BTS SIO — Option SISR

PROJET

VLAN et routage inter-VLAN

sur Cisco

Segmentation, routage L3, DHCP centralisé et ACL de sécurité

Sasiraj GUNARATNARAJAH

Étudiant BTS SIO SISR — 2e année

CNED / F2I — Saint-Gobain Digital & IT

Session 2025

Sommaire

Sommaire 2
1. Contexte et objectifs du projet 4
1.1 Contexte 4
1.2 Objectifs 4
1.3 Cas d'usage simulé 4
2. Principe des VLAN et du routage inter-VLAN 5
2.1 Qu'est-ce qu'un VLAN ? 5
2.2 Le tagging 802.1Q 5
2.3 Routage inter-VLAN par SVI 5
3. Architecture retenue 7
3.1 Schéma logique 7
3.2 Équipements 7
4. Plan d'adressage IP 8
5. Mise en œuvre — Topologie physique 9
5.1 Mise en place des équipements 9
5.2 Câblage 9
5.3 Alimentation du Switch L3 10
6. Mise en œuvre — Configuration des VLAN 12
6.1 Création des VLAN sur SW-CORE 12
6.2 Vérification 12
6.3 Création des VLAN sur les switches d'accès 13
7. Mise en œuvre — Trunks 802.1Q 14
7.1 Principe 14
7.2 Configuration sur SW-CORE 14
7.3 Configuration sur les switches d'accès 15
7.4 Vérification 15
8. Mise en œuvre — Routage inter-VLAN (SVI) 17
8.1 Activation du routage IP 17
8.2 Création des SVI 17
8.3 Sauvegarde de la configuration 17
8.4 Vérification 18
9. Mise en œuvre — Ports d'accès 20
9.1 Principe 20
9.2 Configuration sur SW-COMPTA 20

9.3 Configuration sur SW-DIRECTION et SW-STAGIAIRES 20
9.4 Vérification 20
10. Mise en œuvre — DHCP centralisé 24
10.1 Principe 24
10.2 Exclusion des IP statiques 24
10.3 Création des pools DHCP 24
10.4 Validation côté client 24
11. Tests de connectivité 26
11.1 Ping inter-VLAN (avant ACL) 26
11.2 Traceroute pour visualiser le chemin 27
12. Sécurité — ACL d'isolation 28
12.1 Objectif 28
12.2 Création de l'ACL 28
12.3 Application de l'ACL 29
12.4 Validation 29
12.5 Analyse du résultat 30
13. Bilan et compétences mobilisées 32
13.1 Bilan du projet 32
13.2 Limites et évolutions possibles 32
13.3 Compétences mobilisées 32
14. Annexes 33
14.1 Synthèse des commandes Cisco IOS utilisées 33
14.2 Glossaire 33

1. Contexte et objectifs du projet

1.1 Contexte

Dans le cadre de la préparation de l'épreuve E5 du BTS SIO option SISR, j'ai conçu et déployé une maquette de réseau d'entreprise sur Cisco Packet Tracer. Cette maquette simule l'infrastructure d'une PME comportant trois services distincts (Comptabilité, Direction, Stagiaires) qui doivent être isolés les uns des autres tout en partageant une même infrastructure physique.

Ce projet est un incontournable du référentiel SISR : il mobilise les briques fondamentales de l'administration réseau en entreprise (VLAN, trunk 802.1Q, routage inter-VLAN, DHCP, ACL) et permet de démontrer une maîtrise concrète des équipements Cisco.

1.2 Objectifs

- Segmenter le réseau local en plusieurs VLAN afin d'isoler les services de l'entreprise.
- Mettre en œuvre le routage inter-VLAN via un Switch de niveau 3 (Catalyst 3650).
- Centraliser la distribution des adresses IP grâce à un DHCP intégré au switch L3.
- Appliquer le principe de moindre privilège via une ACL qui empêche les stagiaires d'accéder aux services sensibles.
- Valider l'ensemble de la configuration par des tests de connectivité (ping, tracert).

1.3 Cas d'usage simulé

L'architecture simule le réseau interne d'une PME fictive avec trois équipes :

Service	VLAN	Besoin
Comptabilité	VLAN 10	Accès aux applications comptables et aux partages sensibles
Direction	VLAN 20	Accès aux dossiers RH et aux rapports stratégiques
Stagiaires	VLAN 30	Accès limité : pas d'accès aux VLAN Comptabilité et Direction
Management	VLAN 99	VLAN dédié à l'administration des équipements réseau

2. Principe des VLAN et du routage inter-VLAN

2.1 Qu'est-ce qu'un VLAN ?

Un VLAN (Virtual Local Area Network) est un réseau local virtuel qui permet de segmenter logiquement un réseau physique en plusieurs sous-réseaux indépendants. Chaque VLAN constitue un domaine de diffusion isolé : les trames broadcast ne traversent pas les frontières d'un VLAN.

Les bénéfices sont multiples :

- Sécurité : isolation logique des services (un utilisateur du VLAN Stagiaires ne peut pas sniffer le trafic du VLAN Direction).
- Performance : réduction des domaines de diffusion, moins de broadcast inutile.
- Flexibilité : un même switch physique peut héberger plusieurs réseaux logiques sans recâblage.
- Organisation : regroupement logique par service, indépendant de la localisation physique des postes.

2.2 Le tagging 802.1Q

Lorsque les trames Ethernet traversent des liens entre switches, elles doivent être marquées pour indiquer à quel VLAN elles appartiennent : c'est le rôle du protocole IEEE 802.1Q. Il insère une étiquette de 4 octets dans l'en-tête Ethernet contenant notamment l'identifiant du VLAN (VLAN ID) sur 12 bits (valeurs de 1 à 4094).

Un lien entre switches qui transporte plusieurs VLAN est appelé trunk. À l'inverse, un port qui sert à connecter un terminal (PC, imprimante) est appelé port d'accès : il n'appartient qu'à un seul VLAN et les trames n'y sont pas taguées.

2.3 Routage inter-VLAN par SVI

Par défaut, deux VLAN ne peuvent pas communiquer entre eux : c'est le principe même de la segmentation. Pour permettre la communication (contrôlée) entre VLAN, il faut un équipement de niveau 3 (routeur ou switch L3) qui assure le routage.

Deux approches sont possibles :

- **Router on a stick :** un routeur externe est connecté en trunk au switch et possède une sous-interface par VLAN. Solution classique mais limitée en performance.
- **Switch L3 avec SVI :** le switch lui-même fait le routage grâce à des Switch Virtual Interfaces (interfaces logiques associées à chaque VLAN). Solution moderne, routage en hardware via ASIC, bien plus performante.

Pour ce projet, j'ai retenu l'approche Switch L3 avec SVI, qui correspond aux architectures d'entreprise modernes.

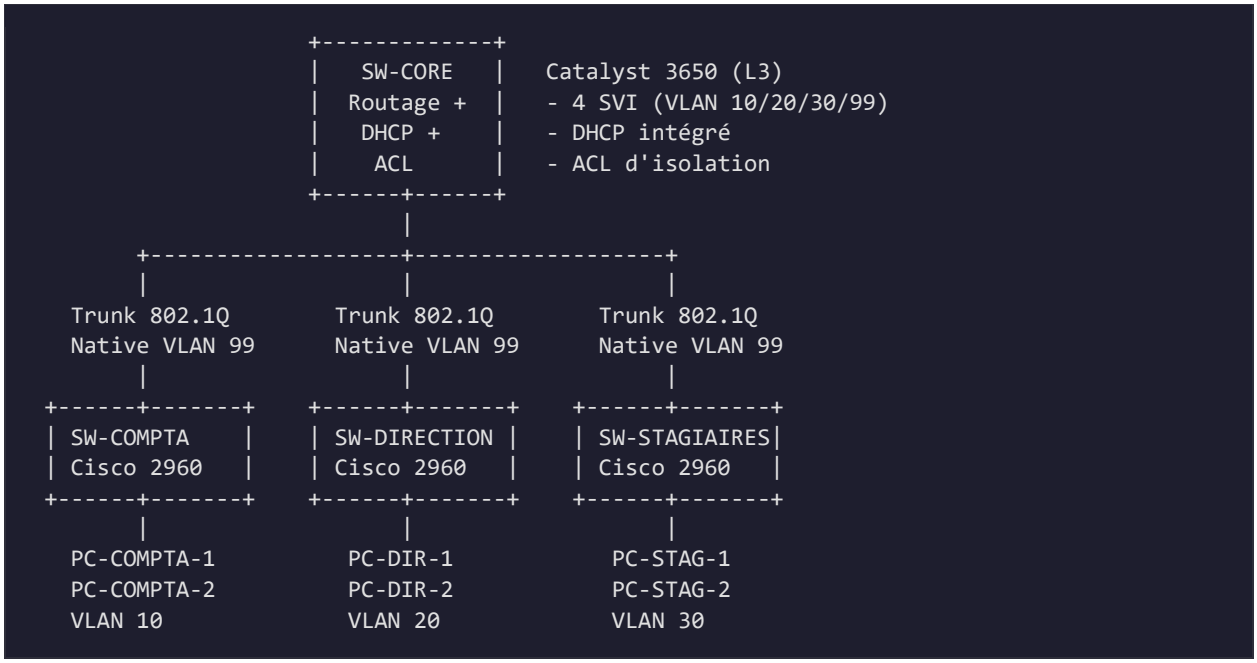
> **À RETENIR — À retenir — SVI**

Une SVI (Switch Virtual Interface) est une interface logique portée par un switch L3 et associée à un VLAN. Elle possède une adresse IP qui sert de passerelle par défaut pour tous les équipements du VLAN. C'est elle qui assure le routage des paquets entre VLAN.

3. Architecture retenue

L'architecture déployée suit le modèle hiérarchique Core/Access : un switch de cœur de réseau (L3) centralise le routage et les services, tandis que trois switches d'accès (L2) desservent chacun un VLAN particulier.

3.1 Schéma logique



3.2 Équipements

Équipement	Qté	Rôle
Cisco Catalyst 3650-24PS (L3)	1	Switch de cœur : routage inter-VLAN, DHCP, ACL
Cisco Catalyst 2960-24TT (L2)	3	Switches d'accès : ports d'accès pour les utilisateurs
PC-PT (poste client)	6	Deux postes par service pour les tests de connectivité

4. Plan d'adressage IP

L'adressage privé de classe C (192.168.0.0/16) a été choisi pour sa simplicité et sa conformité avec les conventions d'entreprise. Chaque VLAN utilise un sous-réseau /24 distinct.

