

3.1	Modélisation de la topologie réseau dans EVE-NG	15
3.1.1	Configuration des équipements réseau	17
3.1.2	Configuration centralisée des VLANs avec VTP	18
3.1.3	Configuration des liaisons trunk et du VLAN natif	19
3.1.4	Configuration des Interfaces en Mode Access	20
3.1.5	Création et gestion des VLANs	20
3.1.6	Configuration d'EtherChannel avec LACP et PAgP	21
3.1.7	Configuration de MSTP	23
3.1.8	Configuration de VRRP	24
3.1.9	Configuration du protocole EIGRP	25
3.2	Conclusion	26
	Conclusion	26
4	Tests et Validation	27
4.1	Tests de Connectivité de Base	28
4.2	Tests EtherChannel	30
4.3	Tests MST (Multiple Spanning Tree)	36
4.4	Tests VRRP	40
4.5	Tests EIGRP	42
Annexe		48
1.	Installation de VMware Workstation Pro	48
2.	Intégration de l'image ISO d'EVE-NG sous VMware	49
3.	Installation de WinSCP	54
4.	Installation et utilisation de PuTTY	55
5.	Transfert des images Cisco IOL via WinSCP	57
6.	Installation du client Windows (client-side EVE-NG)	59

Table des figures

1.1	Logo de la SOTETEL.....	3
1.2	Organigramme de la SOTETEL.....	4
2.1	Architecture hiérarchique du réseau conçue sous Network Notepad Pro.....	9
2.2	Installation de VMware Workstation Pro	11
2.3	Adresse IP fournie par la machine virtuelle EVE-NG.....	12
2.4	Interface Web d'EVE-NG	12
2.5	Transfert des images Cisco IOL via WinSCP.....	12
2.6	Intégration et activation des images Cisco IOL dans EVE-NG	13
3.1	Modélisation de la topologie réseau dans EVE-NG	16
3.2	État VTP du serveur (CSWL3-01)	18
3.3	État VTP des commutateurs clients	19
3.4	Configuration type des interfaces trunk sur CSWL3-01.....	19
3.5	Configuration des interfaces en mode access sur les commutateurs d'accès	20
3.6	Création et gestion des VLANs sur le serveur VTP	21
3.7	État de fonctionnement de l'agrégation PAgP	22
3.8	État de fonctionnement de l'agrégation LACP	23
3.9	Configuration et validation du protocole MSTP	24
3.10	Configuration et validation de VRRP sur CSWL3-01 et CSWL3-02.....	25
3.11	Exemple de configuration EIGRP sur RouteurLAN1	26
4.1	Validation de la connectivité entre PC1 et PC6 au sein du VLAN 10	28
4.2	Validation de la connectivité entre PC2 et PC7 au sein du VLAN 20	29
4.3	Validation de la connectivité entre PC3 et PC8 au sein du VLAN 30	29
4.4	Validation de la connectivité inter-LAN	30
4.5	État du port-channel et des interfaces membres après création	31
4.6	Ping continu avant la défaillance d'un lien EtherChannel.....	32
4.7	Désactivation d'un lien membre de l'EtherChannel.....	33
4.8	Vérification de l'état du port-channel après la désactivation d'un lien	34
4.9	Ping continu pendant la désactivation d'un lien EtherChannel	35
4.10	Rétablissement du lien EtherChannel	36
4.11	Affichage initial des instances MST configurées	37
4.12	Désactivation d'un lien pour tester la convergence MSTP	38

4.13	État du MSTP après désactivation du lien	39
4.14	Analyse du ping capturé par Wireshark lors de la convergence MSTP	40
4.15	Identification des rôles Master et Backup sur les switches Core1	40
4.16	Identification des rôles Master et Backup sur les switches Core2	41
4.17	Ping avant et après désactivation du Master pour tester le basculement VRRP	41
4.18	Désactivation du routeur Master CSWL3-01	42
4.19	Basculement automatique sur CSWL3-02 après défaillance du Master	42
4.20	Voisinages EIGRP sur R-LAN1	43
4.21	Voisinages EIGRP sur R-LAN2	43
4.22	Voisinages EIGRP sur R-LAN3	43
4.23	Table de routage EIGRP sur R-LAN1	44
4.24	Table de routage EIGRP sur R-LAN2	44
4.25	Table de routage EIGRP sur R-LAN3	45
4.26	désactivation d'une interface sur R-LAN2	45
4.27	Ping continu pendant la désactivation du lien sur R-LAN2	46
4.28	Chemins alternatifs et redondance EIGRP	47
1	Lancement de l'installation de VMware Workstation Pro	48
2	Installation et configuration finale de VMware Workstation Pro	49
3	Configuration des ressources matérielles de la VM	50
4	Création de la machine virtuelle et choix de l'image ISO	51
5	Lancement de l'installation de EVE-NG	52
6	Choix de la langue d'installation	52
7	Définition du mot de passe administrateur	53
8	Attribution de l'adresse IP via DHCP	53
9	Adresse IP attribuée après installation	54
10	Lancement de l'installation de WinSCP	54
11	Interface de WinSCP après installation	55
12	Installation de PuTTY	55
13	Connexion SSH à EVE-NG avec PuTTY	56
14	Console de gestion de EVE-NG via PuTTY	56
15	Connexion à EVE-NG via WinSCP	57
16	Transfert des fichiers Cisco IOL vers EVE-NG	58
17	Configuration des permissions pour les binaires Cisco IOL	58
18	Téléchargement du package client-side depuis la documentation officielle EVE-NG	59
19	Lancement de l'installation du package client-side sur Windows	60

Liste des tableaux

3.1 Plan d'adressage IP des VLANs, switches et routeurs	17
---	----

Liste des abréviations

SOTETEL	Société Tunisienne d'Entreprises de Télécommunications
CPU	Central Processing Unit
EVE-NG	Emulated Virtual Environment - Next Generation
FTP	File Transfer Protocol
STP	Spanning Tree Protocol
MSTP	Multiple Spanning Tree Protocol
SFTP	SSH File Transfer Protocol
VRRP	Virtual Router Redundancy Protocol
MST	Multiple Spanning Tree
EIGRP	Enhanced Interior Gateway Routing Protocol
LACP	Link Aggregation Control Protocol
PAgP	Port Aggregation Protocol
VTP	VLAN Trunking Protocol
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
Ping	Packet Internet Groper
RAM	Random Access Memory
URL	Uniform Resource Locator
SSH	Secure Shell
VLAN	Virtual Local Area Network
VM	Virtual Machine

Chapitre 2

Mise en place de l'infrastructure

Sommaire

3 introduction	15
2.2 Architecture de l'infrastructure proposée	9
2.2.1 Installation et configuration de VMware Workstation Pro	10
2.2.2 Installation et configuration de EVE-NG	11
2.2.3 Transfert des images Cisco IOL via WinSCP	12
2.2.4 Hébergement et activation des images Cisco IOL	13
2.3 Conclusion	13

2.1 Introduction

Ce chapitre a pour objet de présenter l'architecture globale du projet ainsi que l'environnement matériel et logiciel déployé pour sa réalisation. La mise en œuvre de la solution repose sur une approche structurée et modulaire, débutant par la configuration de l'environnement de virtualisation. Celui-ci s'appuie sur VMware Workstation Pro pour l'hébergement et sur la plateforme EVE-NG pour l'émulation des équipements réseau, utilisant des images Cisco IOL pour simuler des routeurs et commutateurs. WinSCP a été intégré afin de garantir le transfert sécurisé des fichiers de configuration. Sur cette base, la topologie réseau a été conçue selon une architecture hiérarchique à trois niveaux (Cœur, Distribution, Accès) et implémentée grâce à la configuration de plusieurs protocoles essentiels : VTP pour une gestion centralisée des VLANs, MSTP pour la redondance et la prévention des boucles, EtherChannel pour l'agrégation de liens, VRRP pour la redondance de passerelle par défaut, et EIGRP pour assurer un routage dynamique efficace entre les sous-réseaux. Ce chapitre détaille également les choix techniques, la logique d'interconnexion des équipements et les différentes étapes de déploiement de l'infrastructure.

2.2 Architecture de l'infrastructure proposée

L'architecture déployée dans le cadre de ce projet s'appuie sur le modèle hiérarchique à trois couches (Core, Distribution, Accès), une référence éprouvée dans la conception de réseaux d'entreprise évolutifs et résilients. Chaque niveau assume des fonctions réseau spécifiques et complémentaires, permettant une segmentation claire des responsabilités et une optimisation des flux. La Figure 2.1 illustre cette structure, mettant en évidence l'interconnexion logique et physique des équipements virtualisés sous EVE-NG.

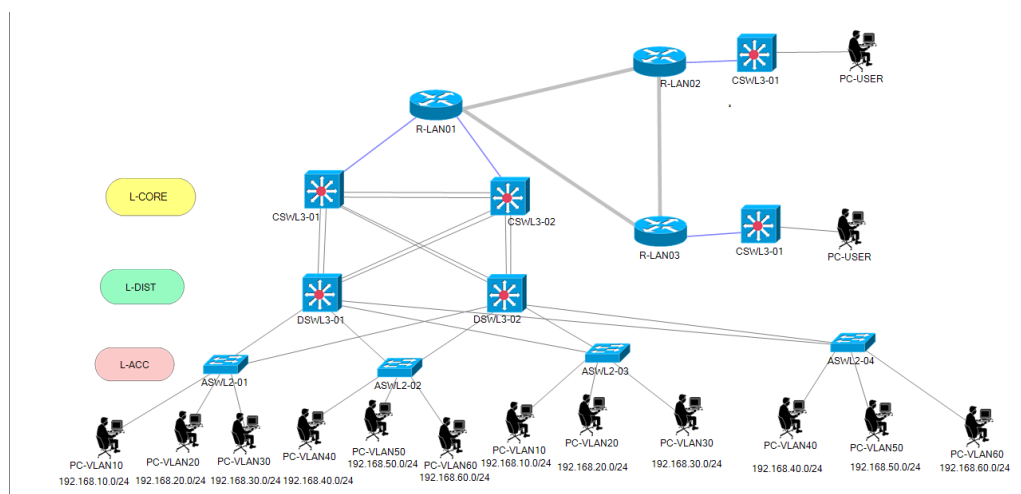


FIGURE 2.1 – Architecture hiérarchique du réseau conçue sous Network Notepad Pro

Couche Core (L-CORE)

Cette couche constitue le fondement du réseau et assure la haute performance ainsi que la transitivité du trafic entre les différents segments. Elle a été configurée avec le protocole **EIGRP** pour garantir un routage dynamique, une convergence rapide et une gestion efficace des routes entre les VLANs et les sites interconnectés.

