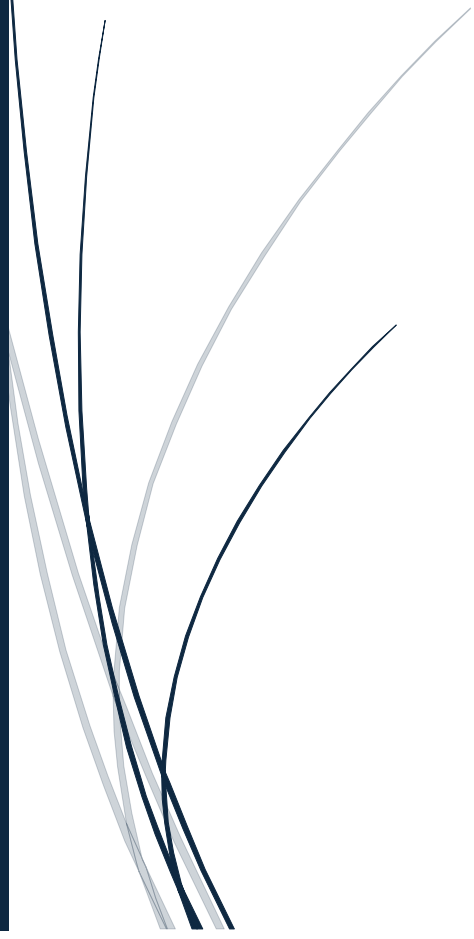
04/01/2025

TP Commutateurs

BTS SIO SISR 2e année

Kyllian Aucher

Anne-Lou Delage-Davies



ST-JO SUP

Table des matières

Introduction 2
Objectif 2
Matériel et logiciels utilisés 2
Prérequis techniques 3
1. Configuration des commutateurs 3
1.1 Connexion aux commutateurs 3
1.2 Configuration initiale 3
2. Configuration et tests des VLAN 3
2.1 Test sur commutateurs HP, Cisco et Alcatel 3
Tests réalisés : 4
3. Mise en place de SSH 4
Configuration et tests 4
4. Transfert des configurations par TFTP 4
Procédure : 4
5. Configuration avancée des ports 5
Sécurité 5
Performance 5
6. Agrégation et STP 5
Agrégation 5
STP (Spanning Tree Protocol) 5
7. Gestion du temps, des journaux et du monitoring 6
NTP (Network Time Protocol) 6
Logs 6
SNMP (Simple Network Management Protocol) 6
Conclusion 6
Tableau récapitulatif 6
Questions 9
3.1 Configuration et test VLAN commutateur HP : 9
3.2 Configuration et test VLAN commutateur Cisco : 10
3.3 Configuration et test VLAN commutateur Alcatel : 10
3.4 Configuration et test VLAN commutateurs HP Cisco : 11
3.5 Configuration et test VLAN commutateurs HP Cisco Alcatel : 12
4 Mise en place SSH : 12

Introduction

Ce TP sur les commutateurs vise à mettre en pratique les notions essentielles de configuration et de sécurisation des équipements réseau. L'objectif principal est de configurer différents types de commutateurs (HP, Cisco, et Alcatel) conformément aux recommandations de l'ANSSI, tout en explorant des concepts clés tels que la segmentation par VLAN, la sécurisation des ports, et l'administration à distance via SSH.

Le travail réalisé permet de consolider des compétences en administration réseau, notamment à travers la mise en place de VLAN pour la segmentation du trafic, le transfert et la sauvegarde de configurations via TFTP, ainsi que l'activation de protocoles comme STP, NTP, et SNMP pour garantir la résilience et la supervision du réseau. Ce rapport détaille les étapes suivies, les tests effectués, et les résultats obtenus pour valider les configurations.

Objectif

L’objectif principal de ce TP est de mettre en place une infrastructure réseau segmentée en utilisant des commutateurs de marques HP, Cisco et Alcatel. Cette configuration doit respecter les préconisations de l’ANSSI (Agence Nationale de la Sécurité des Systèmes d’Information), qui imposent des mesures strictes pour la sécurisation des infrastructures réseaux. Les principales tâches incluent la création de VLAN, la configuration des ports, la mise en place de sécurité et de fonctionnalités avancées (SSH, agrégation de liens, STP), ainsi que la gestion des journaux et des sauvegardes de configuration.