VLAN	Nom	Réseau	Gateway	Plage DHCP
10	Comptabilite	192.168.10.0/24	192.168.10.1	.100-.254
20	Direction	192.168.20.0/24	192.168.20.1	.100-.254
30	Stagiaires	192.168.30.0/24	192.168.30.1	.100-.254
99	Management	192.168.99.0/24	192.168.99.1	Statique

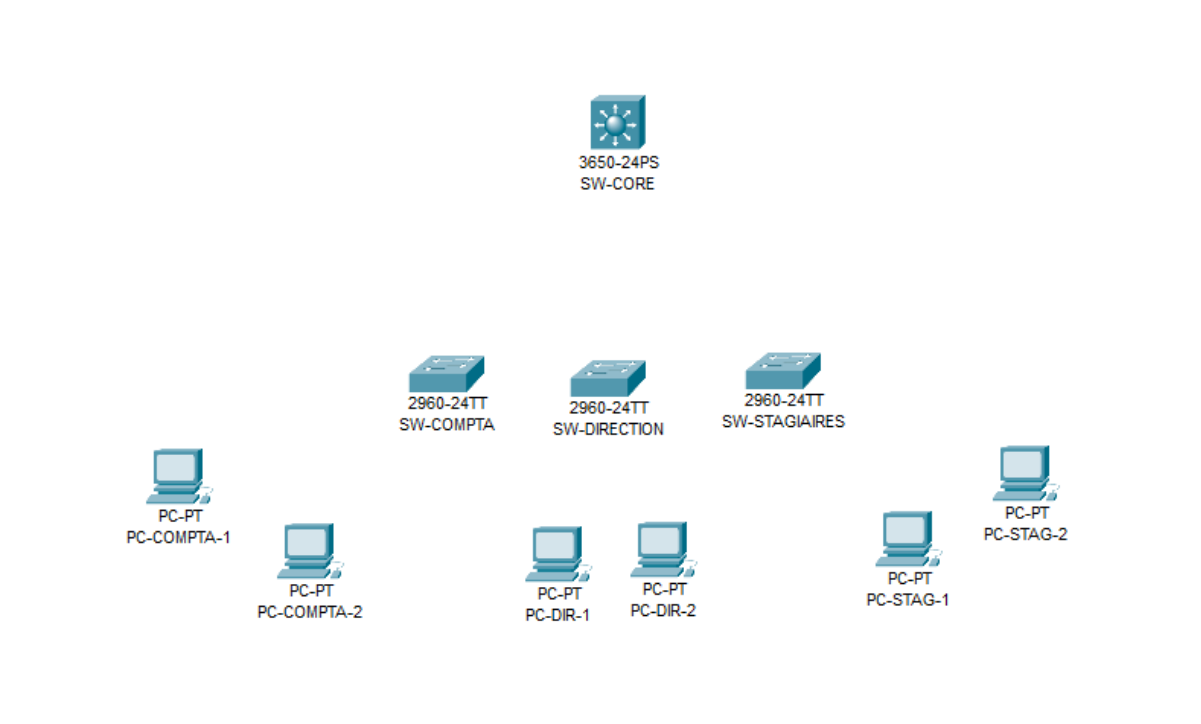
À RETENIR — À retenir — Convention d'adressage

J'ai appliqué la convention professionnelle classique : les IP de .1 à .99 sont réservées aux équipements réseau (switches, serveurs, imprimantes) en statique ; les IP de .100 à .254 sont distribuées dynamiquement par DHCP aux postes utilisateurs. Cela facilite l'inventaire et évite les conflits.

5. Mise en œuvre — Topologie physique

5.1 Mise en place des équipements

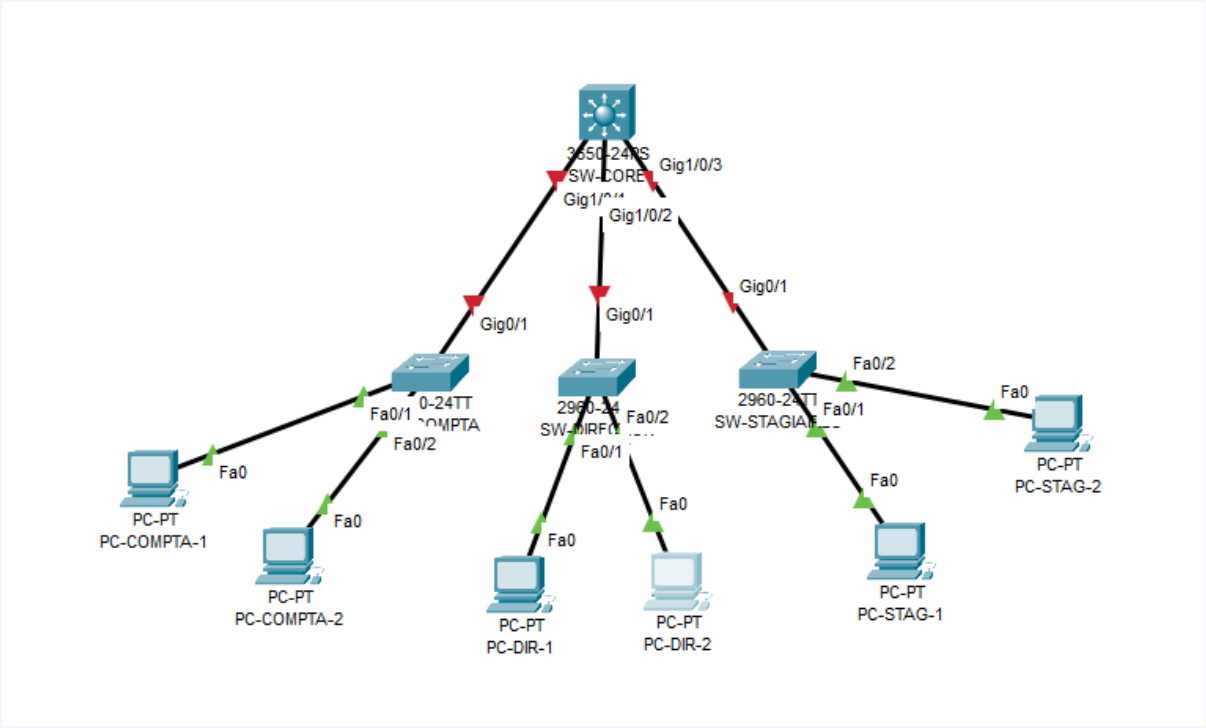
La topologie est construite sur Cisco Packet Tracer : placement des quatre switches, des six PC clients, puis renommage de chaque équipement pour faciliter la lecture de la maquette.



Topologie initiale avec les quatre switches et les six PC placés et renommés

5.2 Câblage

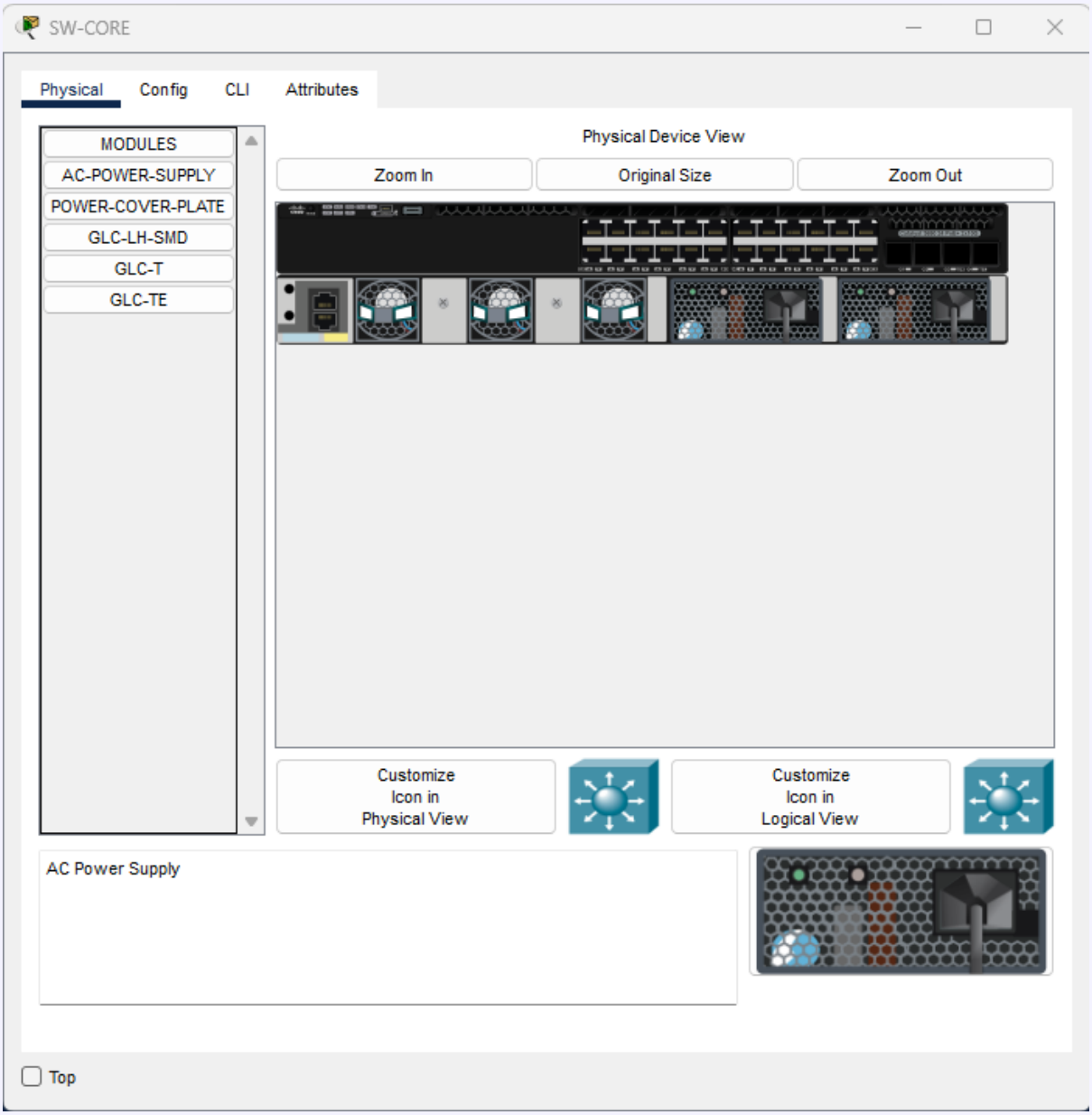
Les liens entre équipements utilisent des câbles cuivre droits. Les liaisons SW-CORE vers chaque switch d'accès empruntent les interfaces GigabitEthernet (Gi1/0/1 à Gi1/0/3) pour offrir un débit supérieur, tandis que les PC sont connectés aux ports FastEthernet des switches d'accès.



Topologie complètement câblée avec les liens trunk (Core-Access) et access (Switch-PC)

5.3 Alimentation du Switch L3

Particularité découverte pendant la mise en œuvre : le Catalyst 3650-24PS est livré sans alimentation dans Packet Tracer. Il est nécessaire d'ajouter manuellement le module AC-POWER-SUPPLY via la vue Physical, après avoir éteint le switch (pas de hot-swap sur ce modèle).



