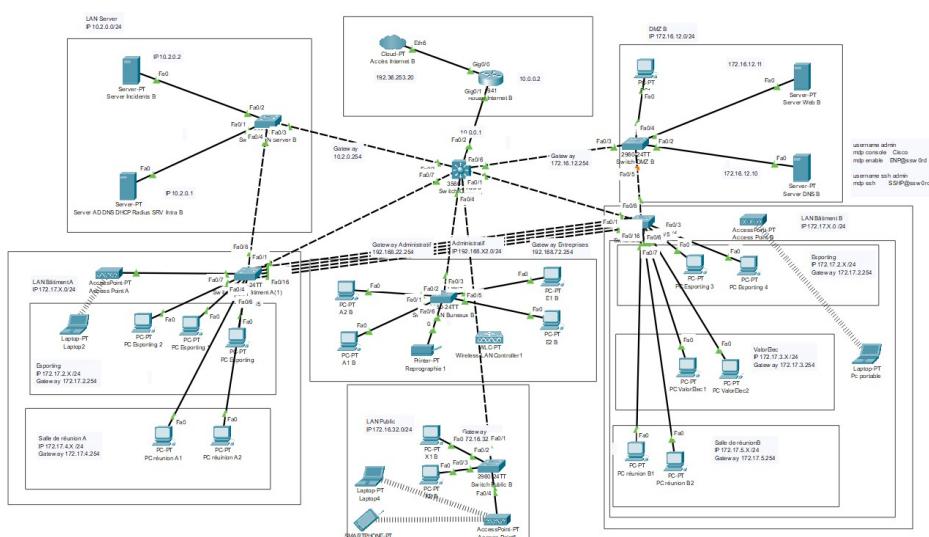


Figure 105 : Maquette

Switch	Port	Avant test				Résultat			
		Interface	Role	Sts	Cost	Interface	Role	Sts	Cost
Switch Bat A	Fa0/1	Fa0/1	Root	FWD	19	Fa0/2	Desg	BLK	19
		Fa0/2	Desg	FWD	19	Pol	Root	FWD	7
		Pol	Altn	BLK	7	Fa0/13	Desg	BLK	19
		Fa0/13	Desg	FWD	19	Fa0/15	Desg	BLK	19
		Fa0/15	Desg	FWD	19	Fa0/8	Altn	BLK	19
		Fa0/8	Altn	BLK	19	Fa0/14	Desg	BLK	19
		Fa0/14	Desg	FWD	19	Fa0/16	Desg	BLK	19
		Fa0/16	Desg	FWD	19				
Switch Bat A	Fa0/1 et Fa0/8	Fa0/2	Desg	BLK	19	Fa0/3	Desg	FWD	19
		Pol	Root	FWD	7	Fa0/4	Desg	FWD	19
		Fa0/13	Desg	BLK	19	Pol	Root	FWD	7
		Fa0/15	Desg	BLK	19	Fa0/13	Desg	FWD	19
		Fa0/8	Altn	BLK	19	Fa0/15	Desg	FWD	19
		Fa0/14	Desg	BLK	19	Fa0/14	Desg	FWD	19
		Fa0/16	Desg	BLK	19	Fa0/16	Desg	FWD	19
Switch Bat B	Fa0/1	Fa0/1	Root	FWD	19	Fa0/8	Altn	BLK	19
		Fa0/8	Altn	BLK	19	Pol	Root	FWD	7
		Pol	Desg	FWD	7	Fa0/15	Desg	BLK	19
		Fa0/15	Desg	FWD	19	Fa0/14	Desg	BLK	19
		Fa0/14	Desg	FWD	19	Fa0/13	Desg	BLK	19
		Fa0/13	Desg	FWD	19	Fa0/16	Desg	BLK	19
		Fa0/16	Desg	FWD	19				
Switch Bat B	Fa0/1 et Fa0/16	Fa0/8	Altn	BLK	19	Fa0/8	Altn	BLK	19
		Pol	Root	FWD	7	Pol	Root	FWD	7
		Fa0/15	Desg	BLK	19	Fa0/15	Desg	BLK	19
		Fa0/14	Desg	BLK	19	Fa0/14	Desg	BLK	19
		Fa0/13	Desg	BLK	19	Fa0/13	Desg	BLK	19
		Fa0/16	Desg	BLK	19				
Switch DMZ	Fa0/3	Fa0/3	Root	FWD	19	Fa0/4	Desg	FWD	19
		Fa0/4	Desg	FWD	19	Fa0/5	Root	FWD	19
		Fa0/5	Desg	FWD	19				
Switch Srv	Fa0/3	Fa0/4	Altn	BLK	19	Fa0/4	Root	FWD	19
		Fa0/3	Root	FWD	19				