Couche Distribution (L-DIST)

Positionnée en intermédiaire entre le cœur et les accès, cette couche intègre les mécanismes de résilience et de gestion de la redondance. Le protocole **VRRP** a été configuré pour assurer la haute disponibilité des passerelles, tandis que **MSTP** (Multiple Spanning Tree Protocol) a été déployé pour optimiser les chemins redondants et prévenir toute boucle de niveau 2.

Couche Accès (L-ACC)

Dédiée à la connexion des utilisateurs finaux, cette couche assure la segmentation logique via les VLANs. La gestion centralisée de ces VLANs est assurée par **VTP** (VLAN Trunking Protocol). Par ailleurs, l'agrégation de liens redondants a été renforcée via **EtherChannel**, avec support des protocoles **PAgP** (Cisco propriétaire) et **LACP** (standard IEEE), améliorant ainsi la bande passante et la tolérance aux pannes.

Cette architecture structurée permet non seulement une segmentation claire des fonctions réseau, mais également une évolutivité aisée et une maintenance simplifiée, tout en offrant un cadre propice à l'intégration de services avancés.

2.2.1 Installation et configuration de VMware Workstation Pro

La mise en place de l'environnement de virtualisation a reposé sur l'utilisation de VMware Workstation Pro en tant qu'hyperviseur de type 2. Cette solution a été retenue pour sa stabilité, sa compatibilité étendue et ses fonctionnalités avancées dédiées aux environnements de test et de développement.

Le processus d'installation a débuté par le téléchargement de l'installateur depuis le site officiel de VMware, assurant ainsi l'authenticité et l'intégrité du logiciel. L'installation s'est déroulée comme suit : - Acceptation du contrat de licence utilisateur ; - Choix du chemin d'installation ; - Saisie de la clé de licence pour activer la version Professionnelle.

Une fois l'installation finalisée, une machine virtuelle dédiée a été créée pour héberger la plateforme d'émulation ****EVE-NG****. Les ressources allouées ont été dimensionnées pour répondre aux besoins du projet : - 2 processeurs virtuels ; - 4 Go de mémoire RAM ; - 150 Go d'espace disque en mode alloué dynamiquement ; - Une interface réseau configurée en mode NAT pour permettre l'accès à Internet tout en isolant le réseau virtuel.

Cette configuration, bien que modeste, s'est avérée suffisante pour exécuter les scénarios de simulation prévus, tout en garantissant des performances stables. Après la création de la

machine virtuelle, un démarrage initial a été effectué pour vérifier son bon fonctionnement et sa compatibilité avec le système hôte.

Cette étape a constitué la fondation indispensable au déploiement ultérieur de l'infrastructure d'émulation, comme le montre la Figure 2.2. Pour des instructions détaillées sur l'installation et la configuration de VMware Workstation Pro, se référer à l'Annexe – Section A.1.

Procédure complète d'installation et de configuration de l'hyperviseur VMware Workstation Pro, incluant les paramètres optimisés pour la virtualisation réseau.

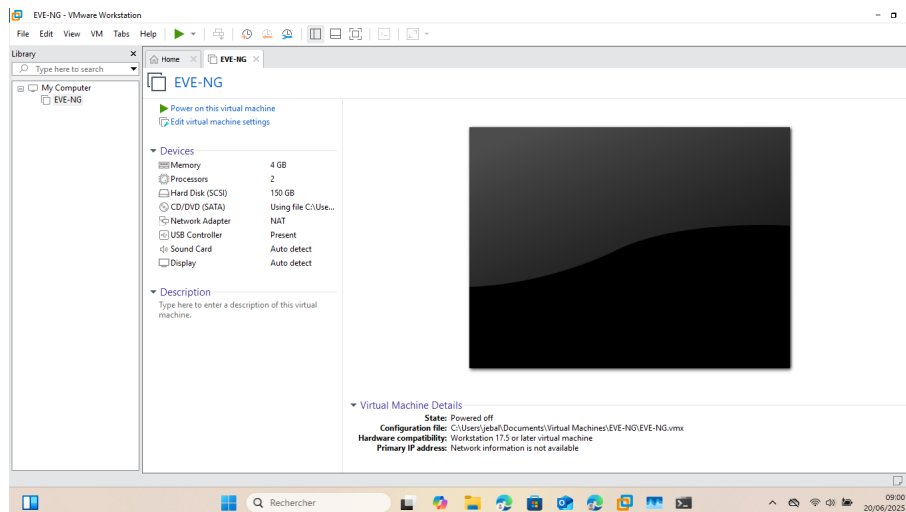


FIGURE 2.2 – Installation de VMware Workstation Pro

2.2.2 Installation et configuration de EVE-NG

Suite à la préparation de la machine virtuelle sous VMware Workstation Pro, l'installation de la plateforme d'émulation EVE-NG Community Edition a été réalisée à partir de l'image ISO officielle. Le processus d'installation a inclus la configuration des paramètres système de base : Définition du fuseau horaire (UTC+1) ; Attribution d'un nom d'hôte ; Définition d'un mot de passe sécurisé pour le compte administrateur ; Configuration des paramètres réseau en mode DHCP pour une intégration simplifiée.

Après l'achèvement de l'installation et le redémarrage du système, la machine virtuelle a obtenu automatiquement une adresse IP via le mécanisme NAT de VMware, comme illustré dans la Figure 2.3. J'ai utilisé cette adresse pour accéder à l'interface web d'EVE-NG via un navigateur, tel que montré dans la Figure 2.4. Cette étape a permis de valider l'accessibilité à l'interface de gestion et de finaliser la configuration de la plateforme. Les informations détaillées concernant cette installation sont accessibles dans l'Annexe A

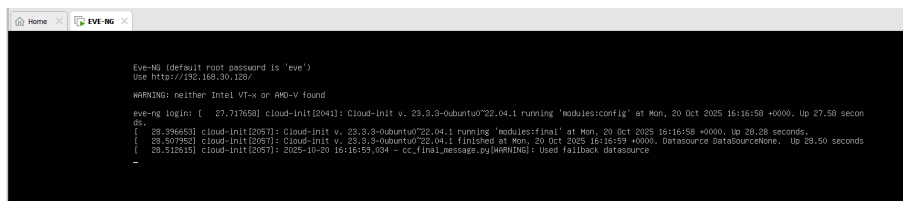


FIGURE 2.3 – Adresse IP fournie par la machine virtuelle EVE-NG

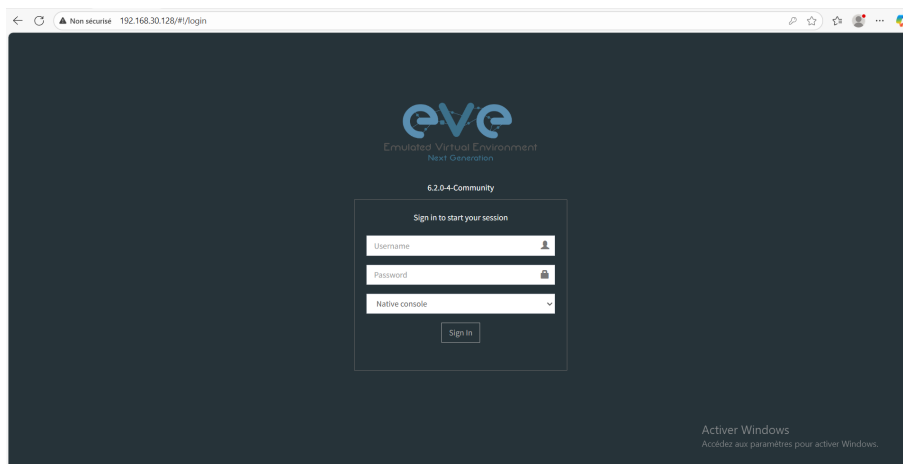


FIGURE 2.4 – Interface Web d'EVE-NG

2.2.3 Transfert des images Cisco IOL via WinSCP

Transfert des images Cisco IOL via WinSCP

Le transfert des images Cisco IOL s'effectue via une connexion SFTP sécurisée à l'aide de WinSCP, comme illustré dans la Figure 2.5