Vue Physical de SW-CORE avec l'emplacement d'alimentation vide et le module AC-POWER-SUPPLY disponible à gauche

À RETENIR — À retenir — Redondance d'alimentation

En environnement professionnel, les switches de cœur de réseau disposent généralement de deux alimentations redondantes (configuration N+1). Cette redondance garantit la continuité de service en cas de défaillance d'une PSU et permet même une maintenance sans interruption grâce au hot-swap sur les modèles haut de gamme.

6. Mise en œuvre — Configuration des VLAN

6.1 Création des VLAN sur SW-CORE

Après connexion au switch SW-CORE via le CLI et passage en mode de configuration globale, les quatre VLAN sont créés et nommés de manière explicite pour faciliter l'administration :

```
SW-CORE> enable
SW-CORE# configure terminal
SW-CORE(config)# hostname SW-CORE

SW-CORE(config)# vlan 10
SW-CORE(config-vlan)# name Comptabilite
SW-CORE(config-vlan)# exit

SW-CORE(config)# vlan 20
SW-CORE(config-vlan)# name Direction
SW-CORE(config-vlan)# exit

SW-CORE(config)# vlan 30
SW-CORE(config-vlan)# name Stagiaires
SW-CORE(config-vlan)# exit

SW-CORE(config)# vlan 99
SW-CORE(config-vlan)# name Management
SW-CORE(config-vlan)# exit
```

Décomposition des commandes :

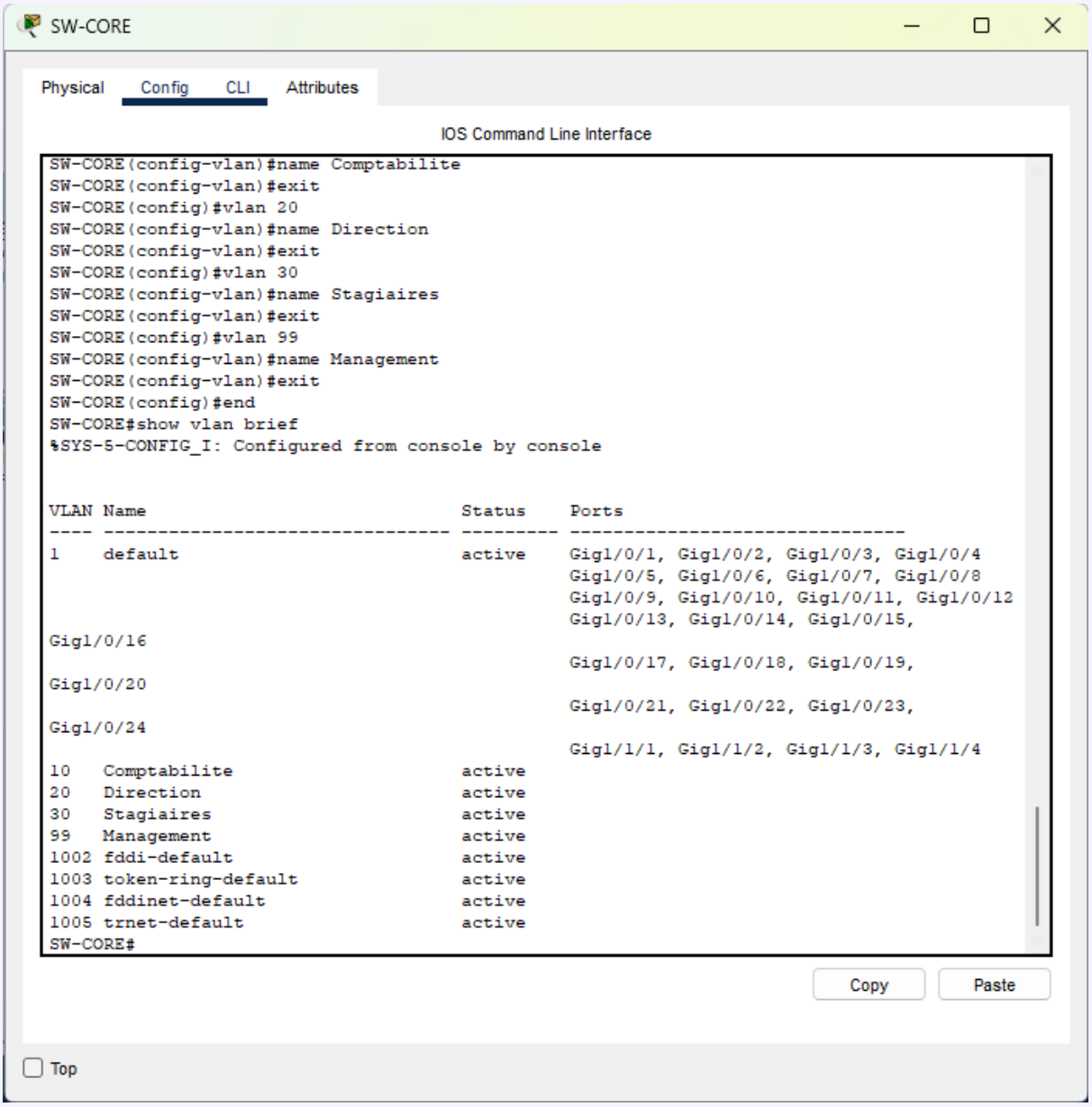
Commande	Rôle
enable	Passage en mode privilégié (prompt #)
configure terminal	Entrée en mode de configuration globale
hostname SW-CORE	Définit le nom du switch (visible dans le prompt)
vlan 10	Crée le VLAN 10 et entre dans son mode de config
name Comptabilite	Attribue un nom lisible au VLAN

6.2 Vérification

La commande show vlan brief permet de vérifier la création effective des VLAN :

```
SW-CORE# show vlan brief
```

Le résultat affiche les quatre VLAN avec le statut active :



Résultat de show vlan brief sur SW-CORE avec les VLAN 10, 20, 30 et 99 en statut active

6.3 Création des VLAN sur les switches d'accès

Les trois switches d'accès (SW-COMPTA, SW-DIRECTION, SW-STAGIAIRES) doivent également connaître les mêmes VLAN dans leur base locale, afin de pouvoir assigner des ports d'accès ou de transporter les trames taguées sur les trunks. Les commandes sont identiques à celles de SW-CORE.

7. Mise en œuvre — Trunks 802.1Q

7.1 Principe

Un trunk est un lien entre switches qui transporte plusieurs VLAN simultanément, en marquant chaque trame avec son VLAN d'origine grâce au protocole 802.1Q. C'est indispensable pour que les VLAN définis sur SW-CORE soient également accessibles depuis les switches d'accès.

7.2 Configuration sur SW-CORE

Les trois interfaces Gi1/0/1 à Gi1/0/3 sont configurées en mode trunk avec les paramètres suivants :

```
SW-CORE(config)# interface range GigabitEthernet1/0/1 - 3
SW-CORE(config-if-range)# switchport mode trunk
SW-CORE(config-if-range)# switchport trunk allowed vlan 10,20,30,99
SW-CORE(config-if-range)# switchport trunk native vlan 99
SW-CORE(config-if-range)# description Trunk vers switch d acces
SW-CORE(config-if-range)# exit
```

Commande	Rôle
interface range Gi1/0/1 - 3	Configure les trois interfaces d'un seul coup (gain de temps et cohérence)
switchport mode trunk	Force le port en mode trunk (pas de négociation DTP)
switchport trunk allowed vlan 10,20,30,99	Limite les VLAN autorisés sur le trunk (moindre privilège)
switchport trunk native vlan 99	Change le VLAN natif de 1 vers 99 (sécurité anti VLAN-hopping)
description ...	Documentation du port (utile pour les opérations futures)

À RETENIR — À retenir — VLAN natif et VLAN hopping

Le VLAN natif est le VLAN par défaut sur un trunk dont les trames ne sont pas taguées. Par défaut c'est le VLAN 1. Un attaquant peut exploiter cette configuration par double-tagging pour envoyer des trames dans un autre VLAN (attaque VLAN hopping). Bonne pratique : changer le VLAN natif pour un VLAN dédié non utilisé (ici, le VLAN 99 Management) rend cette attaque inopérante.

À RETENIR — À retenir — Évolution de l'encapsulation

Sur les anciens switches Catalyst (3560, 3750), il fallait exécuter la commande switchport trunk encapsulation dot1q avant d'activer le mode trunk, car ces équipements supportaient aussi l'encapsulation propriétaire Cisco ISL. Sur le 3650, cette commande n'existe plus : seul le standard IEEE 802.1Q est supporté. C'est représentatif de l'évolution des équipements vers les standards ouverts.

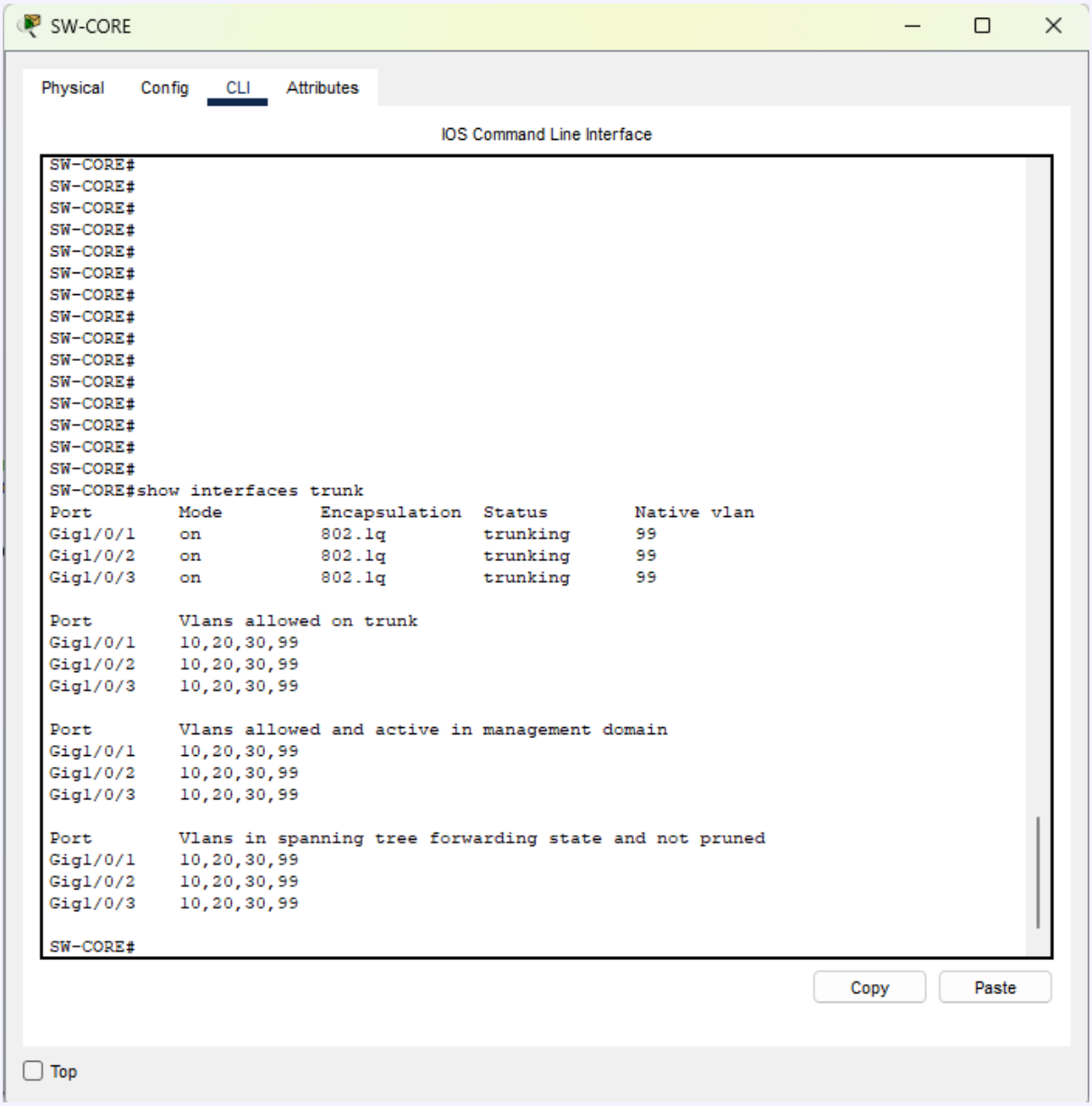
7.3 Configuration sur les switches d'accès