Matériel et logiciels utilisés

Matériel :

- 1 commutateur HP Procurve 2524.
- 1 commutateur Cisco modèle Catalyst 2960-X series.
- 1 commutateur Alcatel modèle OS6250-P24.
- Câbles Ethernet RJ45 pour les connexions réseau.
- Ordinateur avec ports série.

Logiciels :

- **Putty** pour la connexion SSH et console
- **TFTPD32** (transfert de configuration via TFTP)
- Documentation ANSSI sur la sécurisation des commutateurs.

Prérequis techniques

1. Remise à l'état d'usine des commutateurs pour garantir un environnement de travail propre.
2. Configuration initiale par le port console.
3. Transition vers une configuration distante via SSH après avoir défini les paramètres de base.
4. Connaissance des commandes spécifiques à chaque fabricant.

---

1. Configuration des commutateurs

1.1 Connexion aux commutateurs

Les configurations initiales ont été réalisées via un accès console. Cet accès direct permet de travailler sur les commutateurs, même sans réseau configuré. Une fois les paramètres de base configurés, la connexion par SSH a été mise en place pour renforcer la sécurité des communications administratives. SSH, qui offre un chiffrement des données, constitue une alternative sûre à l'utilisation d'outils comme Telnet.

Intérêt :

- L'accès console est indispensable pour les configurations initiales ou les récupérations en cas de panne.
- SSH offre une connexion chiffrée, réduisant les risques d'interception de données sensibles, surtout lors des communications distantes sur des réseaux non sécurisés.

1.2 Configuration initiale

Les actions suivantes ont été effectuées :

- Remise des commutateurs en configuration usine pour garantir un environnement propre.
- Attribution d'un nom et d'un prompt adapté au rôle de chaque commutateur.
- Configuration des VLAN d'administration (VLAN 100).
- Suppression des services inutiles pour réduire la surface d'attaque et minimiser les risques de compromission.

---

2. Configuration et tests des VLAN

2.1 Test sur commutateurs HP, Cisco et Alcatel

Chaque commutateur a été configuré avec des VLAN distincts :

- VLAN 10 pour la direction.
- VLAN 20 pour l'atelier.
- VLAN 30 pour la téléphonie IP.
- VLAN 40 pour la visioconférence.
- VLAN 100 pour l'administration.

Tests réalisés :

1. Les postes connectés au même VLAN (direction ou atelier) doivent pouvoir communiquer entre eux. Cela a été vérifié via des tests de ping.
2. Lorsqu'un poste est déplacé dans un autre VLAN, la communication est bloquée par défaut, comme attendu.

Intérêt : L'isolation des réseaux réduit les risques de propagation de cyberattaques ou de problèmes de performance. Les VLAN permettent également de segmenter efficacement les ressources réseau selon les besoins organisationnels.

---

3. Mise en place de SSH

Configuration et tests

Le protocole SSH a été activé sur les commutateurs HP et Cisco en suivant les commandes fournies. Les postes administratifs ont été configurés pour accéder aux commutateurs via SSH sur le VLAN d'administration. Une attention particulière a été portée à la sécurisation des mots de passe et à la restriction des accès pour éviter toute intrusion non autorisée.

Intérêt : L'utilisation de SSH augmente la sécurité en évitant les communications non chiffrées et en limitant les accès au réseau d'administration. Cela protège les configurations sensibles des attaques potentielles.

---

4. Transfert des configurations par TFTP

L'outil TFTP a été utilisé pour sauvegarder et restaurer les configurations des commutateurs.

Procédure :

1. Sauvegarde des configurations des trois commutateurs via SSH.
2. Restauration après remise à l'état usine, avec transfert des fichiers de configuration sauvegardés depuis le serveur TFTP.

Intérêt : Cette pratique permet de réduire le temps de récupération en cas de panne ou d'incident. Elle assure une reprise rapide des services et minimise les interruptions en cas de problème majeur.

---

5. Configuration avancée des ports

Sécurité

- La fonction port security a été activée pour limiter l'accès aux seuls appareils autorisés par leur adresse MAC.
- Des tests ont confirmé que les ports refusaient les appareils non autorisés ou à adresse MAC multiple (au-delà de la limite).

Performance

- La vitesse des ports a été fixée à 100 Mb/s en mode full-duplex pour garantir une performance optimale.