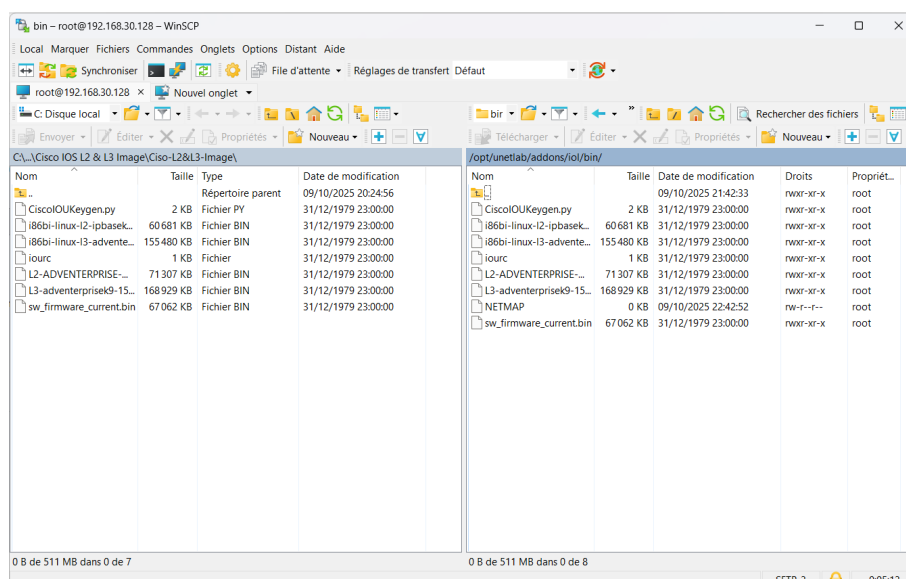
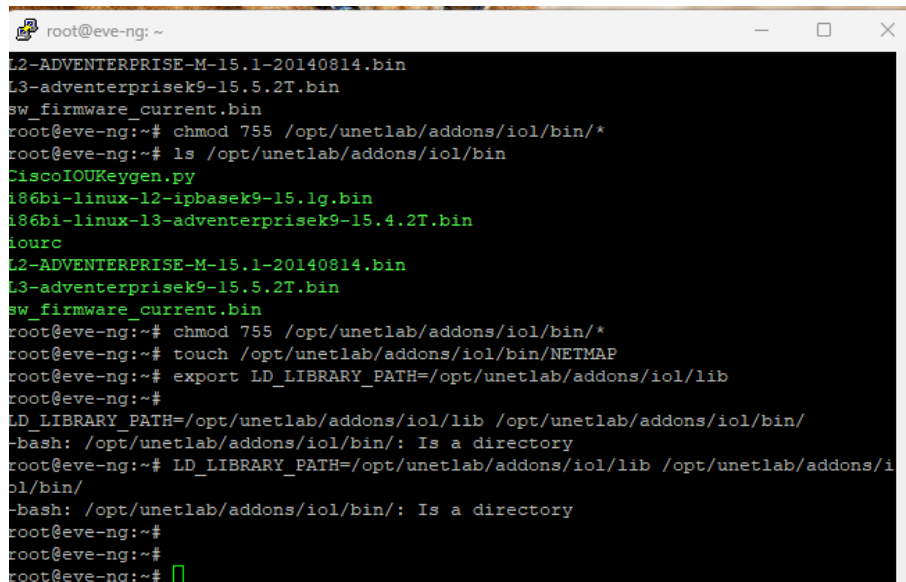


FIGURE 2.5 – Transfert des images Cisco IOL via WinSCP

2.2.4 Hébergement et activation des images Cisco IOL

Intégration et activation des images Cisco IOL

La Figure 2.6 présente la séquence complète des commandes d'activation exécutées dans le terminal EVE-NG après le transfert des images.



```
root@eve-ng: ~  
L2-ADVENTERPRISE-M-15.1-20140814.bin  
L3-adventerprisek9-15.5.2T.bin  
sw_firmware_current.bin  
root@eve-ng:~# chmod 755 /opt/unetlab/addons/iol/bin/*  
root@eve-ng:~# ls /opt/unetlab/addons/iol/bin  
CiscoIOUKeygen.py  
i86bi-linux-l2-ipbasek9-15.1g.bin  
i86bi-linux-l3-adventerprisek9-15.4.2T.bin  
iourc  
L2-ADVENTERPRISE-M-15.1-20140814.bin  
L3-adventerprisek9-15.5.2T.bin  
sw_firmware_current.bin  
root@eve-ng:~# chmod 755 /opt/unetlab/addons/iol/bin/*  
root@eve-ng:~# touch /opt/unetlab/addons/iol/bin/NETMAP  
root@eve-ng:~# export LD_LIBRARY_PATH=/opt/unetlab/addons/iol/lib  
root@eve-ng:~#  
LD_LIBRARY_PATH=/opt/unetlab/addons/iol/lib /opt/unetlab/addons/iol/bin/  
-bash: /opt/unetlab/addons/iol/bin/: Is a directory  
root@eve-ng:~# LD_LIBRARY_PATH=/opt/unetlab/addons/iol/lib /opt/unetlab/addons/i  
ol/bin/  
-bash: /opt/unetlab/addons/iol/bin/: Is a directory  
root@eve-ng:~#  
root@eve-ng:~#  
root@eve-ng:~#
```

FIGURE 2.6 – Intégration et activation des images Cisco IOL dans EVE-NG

2.3 Conclusion

Ce chapitre a décrit la mise en place de l'environnement matériel et logiciel nécessaire à la virtualisation d'une infrastructure réseau hiérarchique. L'association de VMware Workstation Pro et d'EVE-NG a constitué la base d'un laboratoire virtuel performant, permettant l'expérimentation et la configuration de scénarios réseau complexes.

Les différentes étapes d'installation et de configuration, incluant l'utilisation de WinSCP pour le transfert sécurisé des images Cisco IOL et la configuration des éléments virtuels, ont établi les fondations techniques essentielles à ce projet. Ces préparatifs ont abouti à la création d'une plateforme d'émulation fidèle reproduisant les caractéristiques d'une architecture réseau complète.

Cette infrastructure virtualisée offre désormais un environnement propice au test des fonctionnalités avancées telles que le routage dynamique, les mécanismes de redondance et l'agrégation de liens. Le chapitre suivant détaillera la mise en œuvre opérationnelle de cette architecture et les configurations spécifiques appliquées à chaque couche du réseau.

Chapitre 3

Déploiement et réalisation du projet

Sommaire

3 Introduction	15
3.1 Modélisation de la topologie réseau dans EVE-NG	15
3.1.1 Configuration des équipements réseau	17
3.1.2 Configuration centralisée des VLANs avec VTP	18
3.1.3 Configuration des liaisons trunk et du VLAN natif	19
3.1.4 Configuration des interfaces en mode access	20
3.1.5 Création et gestion des VLANs	20
3.1.6 Configuration d’EtherChannel avec LACP et PAgP	21
3.1.7 Configuration de MSTP	23
3.1.8 Configuration de VRRP	24
3.1.9 Configuration du protocole EIGRP	25
4.5 Conclusion	47

Introduction

Ce chapitre expose la mise en œuvre technique de l'architecture réseau hiérarchique conçue pour ce projet. La réalisation inclut le déploiement de la topologie, la configuration des équipements et l'intégration des protocoles retenus.

L'infrastructure a été structurée selon le modèle triple niveau (Core, Distribution, Accès), chaque couche faisant l'objet d'une configuration progressive intégrant les protocoles essentiels : VTP pour la gestion centralisée des VLANs, MSTP pour la prévention des boucles, EtherChannel (modes LACP et PAgP) pour l'agrégation de liens, et le routage inter-VLAN.

Les sections suivantes décrivent de manière méthodique l'ensemble du processus, s'appuyant sur des schémas architecturaux, des extraits de configuration et des résultats de validation technique, assurant ainsi une documentation complète et reproductible de l'implémentation.

3.1 Modélisation de la topologie réseau dans EVE-NG

La modélisation de la topologie réseau a été réalisée dans EVE-NG après l'installation de la plateforme et l'intégration des images Cisco IOL. Conformément à l'architecture cible, une maquette virtuelle a été développée suivant une structure hiérarchique à trois niveaux.

La couche **Core (L-CORE)** comprend deux commutateurs Layer 3 (CSWL3-01 et CSWL3-02) assurant le routage inter-VLAN et l'interconnexion avec les routeurs distants.

La couche **Distribution (L-DIST)** intègre deux commutateurs (DSWL3-01 et DSWL3-02) assurant la liaison entre les couches Accès et Core ainsi que la gestion des politiques de routage et de redondance.

La couche **Accès (L-ACC)** est constituée de quatre commutateurs Layer 2 (ASWL2-01 à ASWL2-04) connectant les postes utilisateurs répartis sur six VLANs (VLAN10 à VLAN60).

Tous les équipements ont été interconnectés manuellement dans EVE-NG selon le schéma directeur, permettant de valider l'organisation logique du réseau avant la configuration avancée, comme illustré dans la Figure 3.1. Cette modélisation préalable établit une base solide pour le déploiement des protocoles et services réseau.