Sur chaque switch d'accès, l'interface Gi0/1 (vers SW-CORE) est configurée en trunk avec les mêmes paramètres :

```
SW-COMPTA(config)# interface GigabitEthernet0/1
SW-COMPTA(config-if)# switchport mode trunk
SW-COMPTA(config-if)# switchport trunk allowed vlan 10,20,30,99
SW-COMPTA(config-if)# switchport trunk native vlan 99
SW-COMPTA(config-if)# description Trunk vers SW-CORE
SW-COMPTA(config-if)# exit
```

7.4 Vérification

La commande show interfaces trunk sur SW-CORE permet de vérifier que les trois trunks sont opérationnels et que les bons VLAN sont autorisés :



Résultat de show interfaces trunk sur SW-CORE — trois ports en trunking 802.1q avec native VLAN 99 et VLANs 10/20/30/99 autorisés

8. Mise en œuvre — Routage inter-VLAN (SVI)

8.1 Activation du routage IP

Par défaut, un switch L3 Cisco ne route pas les paquets entre VLAN. Il faut activer explicitement la fonctionnalité :

```
SW-CORE(config)# ip routing
```

8.2 Création des SVI

Une SVI est créée pour chaque VLAN, avec une adresse IP qui servira de passerelle par défaut aux postes du VLAN :

```
SW-CORE(config)# interface vlan 10
SW-CORE(config-if)# description SVI Comptabilite
SW-CORE(config-if)# ip address 192.168.10.1 255.255.255.0
SW-CORE(config-if)# no shutdown
SW-CORE(config-if)# exit

SW-CORE(config)# interface vlan 20
SW-CORE(config-if)# description SVI Direction
SW-CORE(config-if)# ip address 192.168.20.1 255.255.255.0
SW-CORE(config-if)# no shutdown
SW-CORE(config-if)# exit

SW-CORE(config)# interface vlan 30
SW-CORE(config-if)# description SVI Stagiaires
SW-CORE(config-if)# ip address 192.168.30.1 255.255.255.0
SW-CORE(config-if)# no shutdown
SW-CORE(config-if)# exit

SW-CORE(config)# interface vlan 99
SW-CORE(config-if)# description SVI Management
SW-CORE(config-if)# ip address 192.168.99.1 255.255.255.0
SW-CORE(config-if)# no shutdown
SW-CORE(config-if)# exit
```

Commande	Rôle
interface vlan 10	Crée la SVI (interface logique) pour le VLAN 10
ip address 192.168.10.1 255.255.255.0	Attribue l'IP de gateway au SVI
no shutdown	Active l'interface (par défaut elle est administrativement down)

8.3 Sauvegarde de la configuration

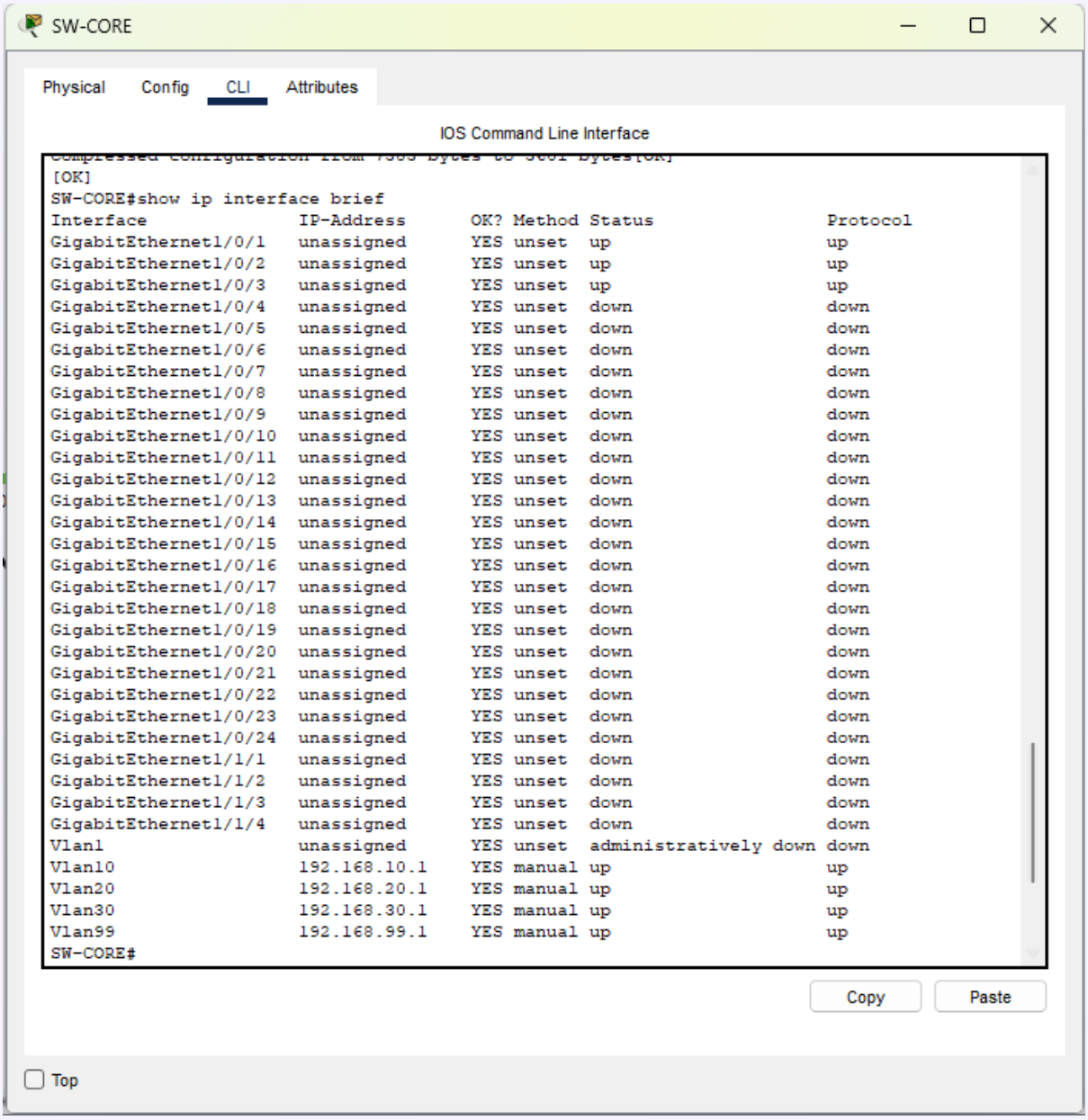
Dans Cisco IOS, la configuration en cours (running-config) est volatile : elle est perdue au redémarrage. Il faut la copier dans la configuration de démarrage (startup-config), stockée en mémoire non volatile :

```
SW-CORE# write memory
```

> **À RETENIR — À retenir — running-config vs startup-config**
>
> Deux fichiers de configuration coexistent sur un équipement Cisco. La running-config est la config active en RAM, modifiée à chaque commande. La startup-config est celle chargée au démarrage. La commande write memory (ou copy running-config startup-config) sauvegarde la config active pour qu'elle survive à un redémarrage. À faire systématiquement après chaque modification importante.

8.4 Vérification

La commande show ip interface brief affiche toutes les interfaces avec leur IP et leur état :



Résultat de show ip interface brief sur SW-CORE — les quatre SVI (Vlan10, Vlan20, Vlan30, Vlan99) sont en up/up avec leur IP

9. Mise en œuvre — Ports d'accès

9.1 Principe

Les ports d'accès sont ceux qui connectent les postes utilisateurs au switch. Ils appartiennent à un seul VLAN et ne tagguent pas les trames. C'est le switch qui associe automatiquement chaque trame reçue au VLAN du port d'accès correspondant.

9.2 Configuration sur SW-COMPTA

```
SW-COMPTA(config)# interface range FastEthernet0/1 - 2
SW-COMPTA(config-if-range)# switchport mode access
SW-COMPTA(config-if-range)# switchport access vlan 10
SW-COMPTA(config-if-range)# description Poste utilisateur VLAN 10 Comptabilite
SW-COMPTA(config-if-range)# exit
```

Commande	Rôle
switchport mode access	Force le port en mode access (1 seul VLAN, pas de tagging)
switchport access vlan 10	Assigne le port au VLAN 10