Figure 106 : Tableau des tests

Bilan

Nous pouvons constater que la redirection fonctionne sur les switches. Or, je pense qu'il y a un problème sur l'Etherchannel car lorsque je fais un shutdown sur l'un des ports le composant, le Port-Channel 1 n'a plus l'air de fonctionner. Je ne vois pas spécialement pourquoi car il a justement été créé dans le but de pallier à ce problème. Cela est sûrement dû à une mauvaise configuration de l'Etherchannel mais après avoir refait la manipulation je ne sais pas où. Le spanning tree est donc opérationnel, hormis lors des tests sur les ports constituant l'Etherchannel à savoir du port fa0/13 à fa0/16.

Mission 8 : tolérance aux pannes des routeurs

Cette mission a comme objectif la tolérance aux pannes de nos routeurs. Cette configuration doit se faire via HSRP ou GLBP.

Mais qu'est-ce que le HSRP ?

HSRP pour Hot Standby Router Protocol est un protocole propriétaire à Cisco présent sur les routeurs et switch de couche 3 permettant une continuité de service si l'un d'eux venait à tomber en panne pour X raisons. Celui-ci permet d'assurer la disponibilité de la passerelle d'un réseau via une IP configurée sur deux routeurs ou switch L3 différents.

Et qu'en est-il du GLBP ?

GLBP pour Gateway Load Balancing Protocol est aussi un protocole propriétaire Cisco. Celui-ci permet la redondance du matériel et la répartition de charge sur plusieurs routeurs en n'utilisant qu'une seule IP virtuelle associée donc à plusieurs adresses MAC.

Tâche 1

Le but est donc de mettre en place le protocole HSRP sur nos switch L3 qui font office de routeur inter-vlan. Pour cela nous devons tout d'abord configurer un autre switch de couche 3 qui permettra de créer une redondance. Nous devons lui mettre des adresses de passerelle différentes. Mes adresses étant en .254 sur le switch L3 numéro 1, j'ai choisi de les mettre en .154 sur le deuxième. Enfin, pour les adresses virtuelles, celles-ci seront en .54.

Pour mettre en place le HSRP, nous devons faire les commandes suivantes sur le switch I3 numéro 1 :

```
enable
configure terminal
interface vlan 2
standby 2 ip 172.17.2.54
standby 2 priority 150 #met la priorité sur cet appareil
standby 2 preempt #cet appareil initiera la connexion
exit
ip routing
write
```

Pour notre deuxième commutateur de couche 3 :

```
enable
configure terminal
interface vlan 2
standby 2 ip 172.17.2.54
exit
ip routing
write
```

Nous pouvons ensuite vérifier que tous nos vlan et leurs passerelles ont été configurés via la commande :

```
enable
show standby brief
```

Switch Coeur 1

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Enter configuration commands, one per line. End with CNTL/Z.
Switchcoeur(config)#hostname "Switchcoeur 1"
% Spaces are not allowed in hostname
Switchcoeur(config)#
Switchcoeur(config)#hostname "Switchcoeur 1"
% Spaces are not allowed in hostname
Switchcoeur(config)#Switchcoeur(config)#
Switchcoeur(config)#hostname Switchcoeur2
Switchcoeur2(config)#
Switchcoeur2(config)#hostname Switchcoeur1
Switchcoeur1(config)#
Switchcoeur1(config)##% Bad secrets