Intérêt : Ces paramètres renforcent à la fois la sécurité et la stabilité du réseau. En ajustant les performances des ports, on garantit une transmission fluide des données, tout en maintenant un contrôle rigoureux sur les connexions.

---

6. Agrégation et STP

Agrégation

Les ports 23 et 24 ont été regroupés pour créer une agrégation, augmentant ainsi la bande passante et la redondance. Ce regroupement permet de maximiser les ressources disponibles pour des liens critiques.

STP (Spanning Tree Protocol)

STP a été activé pour prévenir les boucles réseau potentielles en établissant une topologie sans cycle. Cette fonctionnalité évite les interruptions causées par des réseaux mal configurés ou surchargés.

Intérêt : Ces fonctions sont essentielles pour des réseaux étendus et redondants, offrant une résistance aux pannes et une gestion optimisée des ressources.

---

7. Gestion du temps, des journaux et du monitoring

NTP (Network Time Protocol)

Les commutateurs ont été configurés pour synchroniser leur horloge avec le serveur NTP 192.168.10.250, garantissant un horodatage cohérent des journaux.

Logs

Les journaux des commutateurs sont centralisés sur un serveur à la même adresse IP pour une meilleure traçabilité et une analyse simplifiée des événements.

SNMP (Simple Network Management Protocol)

SNMP a été configuré pour permettre la collecte d'informations et la surveillance des commutateurs via un serveur spécifique (192.168.10.25).

Intérêt : Ces outils garantissent une gestion proactive, permettant d'identifier rapidement les problèmes et d'optimiser les performances du réseau en temps réel.

Conclusion

Ce TP met en pratique les principes fondamentaux de la gestion réseau : segmentation, sécurité, résilience et monitoring. Chaque fonctionnalité contribue à créer un réseau robuste, conforme aux préconisations de l'ANSSI. Les tests réalisés ont validé les configurations, et les procédures documentées permettent une reproductibilité facile pour de futurs projets. En résumé, ce TP constitue une base essentielle pour comprendre les principes avancés d'administration réseau tout en renforçant les compétences techniques nécessaires à une gestion optimisée des infrastructures modernes.

Tableau récapitulatif

Action	**Cisco**	**HP (ProCurve)**	**Alcatel**
Nom du switch	#hostname <nom>	#hostname <nom>	# system name <nom>
Enregistrer modifications	#copy r st	#wr mem	#write memory #copy working certified

Action	**Cisco**	**HP (ProCurve)**	**Alcatel**
Interfaces (vitesse, état)	#show interfaces	#show interfaces brief	show interfaces
Activités sur les ports	#show interfaces counters	#show statistics	#show interfaces
Détail interface	#show interfaces <port>	#show interfaces <port>	#show interfaces <port>
Utilisateur admin	# username admin privilege 15 password securepassword	#password manager user-name admin	#user administrateur password nouveaumotdepasse read-write all
Agrégation	#interface <port> #channel-group 1 mode on #switchport mode trunk #interface Port-Channel1 switchport mode trunk #switchport trunk allowed vlan <numéro>	# trunk 23-24 trk1 trunk # trunk 23-24 trk1 lacp active # vlan 10 # tagged trk1	#static linkagg 1 size <nb liens> #static agg <port> agg num 1 #vlan <numéro> 802.1Q 1
Vérification agréga	# show etherchannel summary # show interfaces etherchannel	# show trunks # show lacp	
Supprimer conf	#write erase	#erase startup-config	#rm /flash/working/boot.cfg #rm /flash/certified/boot.cfg
Sauvegarde conf tftp	#copy running-config tftp	#copy running-config tftp <@IP_DU_SERVEUR> maconfigswitch.txt	#tftp <@IP_DU_SERVEUR> put source-file /flash/working/boot.cfg destination-file cfg.cfg
SSH (taguer VLAN Admin)	#username cisco privilege 15 secret cisco #ip domain-name cisco.com #crypto key generate rsa #ip ssh version 2 #line vty 0 15	#crypto key generate ssh #ip ssh #password manager #aaa authentication ssh login public-key local	#ssh enable