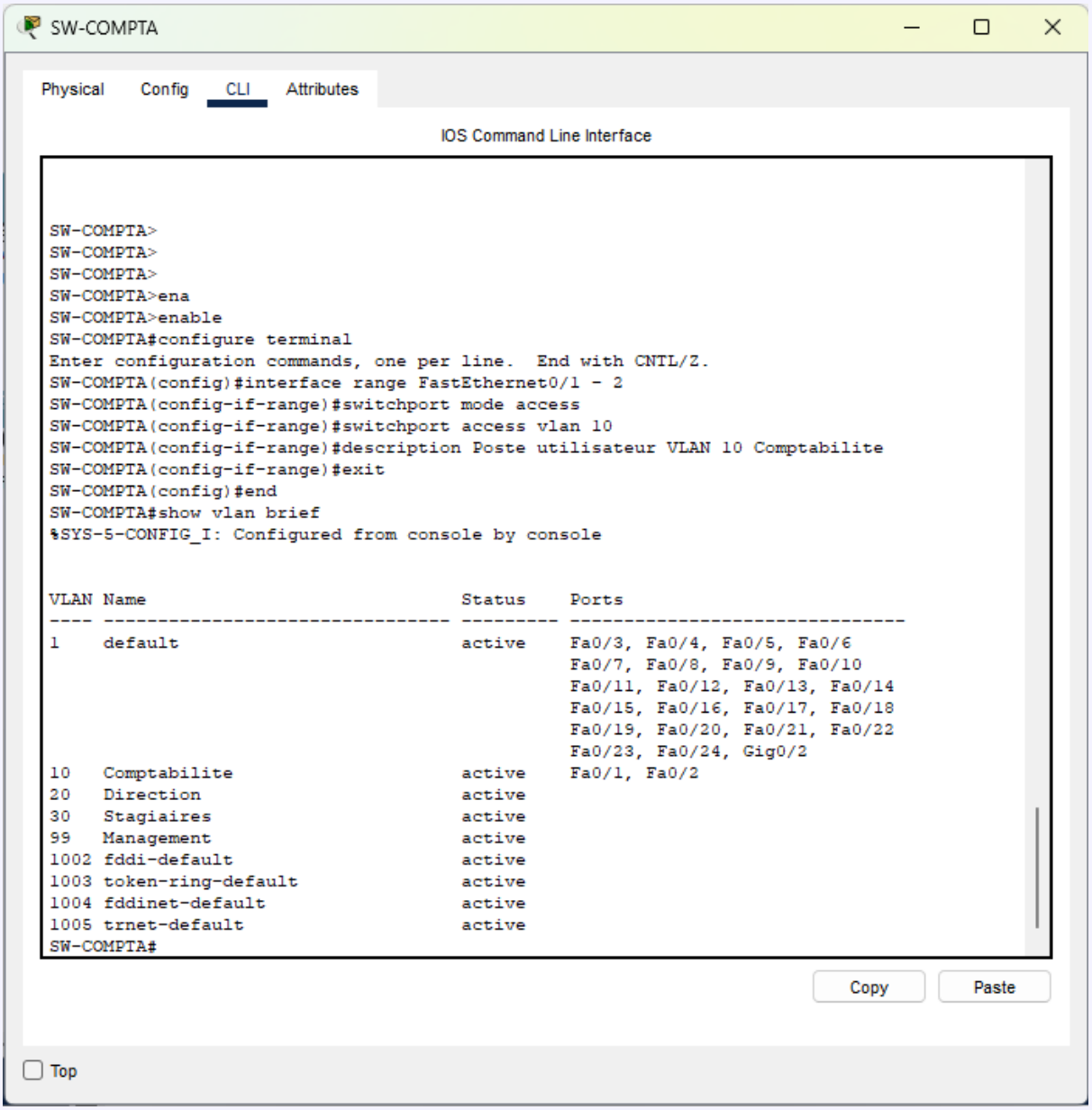
> **À RETENIR — À retenir — Port access vs trunk**
>
> Port access : pour les endpoints (PC, imprimante, serveur). Un seul VLAN. Trames non taguées. Port trunk : pour les liaisons inter-switches ou vers des hyperviseurs. Plusieurs VLAN transportés. Trames taguées en 802.1Q. Ne jamais brancher un PC sur un port trunk : le PC ne comprendrait pas les trames taguées.

9.3 Configuration sur SW-DIRECTION et SW-STAGIAIRES

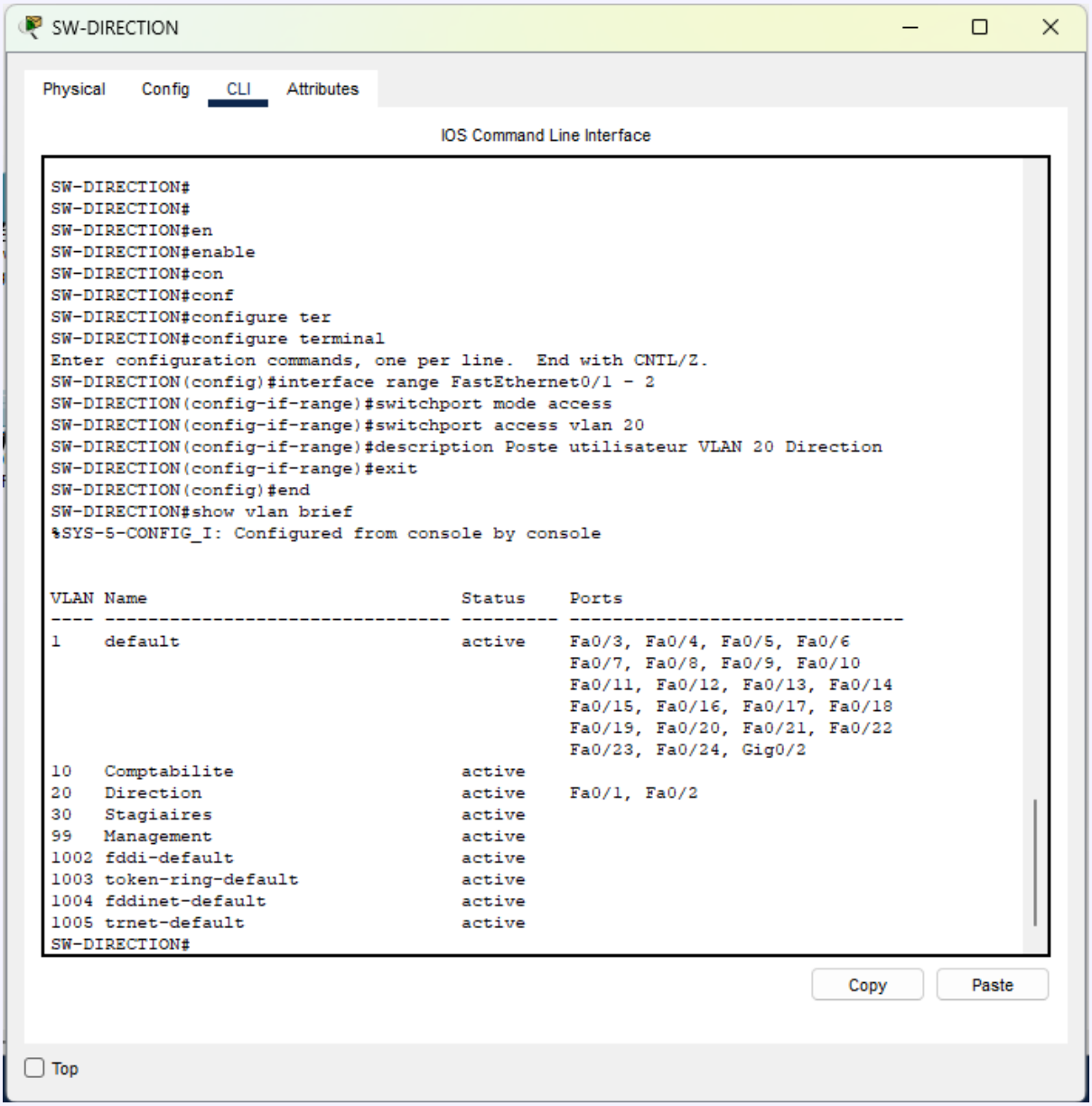
La procédure est identique sur les deux autres switches d'accès, en changeant le numéro de VLAN (20 pour Direction, 30 pour Stagiaires).

9.4 Vérification

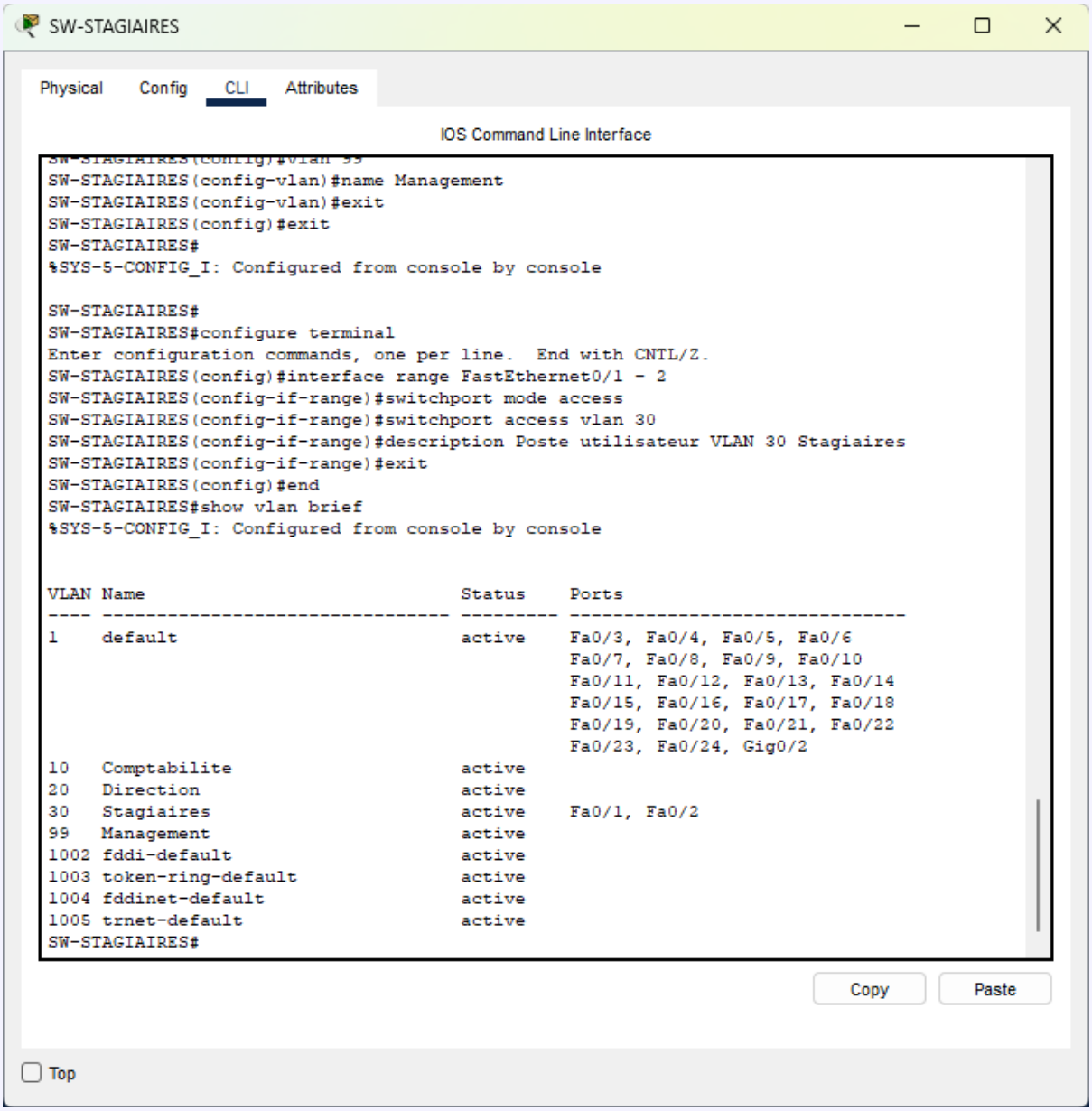
Sur chaque switch d'accès, show vlan brief permet de vérifier que les ports Fa0/1 et Fa0/2 sont bien assignés au VLAN attendu :



Résultat de show vlan brief sur SW-COMPTA — ports Fa0/1 et Fa0/2 dans le VLAN 10



Résultat de show vlan brief sur SW-DIRECTION — ports Fa0/1 et Fa0/2 dans le VLAN 20



Résultat de show vlan brief sur SW-STAGIAIRES — ports Fa0/1 et Fa0/2 dans le VLAN 30

10. Mise en œuvre — DHCP centralisé

10.1 Principe

Plutôt que d'attribuer une IP statique à chaque poste (fastidieux et source d'erreurs), le DHCP (Dynamic Host Configuration Protocol) distribue automatiquement les paramètres réseau (IP, masque, gateway, DNS) aux clients qui en font la demande. SW-CORE joue ici le rôle de serveur DHCP pour les trois VLAN utilisateurs.