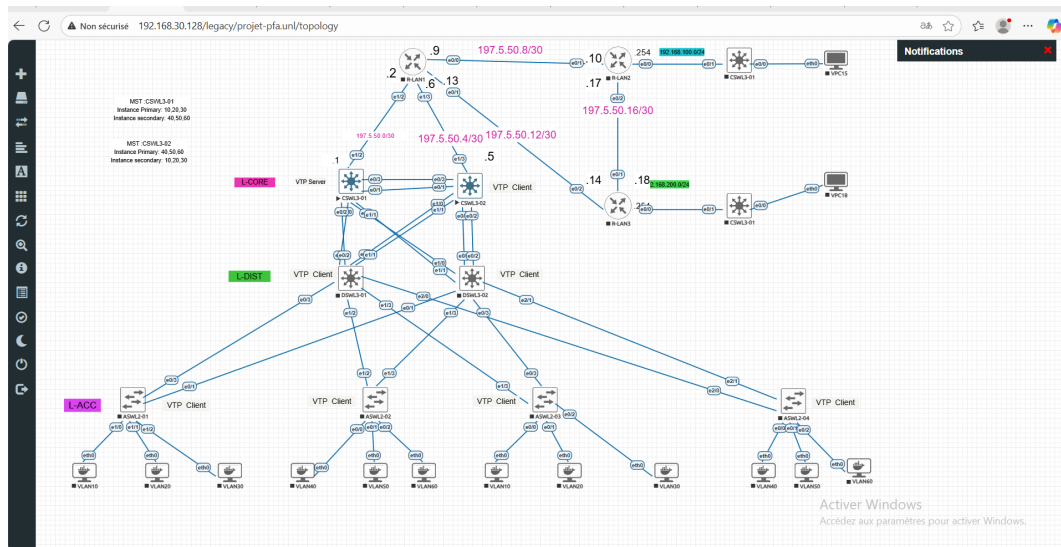


FIGURE 3.1 – Modélisation de la topologie réseau dans EVE-NG

TABLE 3.1 – Plan d’adressage IP des VLANs, switches et routeurs

VLAN / Réseau	Description	Equipement / Interface	IP Adresse	Masque	Passerelle	Commentaires
VLAN 10	Management	CSWL3-01	192.168.10.10	/24	192.168.10.1 (VRRP)	Switch Core
VLAN 10	Management	CSWL3-02	192.168.10.11	/24	192.168.10.1 (VRRP)	Switch Core
VLAN 10	Management	ACC01-02 VPC	192.168.10.12	/24	192.168.10.1	Accès utilisateur
VLAN 10	Management	ACC03 VPC	192.168.10.13	/24	192.168.10.1	Accès utilisateur
VLAN 20	Sales	CSWL3-01	192.168.20.10	/24	192.168.20.1 (VRRP)	Switch Core
VLAN 20	Sales	CSWL3-02	192.168.20.11	/24	192.168.20.1 (VRRP)	Switch Core
VLAN 20	Sales	ACC01-02 VPC	192.168.20.12	/24	192.168.20.1	Accès utilisateur
VLAN 20	Sales	ACC03 VPC	192.168.20.13	/24	192.168.20.1	Accès utilisateur
VLAN 30	IT	CSWL3-01	192.168.30.10	/24	192.168.30.1 (VRRP)	Switch Core
VLAN 30	IT	CSWL3-02	192.168.30.11	/24	192.168.30.1 (VRRP)	Switch Core
VLAN 30	IT	ACC01-02 VPC	192.168.30.12	/24	192.168.30.1	Accès utilisateur
VLAN 30	IT	ACC03 VPC	192.168.30.13	/24	192.168.30.1	Accès utilisateur
VLAN 40	Admin	CSWL3-01	192.168.40.10	/24	192.168.40.1 (VRRP)	Switch Core
VLAN 40	Admin	CSWL3-02	192.168.40.11	/24	192.168.40.1 (VRRP)	Switch Core
VLAN 40	Admin	ACC01-02 VPC	192.168.40.12	/24	192.168.40.1	Accès utilisateur
VLAN 40	Admin	ACC03 VPC	192.168.40.13	/24	192.168.40.1	Accès utilisateur
VLAN 50	Guests	CSWL3-01	192.168.50.10	/24	192.168.50.1 (VRRP)	Switch Core
VLAN 50	Guests	CSWL3-02	192.168.50.11	/24	192.168.50.1 (VRRP)	Switch Core
VLAN 50	Guests	ACC01-02 VPC	192.168.50.12	/24	192.168.50.1	Accès utilisateur
VLAN 50	Guests	ACC03 VPC	192.168.50.13	/24	192.168.50.1	Accès utilisateur
VLAN 60	Servers	CSWL3-01	192.168.60.10	/24	192.168.60.1 (VRRP)	Switch Core
VLAN 60	Servers	CSWL3-02	192.168.60.11	/24	192.168.60.1 (VRRP)	Switch Core
VLAN 60	Servers	ACC01-02 VPC	192.168.60.12	/24	192.168.60.1	Accès utilisateur
VLAN 60	Servers	ACC03 VPC	192.168.60.13	/24	192.168.60.1	Accès utilisateur
Trunk / Core	Inter-CSWL3	CSWL3-01 E1/2	197.5.50.1	/30	-	Vers CSWL3-02
Trunk / Core	Inter-CSWL3	CSWL3-02 E1/3	197.5.50.5	/30	-	Vers CSWL3-01
R-lan1	WAN / Interconnexion	E1/2	197.5.50.2	/30	-	Vers CSWL3-01
R-lan1	WAN / Interconnexion	E1/3	197.5.50.6	/30	-	Vers CSWL3-02
R-lan1	LAN	E0/0	197.5.50.9	/30	-	Vers R-lan2
R-lan1	LAN	E0/0	197.5.50.13	/30	-	Vers R-lan3
R-lan2	WAN / Interconnexion	E0/1	197.5.50.10	/30	-	Vers R-lan1
R-lan2	WAN / Interconnexion	E0/2	197.5.50.17	/30	-	Vers R-lan3
R-lan2	LAN	E0/0	192.168.100.1	/24	-	LAN VPC15
R-lan3	WAN / Interconnexion	E0/1	197.5.50.18	/30	-	Vers R-lan2
R-lan3	WAN / Interconnexion	E0/2	197.5.50.14	/30	-	Vers R-lan1
R-lan3	LAN	E0/0	192.168.200.1	/24	-	LAN VPC18
VPC15	LAN	-	192.168.100.2	/24	192.168.100.1	Connecté R-lan2
VPC18	LAN	-	192.168.200.2	/24	192.168.200.1	Connecté R-lan3

3.1.1 Configuration des équipements réseau

Suite à la modélisation de la topologie, la configuration des équipements réseau virtualisés dans EVE-NG a été réalisée selon une méthodologie structurée. Cette phase comprend la configuration de base des commutateurs et routeurs (attribution des noms d’hôte, configuration des interfaces, définition des VLANs et établissement des liaisons trunk), l’activation des protocoles essentiels (VTP, MSTP, EtherChannel, VRRP, EIGRP), ainsi que la mise en place du routage inter-VLAN et du routage dynamique.

La configuration a été exécutée de manière hiérarchique, en débutant par la couche **Core**. Les commutateurs CSWL3-01 et CSWL3-02 ont été configurés avec les VLANs nécessaires, les interfaces trunk, le routage inter-VLAN, et le rôle de VTP **Server** assigné à CSWL3-01.

La couche **Distribution** a ensuite été paramétrée avec l’activation du mode VTP **Client**, la

configuration des agrégations de liens EtherChannel pour la redondance, et l'implémentation du protocole de routage EIGRP.

Enfin, la couche **Accès** a été configurée avec la définition des ports en mode access, l'affectation aux VLANs appropriés, et la participation au domaine VTP en mode Client. Cette approche méthodique garantit une configuration cohérente et optimisée de l'ensemble de l'infrastructure réseau.

Annexe : Les configurations détaillées des équipements sont disponibles en section 5.2 du présent rapport.

3.1.2 Configuration centralisée des VLANs avec VTP

La gestion des VLANs a été optimisée grâce à l'implémentation du protocole VTP (VLAN Trunking Protocol), permettant une administration centralisée et synchronisée sur l'ensemble des équipements.

Le commutateur CSWL3-01 a été désigné comme **serveur VTP**, assurant la propagation automatique de la base de données VLAN vers tous les commutateurs clients de la topologie.

Tous les autres commutateurs (CSWL3-02, DSWL3-01, DSWL3-02, ASWL2-01 à ASWL2-04) ont été configurés en **mode client VTP**, permettant une synchronisation complète de la configuration VLAN sur l'ensemble du réseau.

Cette approche élimine les risques d'incohérence de configuration et simplifie la maintenance de l'infrastructure réseau. La configuration a été sécurisée par un domaine VTP authentifié et la version 3 du protocole a été adoptée pour bénéficier de ses fonctionnalités avancées.

Les Figures 3.2 et 3.3 présentent respectivement les états VTP du serveur et des clients, confirmant la synchronisation réussie de la configuration VLAN sur l'ensemble du domaine.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname CSWL3-01
CSWL3-01(config)#vtp mode server
Device mode already VTP Server for VLANs.
CSWL3-01(config)#vtp domain salsabil.local
Changing VTP domain name from NULL to salsabil.local
CSWL3-01(config)#
*Jul 18 09:55:17.379: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to
salsabil.local.
CSWL3-01(config)#vtp password isikef
Setting device VTP password to isikef
CSWL3-01(config)#vtp version 3
CSWL3-01(config)#
*Jul 18 09:55:54.037: %SW_VLAN-6-OLD_CONFIG_FILE_READ: Old version 2 VLAN config
uration file detected and read OK.  Version 3
files will be written in the future.
CSWL3-01(config)#
```

FIGURE 3.2 – État VTP du serveur (CSWL3-01)


```

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname CSWL3-02
CSWL3-02(config)#vtp mode client
Setting device to VTP Client mode for VLANs.
CSWL3-02(config)#vtp domain salsabil.local
Changing VTP domain name from NULL to salsabil.local
CSWL3-02(config)#
*Jul 18 09:59:52.097: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to
salsabil.local.
CSWL3-02(config)#vtp password isikef
Setting device VTP password to isikef
CSWL3-02(config)#vtp password isikef
Password already set to isikef
CSWL3-02(config)#vtp version 3
CSWL3-02(config)#exi
CSWL3-02#wr
*Jul 18 10:00:53.010: %SYS-5-CONFIG_I: Configured from console by console
CSWL3-02#wr
Building configuration...
Compressed configuration from 2364 bytes to 895 bytes[OK]
CSWL3-02#

```

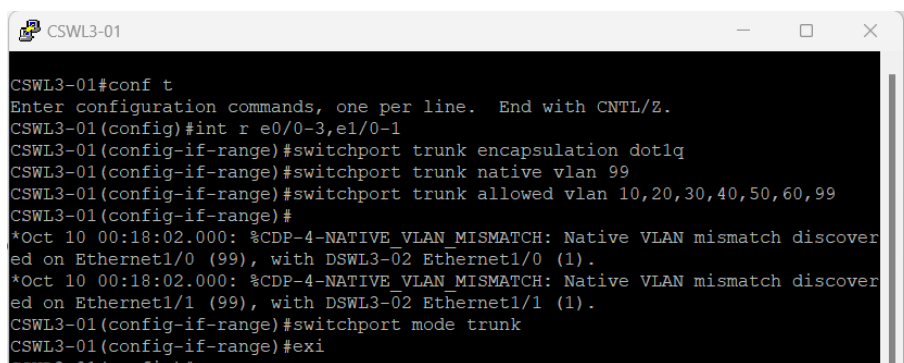
FIGURE 3.3 – État VTP des commutateurs clients

3.1.3 Configuration des liaisons trunk et du VLAN natif

La configuration des liaisons trunk a été systématiquement déployée sur l'ensemble des commutateurs pour assurer le transport multiservices des VLANs entre les différentes couches de l'infrastructure. Les interconnexions entre les équipements de cœur (CSWL3-01, CSWL3-02), de distribution (DSWL3-01, DSWL3-02) et d'accès (ASWL2-01 à ASWL2-04) ont été configurées avec le protocole IEEE 802.1Q, garantissant une encapsulation standardisée des trames VLAN.

Le VLAN 99 a été spécifiquement désigné comme VLAN natif sur l'ensemble des liaisons trunk, tandis qu'une liste restrictive de VLANs autorisés (10, 20, 30, 40, 50, 60 et 99) a été appliquée pour optimiser la sécurité et le contrôle du trafic. Cette approche permet de maintenir la cohérence de la propagation VLAN dans le domaine VTP tout en limitant la diffusion des *broadcast* à des segments réseau non concernés.

Comme illustré dans la Figure 3.4, la configuration type implémentée sur CSWL3-01 a été répliquée de manière homogène sur l'ensemble des interfaces trunk de l'infrastructure, assurant ainsi une gestion uniforme et simplifiée des interconnexions entre équipements.