Action	**Cisco**	**HP (ProCurve)**	**Alcatel**
	#login local #transport input ssh		
Commentaires	#interface <port> #description <...>	#interface <port> ou vlan <id> #name "<...>"	#interfaces <port> alias <...>
Copie conf TFTP	#copy tftp running-config (ou startup-config)	#copy tftp startup-config <@IP_DU_SERVEUR> maconfig.txt	# tftp <@IP_DU_SERVEUR> get source-file cfg.cfg destination-file /flash/working/boot.cfg
Config vitesse, mode connexion	#interface <port> #speed <vitesse> #duplex <full-auto>	#interface <port> #speed-duplex <vitesse>-full	#interfaces <port> speed <vitesse> #interfaces <port> duplex full
NTP	#ntp server <@IP_DU_SERVEUR>	#ntp enable #ntp server <@IP_DU_SERVEUR>	#ntp server <@IP_DU_SERVEUR> #ntp client enable
Verif NTP	#show ntp status	#show ntp status	#show ntp client #show ntp server_list
Logs	#logging host <@IP_SERVEUR_SYSLOG> #logging trap warnings #service timestamps log datetime msec #show logging	#logging <@IP_SERVEUR_SYSLOG> #logging facility local1 #show logging	#swlog output socket <@IP_SERVEUR_SYSLOG>
SNMP	#snmp-server group MONITORING v3 auth #snmp-server user admin MONITORING v3 auth sha MyAuthPassword priv aes 128 MyPrivPassword #snmp-server host 192.168.10.25 version 3 auth admin	#snmpv3 enable #snmpv3 group MONITORING #snmpv3 user admin group MONITORING auth sha MyAuthPassword priv aes MyPrivPassword #snmpv3 targetaddress TARGET 192.168.10.25	#user <username> read-only <snmp> ou <all> password <PASSWORD> #snmp security no security

Action	**Cisco**	**HP (ProCurve)**	**Alcatel**
PoE	Incompatible	Incompatible	#interface <port> #poe enable

Questions

3.1 Configuration et test VLAN commutateur HP :

1. **Le ping entre les 2 postes direction fonctionne-t-il ? Pourquoi ?**

   Oui, le ping entre les deux postes direction (192.168.1.1 et 192.168.1.2) devrait fonctionner. Les deux postes sont connectés aux ports 1 et 2 du commutateur, qui sont configurés dans le même VLAN (VLAN Direction). Les VLANs agissent comme des réseaux locaux virtuels. Les postes appartenant au même VLAN peuvent communiquer directement entre eux.

2. **Que se passe-t-il si on déplace l'un des postes direction dans le VLAN atelier ? Pourquoi ?**

   Le ping entre le poste resté dans le VLAN direction et le poste déplacé dans le VLAN atelier ne fonctionnera plus. En déplaçant un poste dans le VLAN atelier, on le place dans un réseau logique différent. Les VLANs isolent le trafic. Par défaut, les postes appartenant à des VLANs différents ne peuvent pas communiquer sans un routeur (ou une fonctionnalité de routage inter-VLAN sur le commutateur).

3. **Que se passe-t-il si on déplace les deux postes direction dans le VLAN atelier ? Pourquoi ?**

   Le ping entre les deux postes direction fonctionnera à nouveau, mais ils ne pourront plus communiquer avec les appareils restés dans le VLAN direction initial. Ils pourront communiquer avec les postes du VLAN atelier. En déplaçant les deux postes dans le VLAN atelier, ils se retrouvent à nouveau dans le même réseau logique. Ils peuvent donc communiquer entre eux. Cependant, ils sont désormais isolés du VLAN direction initial.

3.2 Configuration et test VLAN commutateur Cisco :

1. **Le ping entre les 2 postes direction fonctionne-t-il ? Pourquoi ?**

   Oui, le ping entre les deux postes direction (192.168.1.1 et 192.168.1.2) devrait fonctionner. Les deux postes sont connectés aux ports 1 et 2 du commutateur, qui sont configurés dans le même VLAN (VLAN Direction). Les VLANs agissent comme des réseaux locaux virtuels. Les postes appartenant au même VLAN peuvent communiquer directement entre eux.

2. **Que se passe-t-il si on déplace l'un des postes direction dans le VLAN atelier ? Pourquoi ?**

   Le ping entre le poste resté dans le VLAN direction et le poste déplacé dans le VLAN atelier ne fonctionnera plus. En déplaçant un poste dans le VLAN atelier, on le place dans un réseau logique différent. Les VLANs isolent le trafic. Par défaut, les postes appartenant à des VLANs différents ne peuvent pas communiquer sans un routeur (ou une fonctionnalité de routage inter-VLAN sur le commutateur).