Switchcoeur1(config)#ex
Switchcoeur1#
*Mar 20, 21:32:52.3232: SYS-5-CONFIG_I: Configured from console by console
Switchcoeur1#show stan
Switchcoeur1#show standby bri
Switchcoeur1#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri  P State    Active      Standby           Virtual IP
V11        1    150  P Active   local       192.168.1.154  192.168.1.54
V12        2    150  P Active   local       172.17.2.154  172.17.2.54
V13        3    100  Standby  172.17.3.154 local       172.17.3.54
V14        4    100  Active   local       172.17.4.154  172.17.4.54
V15        5    100  Active   local       172.17.5.154  172.17.5.54
V112       12   100  Active   local       172.16.12.154 172.16.12.54
V122       22   100  Active   local       192.168.22.154 192.168.22.54
V132       32   100  Active   local       172.16.32.154 172.16.32.54
V152       52   100  Standby  10.2.0.154 local       10.2.0.54
V172       72   100  Active   local       192.168.72.154 192.168.72.54
V182       82   100  Active   local       10.0.82.154   10.0.82.54
V199       99   100  Active   local       192.168.2.154  192.168.2.54

```

Résultat de la commande 1

Switch Coeur 2

Physical Config **CLI** Attributes

IOS Command Line Interface

```

V172      72  100  Standby  192.168.72.254  local          192.168.72.54
V182      82  100  Standby  10.0.82.254    local          10.0.82.54
V199      99  100  Standby  192.168.2.254  local          192.168.2.54
Switchcoeur#Switchcoeur#
Switchcoeur#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switchcoeur(config)#
Switchcoeur(config)#hostname "Switchcoeur 2"
% Spaces are not allowed in hostname
Switchcoeur(config)#
Switchcoeur(config)#hostname Switchcoeur2
Switchcoeur2(config)#
Switchcoeur2(config)#Switchcoeur2(config)#
Switchcoeur2(config)#show stand
Switchcoeur2(config)#ex
Switchcoeur2#
*Mar 20, 21:33:22.3333: SYS-5-CONFIG_I: Configured from console by console
Switchcoeur2#show stand
Switchcoeur2#show standby brief
    P indicates configured to preempt.
    |
Interface  Grp  Pri P State   Active           Standby        Virtual IP
V11        1    100  Standby  192.168.1.254  local          192.168.1.54
V12        2    100  Standby  172.17.2.254  local          172.17.2.54
V13        3    100  Active   local            172.17.3.254  172.17.3.54
V14        4    100  Standby  172.17.4.254  local          172.17.4.54
V15        5    100  Standby  172.17.5.254  local          172.17.5.54
V112       12   100  Standby  172.16.12.254 local          172.16.12.54
V122       22   100  Standby  192.168.22.254 local          192.168.22.54
V132       32   100  Standby  172.16.32.254 local          172.16.32.54
V152       52   100  Active   local          10.2.0.254    10.2.0.54
V172       72  100  Standby  192.168.72.254  local          192.168.72.54
V182       82  100  Standby  10.0.82.254    local          10.0.82.54
V199       99  100  Standby  192.168.2.254  local          192.168.2.54
Switchcoeur2#