10.2 Exclusion des IP statiques

Avant de définir les pools DHCP, on exclut les plages réservées aux équipements réseau (.1 à .99). Sans cette exclusion, le DHCP risquerait d'attribuer à un client une IP déjà utilisée par une SVI ou un équipement fixe :

```
SW-CORE(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.99
SW-CORE(config)# ip dhcp excluded-address 192.168.20.1 192.168.20.99
SW-CORE(config)# ip dhcp excluded-address 192.168.30.1 192.168.30.99
```

10.3 Création des pools DHCP

Un pool DHCP est défini par VLAN avec les paramètres suivants : réseau à distribuer, passerelle par défaut (la SVI du VLAN), serveur DNS et nom de domaine.

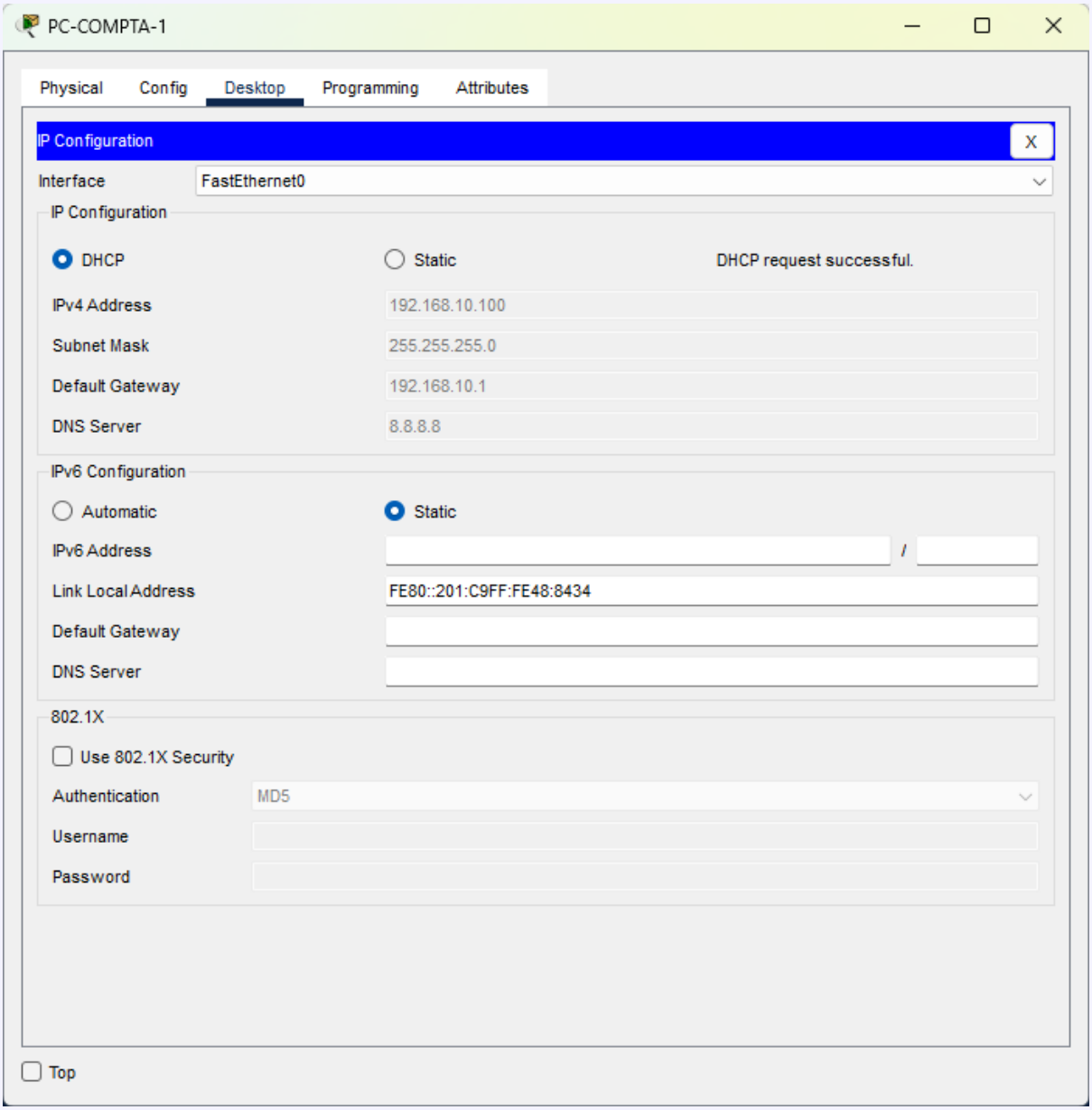
```
SW-CORE(config)# ip dhcp pool POOL_VLAN10
SW-CORE(dhcp-config)# network 192.168.10.0 255.255.255.0
SW-CORE(dhcp-config)# default-router 192.168.10.1
SW-CORE(dhcp-config)# dns-server 8.8.8.8
SW-CORE(dhcp-config)# domain-name comptabilite.local
SW-CORE(dhcp-config)# exit

SW-CORE(config)# ip dhcp pool POOL_VLAN20
SW-CORE(dhcp-config)# network 192.168.20.0 255.255.255.0
SW-CORE(dhcp-config)# default-router 192.168.20.1
SW-CORE(dhcp-config)# dns-server 8.8.8.8
SW-CORE(dhcp-config)# domain-name direction.local
SW-CORE(dhcp-config)# exit

SW-CORE(config)# ip dhcp pool POOL_VLAN30
SW-CORE(dhcp-config)# network 192.168.30.0 255.255.255.0
SW-CORE(dhcp-config)# default-router 192.168.30.1
SW-CORE(dhcp-config)# dns-server 8.8.8.8
SW-CORE(dhcp-config)# domain-name stagiaires.local
SW-CORE(dhcp-config)# exit
```

10.4 Validation côté client

Sur chaque PC, l'onglet Desktop > IP Configuration permet de basculer du mode Static au mode DHCP. Après quelques secondes, le PC reçoit automatiquement une IP dans la plage du VLAN auquel son port switch est associé :



IP Configuration d'un PC de la Comptabilité avec une adresse IP 192.168.10.X obtenue automatiquement par DHCP, gateway 192.168.10.1 et suffixe DNS comptabilite.local

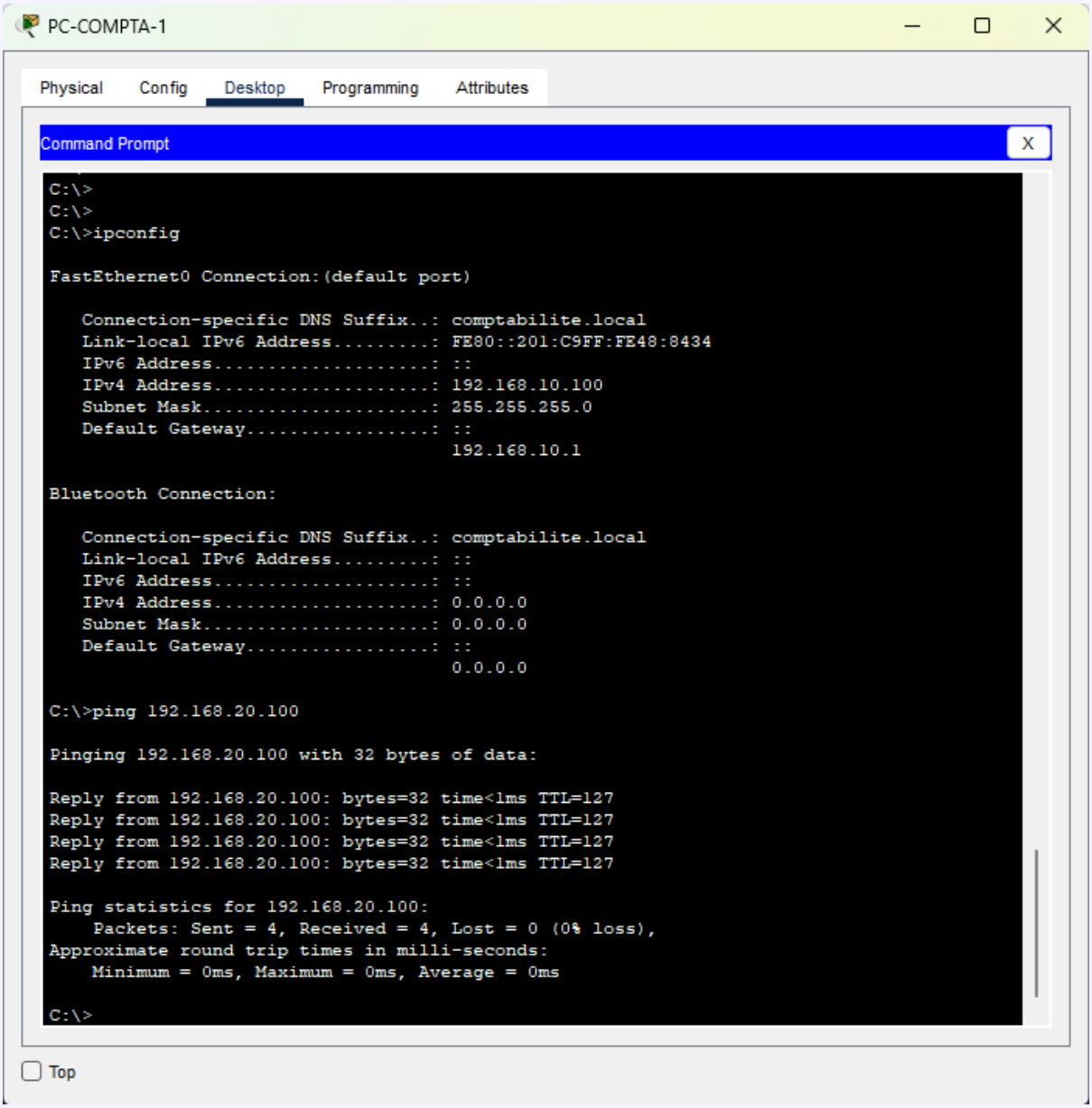
À RETENIR — À retenir — DHCP sur un switch L3

Contrairement à un environnement avec serveur DHCP dédié (souvent un Windows Server), ici le switch L3 porte directement la fonction. Cette approche est courante dans les réseaux de taille modeste ou dans les agences distantes. Pour des réseaux plus grands, on préfère un serveur DHCP centralisé avec des agents DHCP relay sur chaque switch.