3. **Que se passe-t-il si on déplace les deux postes direction dans le VLAN atelier ? Pourquoi ?**

   Le ping entre les deux postes direction fonctionnera à nouveau, mais ils ne pourront plus communiquer avec les appareils restés dans le VLAN direction initial. Ils pourront communiquer avec les postes du VLAN atelier. En déplaçant les deux postes dans le VLAN atelier, ils se retrouvent à nouveau dans le même réseau logique. Ils peuvent donc communiquer entre eux. Cependant, ils sont désormais isolés du VLAN direction initial.

3.3 Configuration et test VLAN commutateur Alcatel :

1. **Le ping entre les 2 postes direction fonctionne-t-il ? Pourquoi ?**

   Oui, le ping entre les deux postes direction (192.168.1.1 et 192.168.1.2) devrait fonctionner. Les deux postes sont connectés aux ports 1 et 2 du commutateur, qui sont configurés dans le même VLAN (VLAN Direction). Les VLANs créent des réseaux locaux virtuels, et les appareils dans le même VLAN peuvent communiquer directement.

2. **Que se passe-t-il si on déplace l'un des postes direction dans le VLAN atelier ? Pourquoi ?**

   Le ping entre le poste resté dans le VLAN direction et le poste déplacé dans le VLAN atelier ne fonctionnera plus. Les VLANs isolent le trafic. Déplacer un poste dans un autre VLAN le place dans un réseau logique différent. Sans routage inter-VLAN, la communication entre les VLANs est impossible.

3. **Que se passe-t-il si on déplace les deux postes direction dans le VLAN atelier ? Pourquoi ?**

   Le ping entre les deux postes direction fonctionnera à nouveau, mais ils ne pourront plus communiquer avec les appareils restés dans le VLAN direction initial. Ils pourront communiquer avec les postes du VLAN atelier. En étant tous les deux dans le VLAN atelier, ils partagent le même domaine de diffusion (broadcast domain) et peuvent donc communiquer. Ils sont cependant isolés du VLAN direction.

3.4 Configuration et test VLAN commutateurs HP Cisco :

1. **Le ping entre les 2 postes direction fonctionne-t-il ? Pourquoi ?**

   Dans la configuration initiale (où seul le VLAN Direction est configuré sur les ports 1 et la liaison inter-switch), le ping *ne fonctionnera pas* initialement. Bien que les postes soient dans le même VLAN (Direction), les commutateurs ne savent pas comment transférer le trafic entre eux pour ce VLAN. Il faut configurer une liaison inter-switch (trunk) pour autoriser le passage du VLAN Direction.

2. **Que se passe-t-il si on déplace l'un des postes dans le VLAN atelier ? Pourquoi ?**

   Si on déplace un poste direction vers le VLAN atelier, il ne pourra plus communiquer ni avec les autres postes direction, ni avec les postes atelier de l'autre commutateur tant que le trunk n'est pas configuré pour le VLAN atelier. Une fois le trunk configuré pour le VLAN atelier, il ne pourra plus communiquer avec les postes direction, mais il pourra communiquer avec les autres postes atelier. Cela illustre l'isolation des VLANs. Sans configuration supplémentaire (trunk pour le VLAN atelier), les VLANs ne communiquent pas entre les commutateurs.

3. **Que se passe-t-il si on déplace les 2 postes dans le VLAN atelier de chaque switch ? Pourquoi ?**

   Initialement, sans configuration du trunk pour le VLAN atelier, les postes atelier de chaque commutateur ne pourront pas communiquer entre eux. Une fois le trunk configuré pour le VLAN atelier, ils pourront communiquer. Même raisonnement que précédemment. Le trunk est indispensable pour la communication inter-VLAN entre les commutateurs.

4. **Modifiez les configurations pour que les pings des 2 postes dans le VLAN atelier fonctionnent ?**

   Il faut configurer un trunk (liaison inter-switch) sur les ports 24 des deux commutateurs et autoriser le VLAN Atelier sur ce trunk.

3.5 Configuration et test VLAN commutateurs HP Cisco Alcatel :

1. **Le ping entre les 3 postes direction fonctionne-t-il ? Pourquoi ?**

   Dans la configuration initiale (où seul le VLAN Direction est configuré sur les ports 1 et les liaisons inter-switch), le ping *ne fonctionnera pas* initialement. Bien que les postes soient dans le même VLAN (Direction), les commutateurs ne savent pas comment transférer le trafic entre eux pour ce VLAN. Il faut configurer des trunks (liaisons inter-switch) pour autoriser le passage du VLAN Direction entre les trois commutateurs.