```

CSWL3-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CSWL3-01(config)#int r e0/0-3,e1/0-1
CSWL3-01(config-if-range)#switchport trunk encapsulation dot1q
CSWL3-01(config-if-range)#switchport trunk native vlan 99
CSWL3-01(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,60,99
CSWL3-01(config-if-range)#
*Oct 10 00:18:02.000: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered
on Ethernet1/0 (99), with DSWL3-02 Ethernet1/0 (1).
*Oct 10 00:18:02.000: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered
on Ethernet1/1 (99), with DSWL3-02 Ethernet1/1 (1).
CSWL3-01(config-if-range)#switchport mode trunk
CSWL3-01(config-if-range)#exi

```

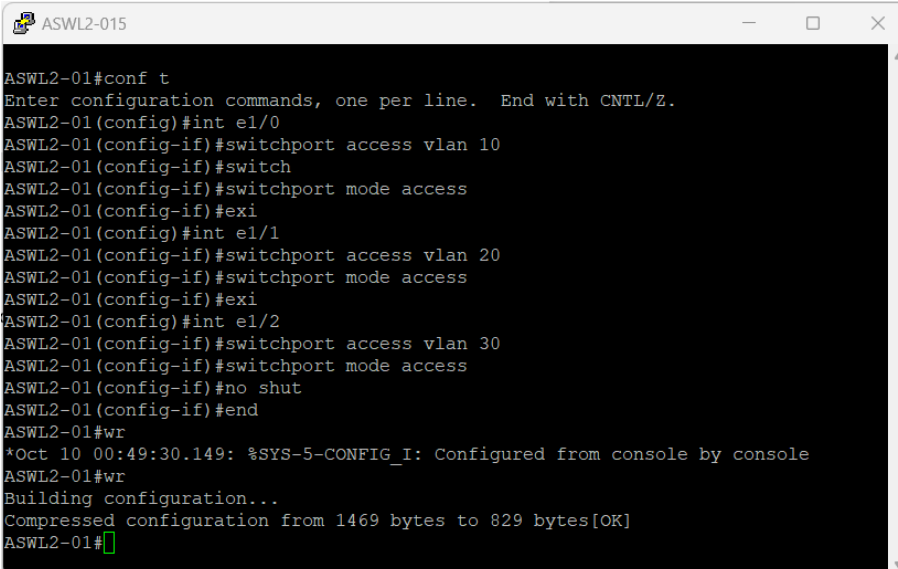
FIGURE 3.4 – Configuration type des interfaces trunk sur CSWL3-01

3.1.4 Configuration des Interfaces en Mode Access

Suite à la création et à la propagation des VLANs dans le domaine VTP, la configuration des interfaces en mode access a été réalisée sur les commutateurs de la couche Accès. Cette étape cruciale permet d'affecter chaque port à un VLAN spécifique selon le type de périphérique terminal connecté (poste utilisateur, imprimante, point d'accès sans fil, etc.).

Cette configuration assure une segmentation logique du réseau alignée avec les besoins opérationnels, tout en renforçant la sécurité en prévenant toute transformation accidentelle des ports en mode trunk. L'approche adoptée respecte les meilleures pratiques industrielles pour garantir une infrastructure stable, segmentée et optimisée.

Comme illustré dans la Figure 3.5, les ports des commutateurs d'accès ASWL2-01 à ASWL2-04 ont été configurés pour associer chaque interface à un VLAN spécifique, permettant ainsi une isolation efficace des flux et une gestion granulaire des politiques de sécurité. Cette configuration participe à la création d'un environnement réseau robuste et adapté aux exigences de l'organisation.



```
ASWL2-01#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ASWL2-01(config)#int e1/0
ASWL2-01(config-if)#switchport access vlan 10
ASWL2-01(config-if)#switch
ASWL2-01(config-if)#switchport mode access
ASWL2-01(config-if)#exi
ASWL2-01(config)#int e1/1
ASWL2-01(config-if)#switchport access vlan 20
ASWL2-01(config-if)#switchport mode access
ASWL2-01(config-if)#exi
ASWL2-01(config)#int e1/2
ASWL2-01(config-if)#switchport access vlan 30
ASWL2-01(config-if)#switchport mode access
ASWL2-01(config-if)#no shut
ASWL2-01(config-if)#end
ASWL2-01#wr
*Oct 10 00:49:30.149: %SYS-5-CONFIG_I: Configured from console by console
ASWL2-01#wr
Building configuration...
Compressed configuration from 1469 bytes to 829 bytes[OK]
ASWL2-01#
```

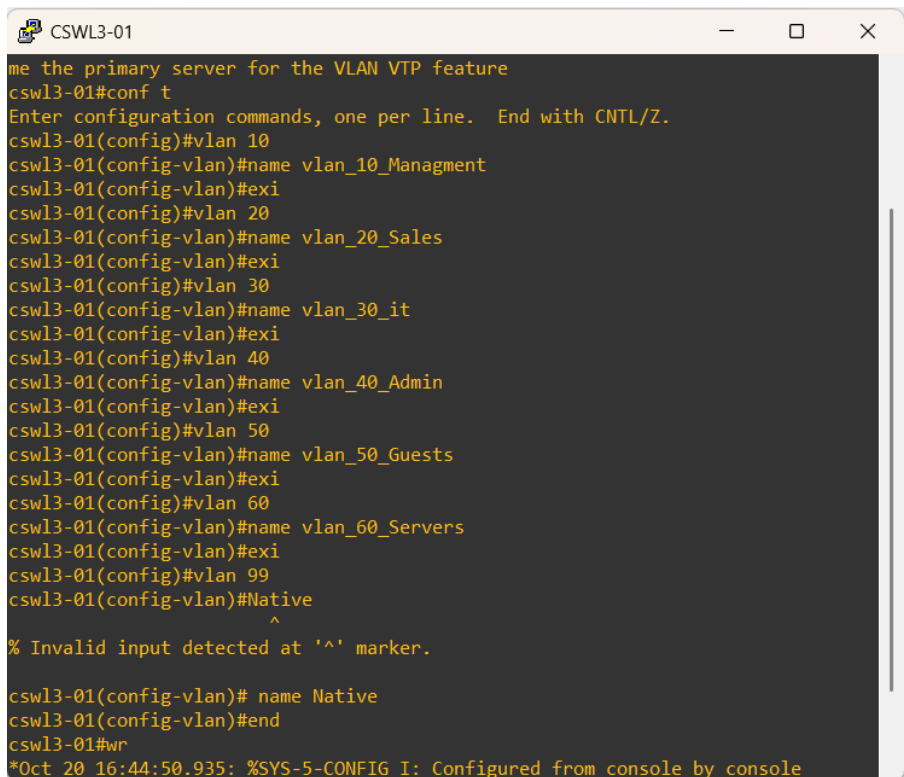
FIGURE 3.5 – Configuration des interfaces en mode access sur les commutateurs d'accès

3.1.5 Création et gestion des VLANs

La segmentation logique du réseau a été implémentée par la création des VLANs sur le commutateur principal CSWL3-01, configuré en mode serveur VTP. Cette approche permet de structurer l'infrastructure en domaines de diffusion distincts, alignés sur les besoins organisationnels et les profils des utilisateurs.

La configuration manuelle des VLANs sur CSWL3-01 assure une gestion centralisée et cohérente, avec une propagation automatique vers l'ensemble des commutateurs clients du domaine VTP. Chaque VLAN a été configuré avec un identifiant unique et une description fonctionnelle, facilitant ainsi la maintenance et l'administration du réseau.

Comme illustré dans la Figure 3.6, cette méthodologie garantit une mise en œuvre efficace et scalable de la segmentation VLAN, tout en optimisant la sécurité et la performance du réseau grâce à l'isolation logique des flux.



```
me the primary server for the VLAN VTP feature
cswl3-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cswl3-01(config)#vlan 10
cswl3-01(config-vlan)#name vlan_10_Managment
cswl3-01(config-vlan)#exi
cswl3-01(config)#vlan 20
cswl3-01(config-vlan)#name vlan_20_Sales
cswl3-01(config-vlan)#exi
cswl3-01(config)#vlan 30
cswl3-01(config-vlan)#name vlan_30_it
cswl3-01(config-vlan)#exi
cswl3-01(config)#vlan 40
cswl3-01(config-vlan)#name vlan_40_Admin
cswl3-01(config-vlan)#exi
cswl3-01(config)#vlan 50
cswl3-01(config-vlan)#name vlan_50_Guests
cswl3-01(config-vlan)#exi
cswl3-01(config)#vlan 60
cswl3-01(config-vlan)#name vlan_60_Servers
cswl3-01(config-vlan)#exi
cswl3-01(config)#vlan 99
cswl3-01(config-vlan)#Native
^
% Invalid input detected at '^' marker.
cswl3-01(config-vlan)# name Native
cswl3-01(config-vlan)#end
cswl3-01#wr
*Oct 20 16:44:50.935: %SYS-5-CONFIG_I: Configured from console by console
```

FIGURE 3.6 – Création et gestion des VLANs sur le serveur VTP

3.1.6 Configuration d'EtherChannel avec LACP et PAgP

La technologie EtherChannel a été déployée sur les interconnexions critiques entre les commutateurs de cœur et de distribution afin d'optimiser la bande passante et d'assurer la redondance des liaisons. Deux protocoles d'agrégation ont été implémentés : **PAgP** (Port Aggregation Protocol) pour les liaisons entre équipements Cisco exclusifs, et **LACP** (Link Aggregation Control Protocol) pour les interconnexions nécessitant une compatibilité multi-vendeurs.

Chaque canal logique a été configuré avec une interface `Port-channel` dédiée, utilisant l'encapsulation `802.1Q`, le VLAN natif 99, et une liste restreinte de VLANs autorisés. Cette configuration permet une augmentation significative de la bande passante tout en maintenant une topologie dépourvue de boucles.

Comme illustré dans les Figures 3.7 et 3.8, les états de fonctionnement des agrégations **PAgP** et **LACP** confirment la mise en service réussie des liens et la répartition optimale du trafic sur les interfaces membres.