11. Tests de connectivité

11.1 Ping inter-VLAN (avant ACL)

Avant la mise en place de l'ACL de sécurité, tous les VLAN peuvent communiquer entre eux via le routage SVI. Le test ping depuis PC-COMPTA-1 vers un PC de la Direction le confirme :



Depuis PC-COMPTA-1, résultat de ipconfig (192.168.10.100) puis ping réussi vers 192.168.20.100 — 4 Reply, 0 % loss, TTL=127

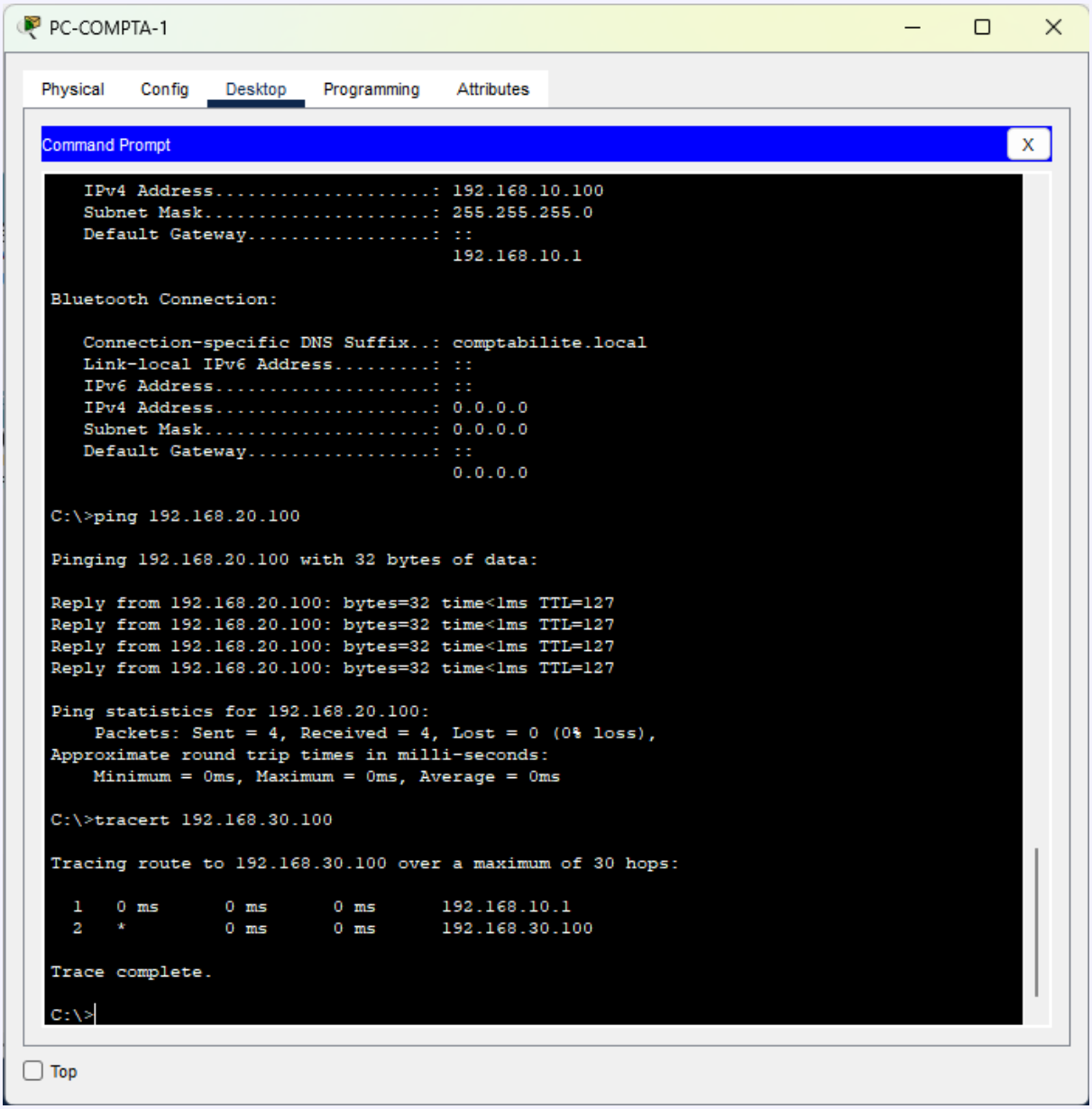
À RETENIR — À retenir — Le TTL révèle le routage

Windows envoie ses paquets ICMP avec un TTL initial de 128. Chaque fois qu'un paquet traverse un routeur (ou une SVI), le TTL est décrémenté de 1. Observer TTL=127 dans la réponse prouve que le

paquet a bien traversé exactement un équipement L3 — en l'occurrence, le switch SW-CORE qui a routé le paquet entre les VLAN 10 et 20.

11.2 Traceroute pour visualiser le chemin

La commande tracert affiche explicitement chaque saut emprunté par le paquet. Depuis PC-COMPTA-1 vers un PC stagiaire, on observe deux sauts : d'abord la gateway du VLAN 10 (la SVI de SW-CORE), puis la destination dans le VLAN 30 :



Résultat de tracert 192.168.30.100 depuis PC-COMPTA-1 : saut 1 = 192.168.10.1 (SVI VLAN 10), saut 2 = 192.168.30.100 (PC destination)

12. Sécurité — ACL d'isolation

12.1 Objectif

Les stagiaires ne doivent pas pouvoir accéder aux ressources des services Comptabilité et Direction. La mise en place d'une ACL étendue sur la SVI VLAN 30 permet de bloquer le trafic IP sortant vers ces deux VLAN tout en laissant passer le reste (Internet, intra-VLAN, etc.).

12.2 Création de l'ACL

```
SW-CORE(config)# ip access-list extended ACL_STAGIAIRES
SW-CORE(config-ext-nacl)# remark Bloquer l acces des stagiaires aux VLAN sensibles
SW-CORE(config-ext-nacl)# deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
SW-CORE(config-ext-nacl)# deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
SW-CORE(config-ext-nacl)# permit ip any any
SW-CORE(config-ext-nacl)# exit
```

Commande	Rôle
ip access-list extended ACL_STAGIAIRES	Crée une ACL étendue nommée (filtrage sur source + destination + protocole)
remark ...	Commentaire non exécuté, utile pour la documentation dans la config
deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255	Bloque tout trafic IP du VLAN 30 vers le VLAN 10 (wildcard mask 0.0.0.255 = /24)
deny ip ... 192.168.20.0 ...	Idem vers le VLAN 20
permit ip any any	Autorise tout le reste (indispensable à cause du deny implicite en fin d'ACL)

À RETENIR — À retenir — Wildcard mask

Cisco utilise des wildcard masks (inverses des masques réseau classiques) dans les ACL. Un /24 classique (255.255.255.0) devient 0.0.0.255 en wildcard. La règle est simple : les bits à 0 doivent matcher exactement, les bits à 1 sont libres. Pour une seule IP : 0.0.0.0. Pour un /16 : 0.0.255.255.

À RETENIR — À retenir — Ordre d'évaluation et deny implicite

Les règles d'une ACL sont évaluées de haut en bas, et dès qu'une règle correspond au paquet, l'évaluation s'arrête. À la fin de toute ACL Cisco, il existe un deny ip any any implicite et invisible. D'où l'importance de toujours terminer par permit ip any any si l'on veut laisser passer le trafic non explicitement bloqué.

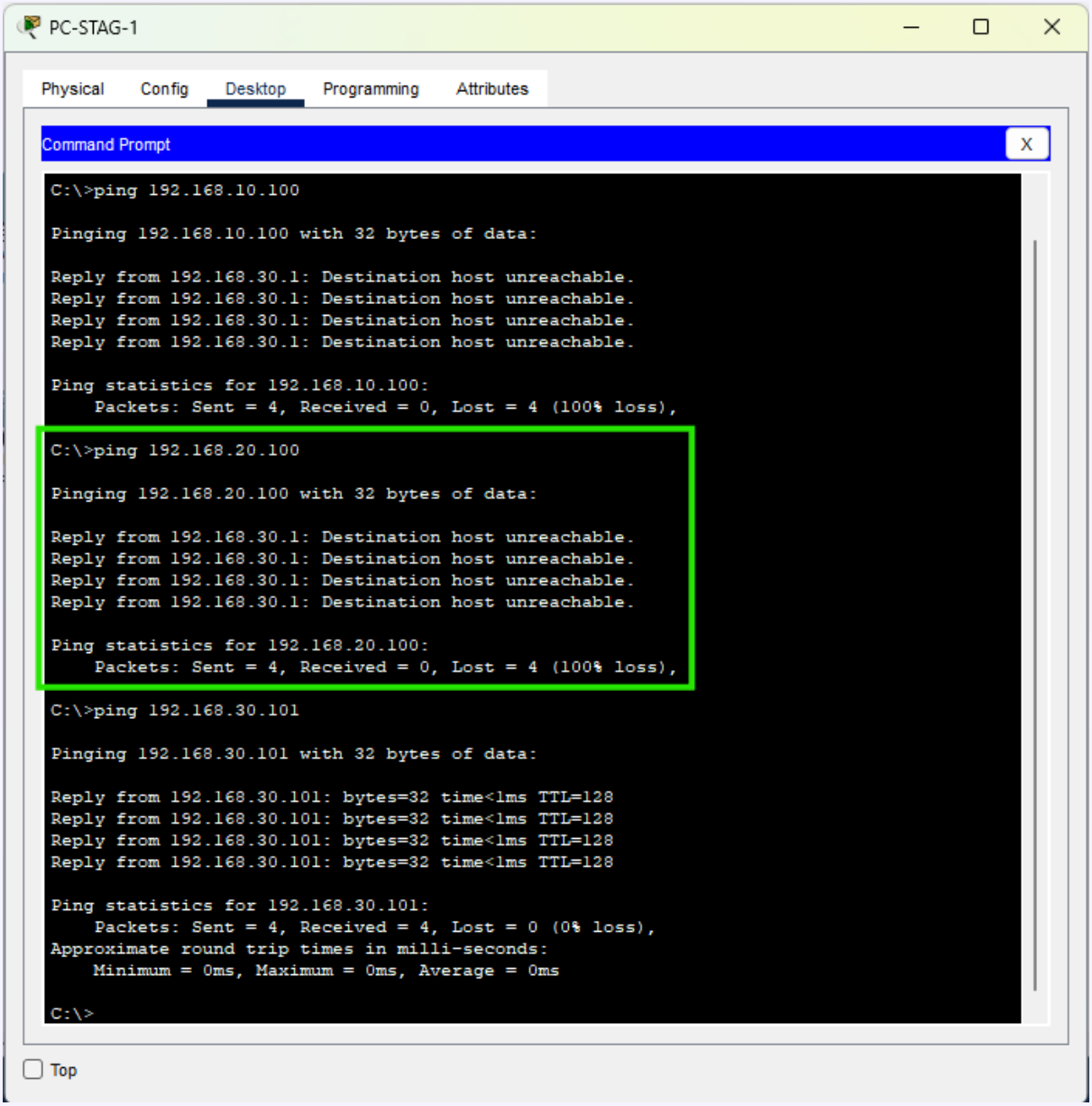
12.3 Application de l'ACL

L'ACL est appliquée en entrée (direction in) de la SVI VLAN 30, c'est-à-dire sur le trafic qui arrive des PC Stagiaires vers le switch. C'est le point le plus efficace pour filtrer : le trafic est bloqué avant même d'être routé.

```
SW-CORE(config)# interface vlan 30
SW-CORE(config-if)# ip access-group ACL_STAGIAIRES in
SW-CORE(config-if)# exit
SW-CORE(config)# end
SW-CORE# write memory
```