2. **Que se passe-t-il si on déplace l'un des postes dans le VLAN atelier ? Pourquoi ?**

   Si on déplace un poste direction vers le VLAN atelier, il ne pourra plus communiquer ni avec les autres postes direction, ni avec les postes atelier tant que les trunks ne sont pas configurés pour le VLAN atelier. Une fois les trunks configurés pour le VLAN atelier, il ne pourra plus communiquer avec les postes direction, mais il pourra communiquer avec les autres postes atelier. Cela illustre l'isolation des VLANs. Sans configuration supplémentaire (trunks pour le VLAN atelier), les VLANs ne communiquent pas entre les commutateurs.

3. **Que se passe-t-il si on déplace les 3 postes dans le VLAN atelier de chaque switch ? Pourquoi ?**

   Initialement, sans configuration des trunks pour le VLAN atelier, les postes atelier de chaque commutateur ne pourront pas communiquer entre eux. Une fois les trunks configurés pour le VLAN atelier, ils pourront communiquer. Même raisonnement que précédemment. Les trunks sont indispensables pour la communication inter-VLAN entre les commutateurs.

4. **Modifiez les configurations pour que les ping des 3 postes dans le VLAN atelier fonctionnent ?**

   Il faut configurer des trunks (liaisons inter-switch) sur les ports 24 des trois commutateurs et autoriser le VLAN Atelier sur ces trunks.

4 Mise en place SSH :

1. **Sur quel VLAN devez-vous configurer le port pour connecter le poste ?**

   Idéalement, le port sur lequel vous connectez votre poste pour accéder en SSH aux commutateurs devrait être configuré dans un VLAN de management dédié. Ce VLAN est séparé des VLANs utilisateurs (comme les VLANs Direction et Atelier des exercices précédents) pour des raisons de sécurité. Si vous n'avez pas de VLAN de management dédié, vous pouvez utiliser un VLAN existant, mais assurez-vous qu'il n'est pas utilisé par des équipements sensibles. Dans

le contexte des exercices précédents, le VLAN Atelier pourrait être utilisé temporairement pour les tests, mais ce n'est pas une bonne pratique en production.

2. **Le port sera en tagged ou untagged pour HP ? Pour Cisco indiquer le type de port.**

HP : Le port sera en mode *untagged* (ou *access* dans certaines versions de firmware HP) si vous connectez directement un PC. Le PC ne comprend pas les trames taguées 802.1Q. Si vous connectez un autre commutateur, le port sera en mode *tagged* (ou *trunk*).

Cisco : Le port sera configuré en mode *access* si vous connectez un PC. Si vous connectez un autre commutateur, le port sera configuré en mode *trunk*.

3. **Que devez-vous faire au niveau de la configuration réseau du poste ?**

Le poste doit avoir une adresse IP dans le même sous-réseau que l'interface VLAN du commutateur que vous essayez d'atteindre en SSH. Par exemple : Si l'interface VLAN du commutateur a l'adresse 192.168.10.254/24, le poste doit avoir une adresse comme 192.168.10.10/24 avec un masque de sous-réseau 255.255.255.0 et une passerelle par défaut (optionnelle, mais recommandée) pointant vers l'adresse de l'interface VLAN (192.168.10.254 dans cet exemple).

4. **Pouvez-vous vous connecter en SSH sur le HP ?**

Oui, après avoir configuré SSH sur le commutateur HP et configuré correctement l'adresse IP du poste et son port sur le bon VLAN, vous devriez pouvoir vous connecter en SSH en utilisant Putty.

5. **En laissant le poste relié sur le port 22 du commutateur HP, pouvez-vous vous connectez en SSH sur le Cisco ?**

Non, ce n'est pas possible directement. Le poste est connecté au réseau du commutateur HP. Pour atteindre le commutateur Cisco en SSH, il faut que :

- Les deux commutateurs soient connectés entre eux via un trunk (comme dans les exercices précédents avec le port 24).
- Le VLAN de management (ou le VLAN utilisé pour SSH) soit autorisé sur ce trunk.
- Le commutateur Cisco ait une interface VLAN avec une adresse IP dans le même sous-réseau que le poste.