```

CSWL3-02
CSWL3-02>en
CSWL3-02#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CSWL3-02(config)#int r e1/0,e1/1
CSWL3-02(config-if-range)#channel-protocol pagp
CSWL3-02(config-if-range)#channel-group 2 mode auto
Creating a port-channel interface Port-channel 2

CSWL3-02(config-if-range)#
*Oct 10 01:50:40.541: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
0, changed state to down
*Oct 10 01:50:40.541: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
1, changed state to down
CSWL3-02(config-if-range)#
*Oct 10 01:50:41.698: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
1, changed state to up
*Oct 10 01:50:41.699: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
0, changed state to up
CSWL3-02(config-if-range)#exi
CSWL3-02(config)#int port-channel 2
CSWL3-02(config-if)#
*Oct 10 01:50:57.310: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-chann
el2, changed state to up
CSWL3-02(config-if)#switchport mode trunk
CSWL3-02(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,99
CSWL3-02(config-if)#no shut
CSWL3-02(config-if)#end
CSWL3-02#
*Oct 10 01:51:41.686: %SYS-5-CONFIG_I: Configured from console by console
CSWL3-02#wr
Building configuration...
Compressed configuration from 2184 bytes to 1084 bytes[OK]
CSWL3-02#

```

FIGURE 3.7 – État de fonctionnement de l'agrégation PAgP

```
CSWL3-01
CSWL3-01>en
CSWL3-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CSWL3-01(config)#int range e1/0,e1/0
CSWL3-01(config-if-range)#channel-protocol lacp
CSWL3-01(config-if-range)#channel-group 4 mode active
Creating a port-channel interface Port-channel 4

CSWL3-01(config-if-range)#exi
CSWL3-01(config)#
*Oct 10 02:03:29.607: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
0, changed state to down
CSWL3-01(config)#int port-channel
*Oct 10 02:03:37.033: %EC-5-L3DONTBNDL2: Et1/0 suspended: LACP currently not ena
bled on the remote port.
CSWL3-01(config)#int port-channel 4
CSWL3-01(config-if)#
*Oct 10 02:03:38.573: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
0, changed state to up
CSWL3-01(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be co
nfigured to "trunk" mode.
CSWL3-01(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,99
^
% Invalid input detected at '^' marker.

CSWL3-01(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,99
CSWL3-01(config-if)#no shut
CSWL3-01(config-if)#end
CSWL3-01#wr
*Oct 10 02:04:31.981: %SYS-5-CONFIG_I: Configured from console by console
CSWL3-01#wr
Building configuration...
Compressed configuration from 2336 bytes to 1143 bytes[OK]
CSWL3-01#
```

FIGURE 3.8 – État de fonctionnement de l'agrégation LACP

3.1.7 Configuration de MSTP

Le protocole MSTP a été déployé sur l'ensemble des commutateurs pour optimiser la résilience du réseau et la gestion de la redondance. Cette implémentation permet de regrouper les VLANs en deux instances distinctes : l'instance 1 pour les VLANs 10, 20 et 30, et l'instance 2 pour les VLANs 40, 50 et 60. Un équilibrage de charge a été configuré en désignant CSWL3-01 comme pont racine principal pour l'instance 1 et secondaire pour l'instance 2, tandis que CSWL3-02 assume les rôles inverses. Tous les équipements partagent la même région MST avec des paramètres synchronisés, garantissant une convergence rapide et une continuité de service optimale. Comme illustré dans la Figure 3.9, la configuration valide la cohérence des paramètres MSTP sur les commutateurs.

```
CSWL3-01
CSWL3-01>en
CSWL3-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CSWL3-01(config)#spanning-tree mode mst
CSWL3-01(config)#spanning-tree mst configuration
CSWL3-01(config-mst)#name SOTETEL-MST
CSWL3-01(config-mst)#revision 1
CSWL3-01(config-mst)#instance 1 vlan 10,20,30
CSWL3-01(config-mst)#instance 2 vlan 40,50,60
CSWL3-01(config-mst)#exi
CSWL3-01(config)#spanning-tree mst 1 root primary
CSWL3-01(config)#spanning-tree mst 2 root secondary
CSWL3-01(config)#exi
CSWL3-01#
*Aug 25 19:37:29.439: %SYS-5-CONFIG_I: Configured from console by console
CSWL3-01#wr
Building configuration...
Compressed configuration from 3268 bytes to 1458 bytes[OK]
CSWL3-01#
```

FIGURE 3.9 – Configuration et validation du protocole MSTP

3.1.8 Configuration de VRRP

Le protocole VRRP (Virtual Router Redundancy Protocol) a été configuré sur les commutateurs CSWL3-01 et CSWL3-02 afin d'assurer la redondance des passerelles par défaut. CSWL3-01 joue le rôle de routeur principal pour les VLANs 10, 20 et 30, et de routeur secondaire pour les VLANs 40, 50 et 60, tandis que CSWL3-02 assume les rôles inverses, permettant un équilibrage efficace du trafic. La préemption est activée sur toutes les interfaces, garantissant un basculement automatique en cas de panne et une restauration rapide des services. Cette configuration assure une haute disponibilité et une répartition optimale du trafic réseau.

```

CSWL3-01>en
CSWL3-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CSWL3-01(config)#int vlan10
CSWL3-01(config-if)#vrrp 10 ip 192.168.10.1
CSWL3-01(config-if)#
*Jul  8 11:45:12.710: %VRRP-6-STATECHANGE: V110 Grp 10 state Init -> Backup
*Jul  8 11:45:12.715: %VRRP-6-STATECHANGE: V110 Grp 10 state Init -> Backup
CSWL3-01(config-if)#
*Jul  8 11:45:16.325: %VRRP-6-STATECHANGE: V110 Grp 10 state Backup -> Master
CSWL3-01(config-if)#vrrp 10 priority 110
CSWL3-01(config-if)#vrrp 10 preempt
CSWL3-01(config-if)#exi
CSWL3-01(config)#int vlan20
CSWL3-01(config-if)#vrrp 20 ip 192.168.20.1
CSWL3-01(config-if)#
*Jul  8 11:47:22.942: %VRRP-6-STATECHANGE: V120 Grp 20 state Init -> Backup
CSWL3-01(config-if)#vrrp 20 preempt
*Jul  8 11:47:26.551: %VRRP-6-STATECHANGE: V120 Grp 20 state Backup -> Master
CSWL3-01(config-if)#exi
CSWL3-01(config)#int vlan20
CSWL3-01(config-if)#vrrp 20 ip 192.168.20.1
CSWL3-01(config-if)#vrrp 20 priority 90
CSWL3-01(config-if)#vrrp 20 preempt
CSWL3-01(config-if)#exi
CSWL3-01(config)#exi
CSWL3-01#
*Jul  8 11:51:31.023: %SYS-5-CONFIG_I: Configured from console by console
CSWL3-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CSWL3-01(config)#int vlan 30
CSWL3-01(config-if)#vrrp 30 ip 192.168.30.1
CSWL3-01(config-if)#vrrp 30 ip 192.168.30.1
*Jul  8 11:55:27.026: %VRRP-6-STATECHANGE: V130 Grp 30 state Init -> Backup
CSWL3-01(config-if)#int vlan 30
*Jul  8 11:55:30.638: %VRRP-6-STATECHANGE: V130 Grp 30 state Backup -> Master
CSWL3-01(config-if)#vrrp 30 priority 110
CSWL3-01(config-if)#vrrp 30 preempt
CSWL3-01(config-if)#exi
CSWL3-01(config)#int vlan40
CSWL3-01(config-if)#vrrp 40 ip 192.168.40.1
CSWL3-01(config-if)#int vlan40
*Jul  8 11:56:26.266: %VRRP-6-STATECHANGE: V140 Grp 40 state Init -> Backup

```

FIGURE 3.10 – Configuration et validation de VRRP sur CSWL3-01 et CSWL3-02

3.1.9 Configuration du protocole EIGRP

Le protocole **EIGRP** (Enhanced Interior Gateway Routing Protocol) a été déployé afin d'assurer un routage dynamique fiable et redondant au sein de l'infrastructure réseau, avec le système autonome 100. Il a été configuré sur les équipements centraux (RouteurLAN1, CoreSW1, CoreSW2) ainsi que sur les routeurs périphériques (RouteurLAN2, RouteurLAN3).

La fonction de résumé automatique a été désactivée (no auto-summary) pour garantir la diffusion précise de tous les sous-réseaux. Les VLANs de la couche Core (192.168.10.0 à 192.168.60.0) ainsi que les interconnexions WAN (197.5.50.0/30) ont été explicitement inclus dans le processus de routage.

Cette configuration permet une **convergence rapide** en cas de panne de lien et optimise le cheminement des données grâce aux métriques composites d'EIGRP, assurant ainsi la disponibilité et la performance du réseau.

La Figure 3.11 présente un exemple de configuration sur RouteurLAN1, montrant l'intégration des réseaux WAN dans le protocole EIGRP.


```
R-LAN13
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R-LAN1
R-LAN1(config)#int e1/2
R-LAN1(config-if)#description lien vers CSW13-01
R-LAN1(config-if)#ip add 197.5.50.1 255.255.255.252
R-LAN1(config-if)#exi
R-LAN1(config)#int e1/3
R-LAN1(config-if)#description lien vers CSW13-02
R-LAN1(config-if)#ip add 197.5.50.5 255.255.255.252
R-LAN1(config-if)#exi
R-LAN1(config)#int e0/0
R-LAN1(config-if)#description lien vers R-LAN2
R-LAN1(config-if)#ip add 197.5.50.9 255.255.255.252
R-LAN1(config-if)#exi
R-LAN1(config)#int e0/1
R-LAN1(config-if)#description lien vers R-LAN3
R-LAN1(config-if)#ip add 197.5.50.13 255.255.255.252
R-LAN1(config-if)#exi
R-LAN1(config)#router eigrp 100
R-LAN1(config-router)#netwoek 197.5.50.0 0.0.0.3
^
% Invalid input detected at '^' marker.