12.4 Validation

Depuis PC-STAG-1, les pings vers les VLAN 10 et 20 sont bien bloqués et retournent le message Destination host unreachable émis par la SVI VLAN 30 (192.168.30.1) qui joue le rôle de routeur filtrant. Le ping intra-VLAN vers PC-STAG-2 continue en revanche à fonctionner :

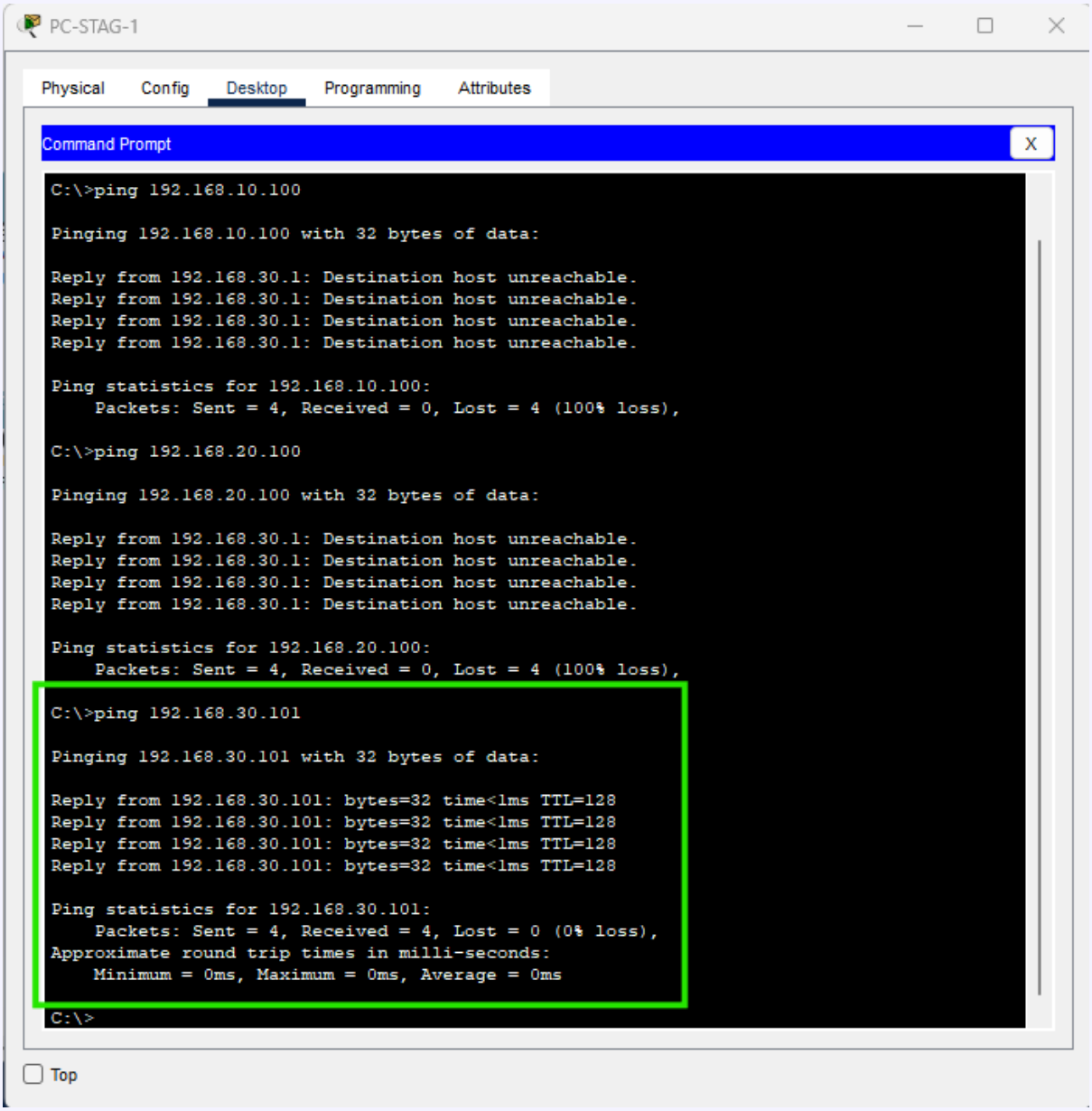


Depuis PC-STAG-1, ping vers 192.168.10.100 et 192.168.20.100 — échec avec Destination host unreachable (ACL bloque), mais ping vers 192.168.30.101 réussi (intra-VLAN, TTL=128)

12.5 Analyse du résultat

Deux éléments confirment que la sécurité fonctionne comme prévu :

- **Message Destination host unreachable émis par 192.168.30.1 :** c'est la SVI du VLAN Stagiaires qui répond explicitement, preuve que c'est bien l'ACL qui bloque et pas un souci de routage.
- **TTL=128 sur le ping intra-VLAN :** aucun routeur traversé — le trafic passe directement par SW-STAGIAIRES au niveau L2 sans remonter à SW-CORE. Cela démontre que l'ACL agit uniquement au niveau L3, comme prévu.



Gros plan sur le ping intra-VLAN 30 réussi (192.168.30.100 → 192.168.30.101) avec TTL=128, preuve que l'ACL n'affecte pas le trafic interne au VLAN Stagiaires

13. Bilan et compétences mobilisées

13.1 Bilan du projet

Le projet a été mené à son terme avec succès : l'ensemble des objectifs fixés en début de projet ont été atteints et validés par des tests concrets.

Objectif	Résultat
Segmentation en VLAN par service	Atteint (4 VLAN + 1 Management)
Routage inter-VLAN par Switch L3	Atteint (4 SVI opérationnelles)
DHCP centralisé et distribution par VLAN	Atteint (3 pools DHCP actifs)
Isolation des Stagiaires par ACL	Atteint (ACL étendue validée par tests)
Validation par tests de connectivité	Atteint (ping + tracert + analyse TTL)

13.2 Limites et évolutions possibles

- Ajouter du Port Security sur les ports d'accès pour limiter les MAC autorisées (anti-branchement sauvage).
- Activer SSH sur les switches avec PKI locale pour l'administration distante sécurisée (en remplacement de Telnet).
- Forcer SW-CORE comme root bridge explicite via spanning-tree vlan 1-99 priority 0 pour maîtriser la topologie STP.
- Mettre en place une redondance HSRP/VRRP sur deux switches L3 pour garantir la haute disponibilité du routage.
- Reproduire l'architecture sur matériel physique réel (switches 2960/3650) pour valider en conditions professionnelles.

13.3 Compétences mobilisées

Bloc	Compétence / sous-compétence mobilisée
Support et mise à disposition	Gérer le patrimoine — Recenser les ressources, plan d'adressage, standards (802.1Q)
Support et mise à disposition	Gérer les habilitations — Segmentation par VLAN, ACL par rôle
Administration réseau	Configurer les équipements d'interconnexion — Switch L2 et L3, trunks 802.1Q, SVI
Services réseau	Déployer des services de base — DHCP serveur intégré, routage IP
Cybersécurité	Appliquer le moindre privilège — ACL d'isolation, VLAN natif sécurisé
Pilotage	Travailler en mode projet — Conception, déploiement, tests, documentation

14. Annexes

14.1 Synthèse des commandes Cisco IOS utilisées

Commande	Rôle
enable	Passage en mode privilégié
configure terminal	Entrée en mode config globale
vlan X / name ...	Création et nommage d'un VLAN
switchport mode trunk / access	Définit le mode d'un port
switchport trunk allowed vlan ...	Liste des VLAN autorisés sur un trunk
switchport access vlan X	Assigne un port d'accès à un VLAN
ip routing	Active le routage IP sur un switch L3
interface vlan X	Crée la SVI d'un VLAN
ip address ... / no shutdown	Attribue une IP et active l'interface
ip dhcp pool / network / default-router	Configuration d'un pool DHCP
ip access-list extended / permit / deny	Création d'une ACL étendue nommée
ip access-group X in|out	Application d'une ACL à une interface
show vlan brief	Liste les VLAN et leur assignation
show interfaces trunk	Vérifie l'état des trunks
show ip interface brief	Liste les interfaces IP et leur état
show running-config	Affiche la configuration active
write memory	Sauvegarde la config en NVRAM

14.2 Glossaire

Terme	Définition
VLAN	Virtual LAN — Réseau local virtuel, segmente un réseau physique en sous-réseaux logiques isolés
802.1Q	Standard IEEE de tagging VLAN sur les trames Ethernet (tag de 4 octets)
SVI	Switch Virtual Interface — Interface logique L3 d'un switch associée à un VLAN
Trunk	Lien qui transporte plusieurs VLAN, avec trames taguées en 802.1Q
Port d'accès	Port pour un endpoint, appartient à un seul VLAN, trames non taguées

VLAN natif	VLAN par défaut d'un trunk (trames non taguées) — à changer pour la sécurité
ACL	Access Control List — Liste de règles de filtrage appliquée à une interface
Wildcard mask	Masque inversé utilisé par Cisco dans les ACL (ex: /24 = 0.0.0.255)
DHCP	Dynamic Host Configuration Protocol — Distribue automatiquement les paramètres IP
TTL	Time To Live — Compteur décrémenté à chaque saut L3, permet de détecter les boucles
VLAN hopping	Attaque réseau exploitant le double-tagging pour accéder à un VLAN non autorisé
Router on a stick	Topologie classique : un routeur en trunk avec sous-interfaces par VLAN