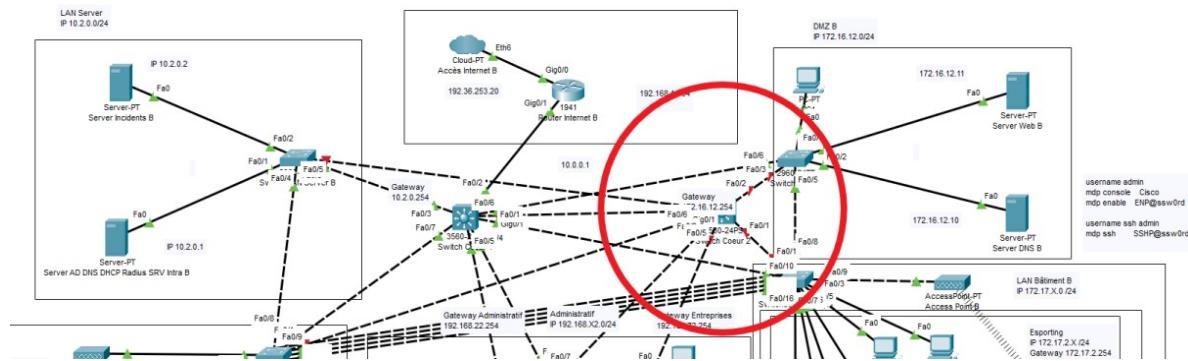
```

Résultat de la commande 2

Nous devons faire ces commandes sur tous nos vlan, de plus nous devons modifier nos pool dhcp pour que la passerelle soit celle en .54, sinon les appareils ne pourront plus communiquer. Une fois ces deux choses faites nous pouvons passer au test.

Tâche 2

Cette tâche finale consiste au test de la solution apportée. Nous devons pour cela simuler la panne d'un routeur. Pour cela je vais faire un shutdown sur les interfaces du switch I3 n°2, de façon à ce qu'aucun port ne soit opérationnel. Une fois cela fait je vais procéder à des tests de ping entre différents VLAN. Etant donné que nos ordinateurs et appareils ont une passerelle en .54, et que notre switch à une IP en .254 alors, si HSRP était mal paramétré aucune machine ne pourrait dialoguer.



Shutdown des interfaces

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

  Connection-specific DNS Suffix...:
  Link-local IPv6 Address..... FE80::2D0:97FF:FEA3:BB58
  IPv6 Address..... :: :
  IPv4 Address..... 172.17.2.4
  Subnet Mask..... 255.255.255.0
  Default Gateway..... :: :
                           172.17.2.54

Bluetooth Connection:

  Connection-specific DNS Suffix...:
  Link-local IPv6 Address..... :: :
  IPv6 Address..... :: :
  IPv4 Address..... 0.0.0.0
  Subnet Mask..... 0.0.0.0
  Default Gateway..... :: :
                           0.0.0.0

C:\>ping 172.17.4.3

Pinging 172.17.4.3 with 32 bytes of data:

Request timed out.
Reply from 172.17.4.3: bytes=32 time<1ms TTL=127
Reply from 172.17.4.3: bytes=32 time<1ms TTL=127
Reply from 172.17.4.3: bytes=32 time<1ms TTL=127

Ping statistics for 172.17.4.3:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping 1

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

  Connection-specific DNS Suffix...:
  Link-local IPv6 Address.....: FE80::2D0:58FF:FE03:13C4
  IPv6 Address.....: ::1
  IPv4 Address.....: 172.17.4.3
  Subnet Mask.....: 255.255.255.0
  Default Gateway.....: ::1
                                172.17.4.54

Bluetooth Connection:

  Connection-specific DNS Suffix...:
  Link-local IPv6 Address.....: ::1
  IPv6 Address.....: ::1
  IPv4 Address.....: 0.0.0.0
  Subnet Mask.....: 0.0.0.0
  Default Gateway.....: ::1
                                0.0.0.0

C:\>ping 172.17.2.2

Pinging 172.17.2.2 with 32 bytes of data:

Reply from 172.17.2.2: bytes=32 time<1ms TTL=127
Reply from 172.17.2.2: bytes=32 time<1ms TTL=127
Reply from 172.17.2.2: bytes=32 time=1ms TTL=127
Reply from 172.17.2.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.17.2.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ping 2

```
C:\>ipconfig

Wireless0 Connection: (default port)

  Connection-specific DNS Suffix...:
  Link-local IPv6 Address.....: FE80::2E0:F9FF:FE13:253A
  IPv6 Address.....: ::1
  IPv4 Address.....: 10.0.82.6
  Subnet Mask.....: 255.255.255.0
  Default Gateway.....: ::1
                                10.0.82.54

Bluetooth Connection:

  Connection-specific DNS Suffix...:
  Link-local IPv6 Address.....: ::1
  IPv6 Address.....: ::1
  IPv4 Address.....: 0.0.0.0
  Subnet Mask.....: 0.0.0.0
  Default Gateway.....: ::1
                                0.0.0.0