R-LAN1(config-router)#network 197.5.50.0 0.0.0.3
R-LAN1(config-router)#network 197.5.50.4 0.0.0.3
R-LAN1(config-router)#network 197.5.50.8 0.0.0.3
R-LAN1(config-router)#network 197.5.50.12 0.0.0.3
R-LAN1(config-router)#no auto-summary
R-LAN1(config-router)#end
R-LAN1#wr
*Oct 20 16:54:34.914: %SYS-5-CONFIG_I: Configured from console by console
R-LAN1#wr
Building configuration...
```

FIGURE 3.11 – Exemple de configuration EIGRP sur RouteurLAN1

3.2 Conclusion

Conclusion

Ce chapitre a marqué la concrétisation technique du projet par le déploiement effectif de l'architecture réseau hiérarchique sous **EVE-NG**. L'ensemble des équipements a été configuré selon le modèle à trois niveaux, et les protocoles fondamentaux assurant la performance et la résilience du réseau ont été intégrés avec succès.

L'infrastructure ainsi finalisée constitue une base solide et opérationnelle pour la phase de validation qui fera l'objet du prochain chapitre.

Chapitre 4

Tests et Validation

Sommaire

4 Introduction	28
4.1 Tests de Connectivité de Base	28
4.2 Tests EtherChannel	30
4.3 Tests MST	36
4.4 Tests VRRP	40
4.5 Tests EIGRP	42
4.5 Conclusion	47

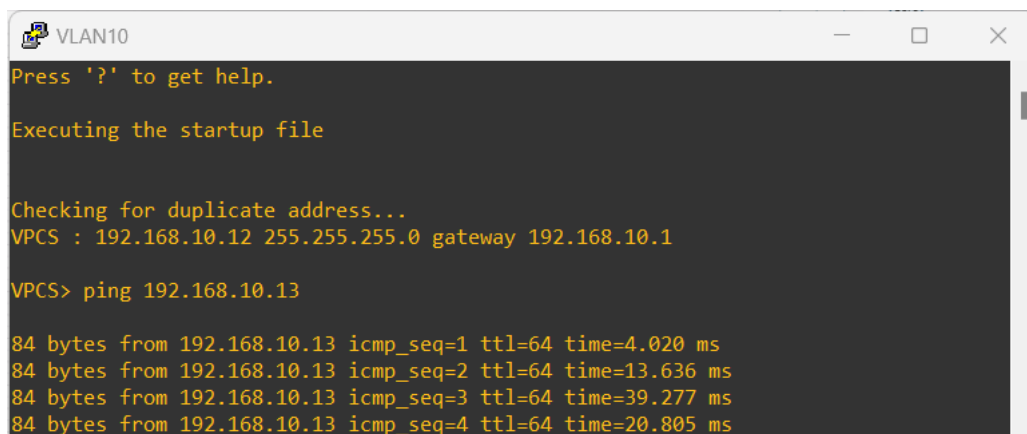
Introduction

Cette partie présente les essais réalisés pour vérifier le bon fonctionnement du réseau. Tous les tests ont été effectués dans l'environnement virtualisé **EVE-NG** afin de s'assurer que l'infrastructure réponde pleinement aux besoins techniques et fonctionnels du projet.

4.1 Tests de Connectivité de Base

Ping intra-VLAN (même VLAN)

Un test de ping a été exécuté entre deux hôtes appartenant au même VLAN afin de s'assurer de la connectivité interne et de la conformité préalable au routage inter-VLAN.



```
VLAN10
Press '?' to get help.

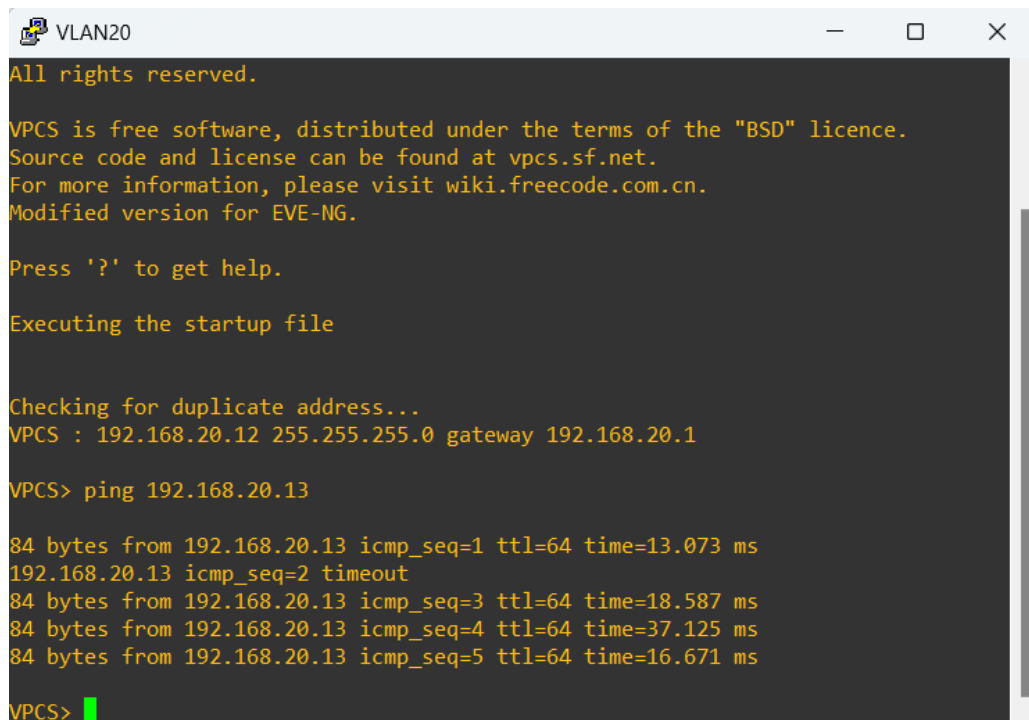
Executing the startup file

Checking for duplicate address...
VPCS : 192.168.10.12 255.255.255.0 gateway 192.168.10.1

VPCS> ping 192.168.10.13

84 bytes from 192.168.10.13 icmp_seq=1 ttl=64 time=4.020 ms
84 bytes from 192.168.10.13 icmp_seq=2 ttl=64 time=13.636 ms
84 bytes from 192.168.10.13 icmp_seq=3 ttl=64 time=39.277 ms
84 bytes from 192.168.10.13 icmp_seq=4 ttl=64 time=20.805 ms
```

FIGURE 4.1 – Validation de la connectivité entre PC1 et PC6 au sein du VLAN 10



```
VLAN20
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.

Press '?' to get help.

Executing the startup file

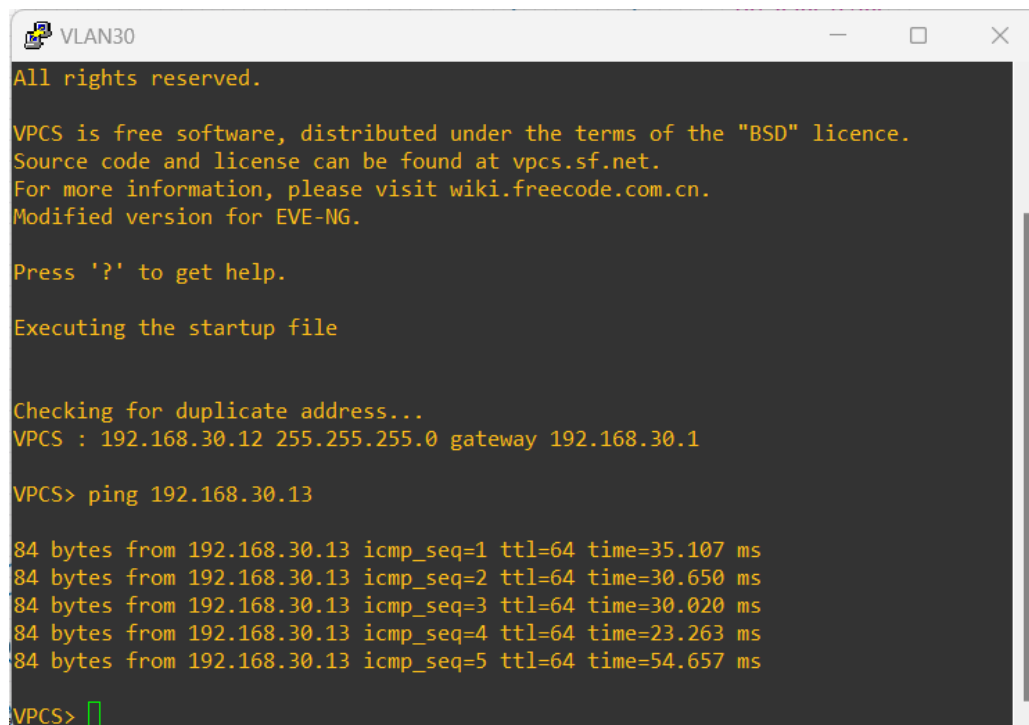
Checking for duplicate address...
VPCS : 192.168.20.12 255.255.255.0 gateway 192.168.20.1

VPCS> ping 192.168.20.13

84 bytes from 192.168.20.13 icmp_seq=1 ttl=64 time=13.073 ms
192.168.20.13 icmp_seq=2 timeout
84 bytes from 192.168.20.13 icmp_seq=3 ttl=64 time=18.587 ms
84 bytes from 192.168.20.13 icmp_seq=4 ttl=64 time=37.125 ms
84 bytes from 192.168.20.13 icmp_seq=5 ttl=64 time=16.671 ms

VPCS>
```

FIGURE 4.2 – Validation de la connectivité entre PC2 et PC7 au sein du VLAN 20



```
VLAN30
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
VPCS : 192.168.30.12 255.255.255.0 gateway 192.168.30.1

VPCS> ping 192.168.30.13

84 bytes from 192.168.30.13 icmp_seq=1 ttl=64 time=35.107 ms
84 bytes from 192.168.30.13 icmp_seq=2 ttl=64 time=30.650 ms
84 bytes from 192.168.30.13 icmp_seq=3 ttl=64 time=30.020 ms
84 bytes from 192.168.30.13 icmp_seq=4 ttl=64 time=23.263 ms
84 bytes from 192.168.30.13 icmp_seq=5 ttl=64 time=54.657 ms