C:\>ping 192.168.22.6

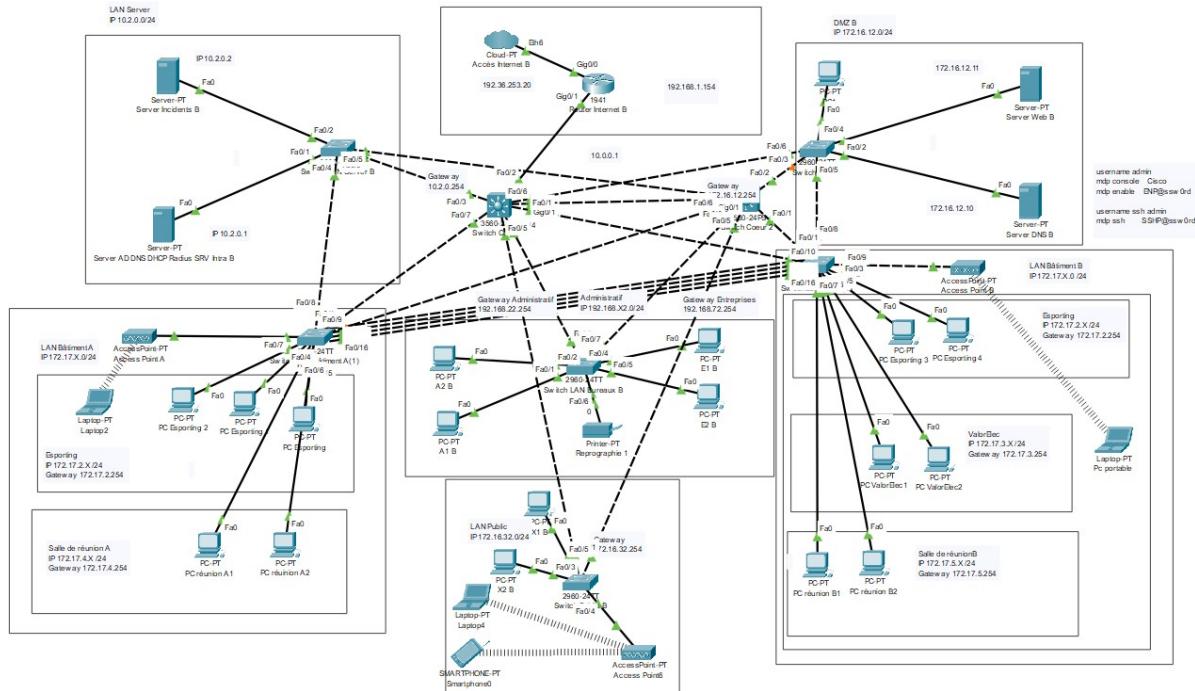
Pinging 192.168.22.6 with 32 bytes of data:

Reply from 192.168.22.6: bytes=32 time=58ms TTL=127
Reply from 192.168.22.6: bytes=32 time=5ms TTL=127
Reply from 192.168.22.6: bytes=32 time=26ms TTL=127
Reply from 192.168.22.6: bytes=32 time=25ms TTL=127

Ping statistics for 192.168.22.6:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 58ms, Average = 28ms
```

Ping 3

Les tests ne seront pas exhaustifs puisque le nombre d'appareils est trop important. Nous pouvons le constater via le dernier G de la maquette.



Bilan

Cet atelier m'a été bénéfique, j'ai pu approfondir mes connaissances dans le réseau en alliant théorie et pratique. Les protocoles et services mis en place n'étaient pas forcément tous très facile à prendre ou reprendre en main. Néanmoins cela m'a permis de revoir des notions que j'avais étudié pendant mon cursus, me permettant d'améliorer mes compétences tout en respectant les contraintes des différentes missions et tâches données.

Sources

Spanning Tree: [*Commandes Explications*](#)

Etherchannel: [*Commandes Explication*](#)

HSRP VLAN: [*Commandes*](#)