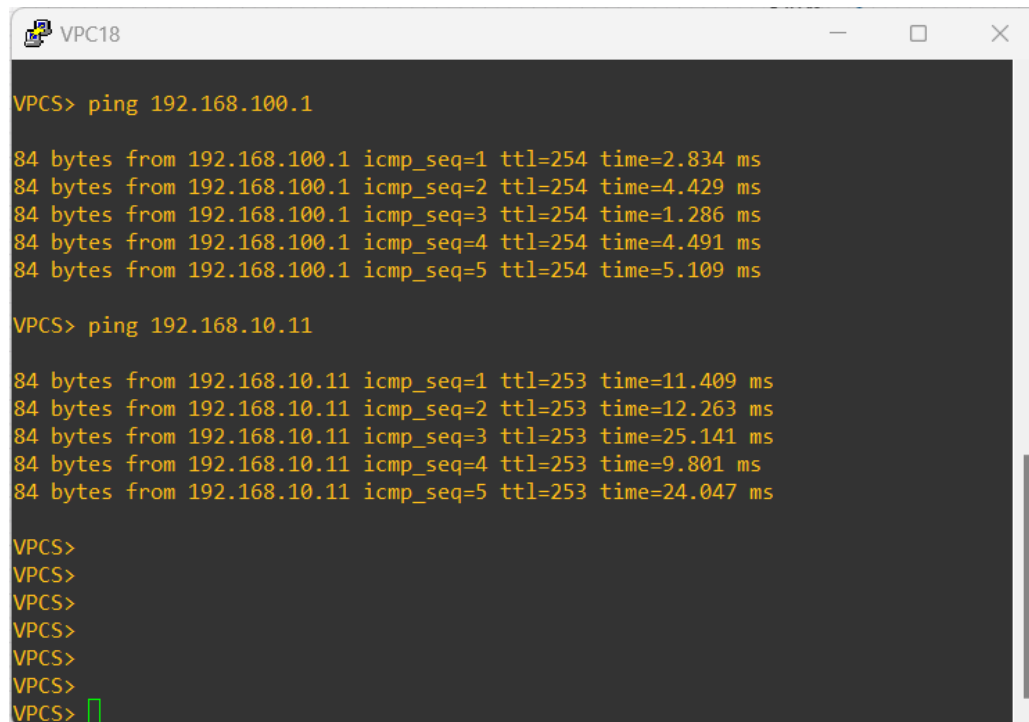
VPCS>
```

FIGURE 4.3 – Validation de la connectivité entre PC3 et PC8 au sein du VLAN 30

Ping inter-LANs

Afin de valider la communication entre différents réseaux locaux, un test de ping a été effectué depuis le routeur du LAN3 vers les VLANs des LAN2 et LAN1. Cette vérification

confirme le bon fonctionnement du routage inter-LAN et la connectivité entre les segments réseau.



```
VPC18
VPCS> ping 192.168.100.1
84 bytes from 192.168.100.1 icmp_seq=1 ttl=254 time=2.834 ms
84 bytes from 192.168.100.1 icmp_seq=2 ttl=254 time=4.429 ms
84 bytes from 192.168.100.1 icmp_seq=3 ttl=254 time=1.286 ms
84 bytes from 192.168.100.1 icmp_seq=4 ttl=254 time=4.491 ms
84 bytes from 192.168.100.1 icmp_seq=5 ttl=254 time=5.109 ms

VPCS> ping 192.168.10.11
84 bytes from 192.168.10.11 icmp_seq=1 ttl=253 time=11.409 ms
84 bytes from 192.168.10.11 icmp_seq=2 ttl=253 time=12.263 ms
84 bytes from 192.168.10.11 icmp_seq=3 ttl=253 time=25.141 ms
84 bytes from 192.168.10.11 icmp_seq=4 ttl=253 time=9.801 ms
84 bytes from 192.168.10.11 icmp_seq=5 ttl=253 time=24.047 ms

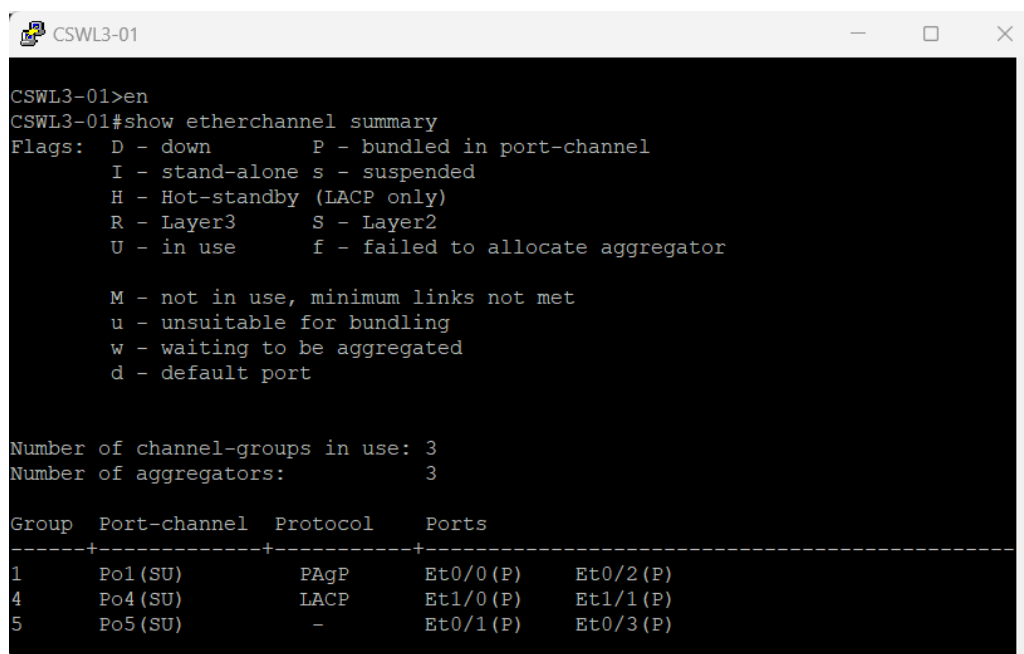
VPCS>
VPCS>
VPCS>
VPCS>
VPCS>
VPCS>
VPCS>
```

FIGURE 4.4 – Validation de la connectivité inter-LAN

4.2 Tests EtherChannel

Ce test vise à s'assurer du bon fonctionnement et de la tolérance aux pannes d'un EtherChannel configuré entre deux switches. L'objectif est de vérifier l'agrégation correcte des interfaces, le maintien de la connectivité et la résilience en cas de défaillance d'un lien.

Étape 1 : Vérification de la création de l'EtherChannel



```
CSWL3-01>en
CSWL3-01#show etherchannel summary
Flags:  D - down          P - bundled 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

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 3
Number of aggregators:          3

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1 (SU)      PAgP        Et0/0 (P)  Et0/2 (P)
4      Po4 (SU)      LACP        Et1/0 (P)  Et1/1 (P)
5      Po5 (SU)      -           Et0/1 (P)  Et0/3 (P)
```

FIGURE 4.5 – État du port-channel et des interfaces membres après création

Étape 2 : Test de connectivité

Un ping a été effectué entre les VLANs connectés via l'EtherChannel pour confirmer que la communication est opérationnelle avant toute modification.

```
VLAN10
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
Copyright (c) 2021, Alain Degreffe (alain.degreffe@eve-ng.net)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
VPCS : 192.168.10.12 255.255.255.0 gateway 192.168.10.1

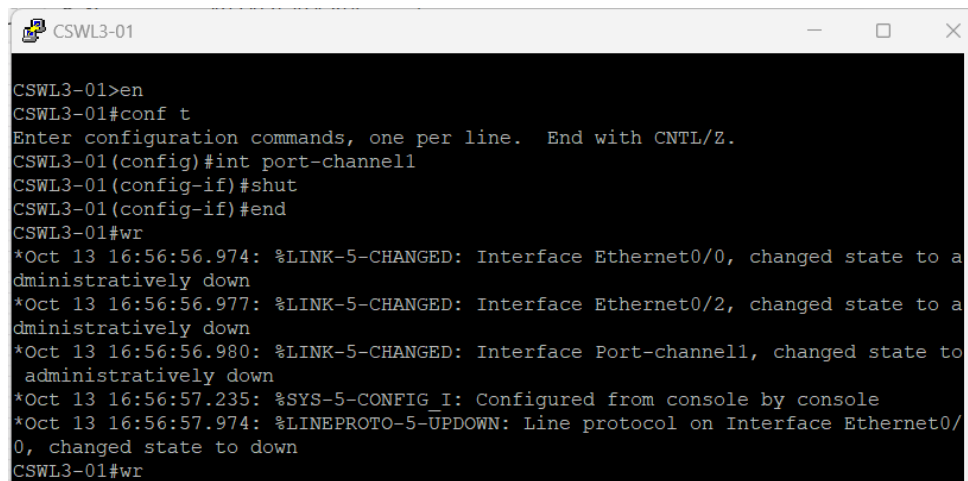
VPCS> ping 192.168.10.10 -c 50

84 bytes from 192.168.10.10 icmp_seq=1 ttl=255 time=4.812 ms
84 bytes from 192.168.10.10 icmp_seq=2 ttl=255 time=18.105 ms
84 bytes from 192.168.10.10 icmp_seq=3 ttl=255 time=18.895 ms
84 bytes from 192.168.10.10 icmp_seq=4 ttl=255 time=26.155 ms
84 bytes from 192.168.10.10 icmp_seq=5 ttl=255 time=18.972 ms
84 bytes from 192.168.10.10 icmp_seq=6 ttl=255 time=13.553 ms
84 bytes from 192.168.10.10 icmp_seq=7 ttl=255 time=12.666 ms
192.168.10.10 icmp_seq=8 timeout
192.168.10.10 icmp_seq=9 timeout
192.168.10.10 icmp_seq=10 timeout
192.168.10.10 icmp_seq=11 timeout
192.168.10.10 icmp_seq=12 timeout
84 bytes from 192.168.10.10 icmp_seq=13 ttl=255 time=22.013 ms
84 bytes from 192.168.10.10 icmp_seq=14 ttl=255 time=11.131 ms
84 bytes from 192.168.10.10 icmp_seq=15 ttl=255 time=23.105 ms
84 bytes from 192.168.10.10 icmp_seq=16 ttl=255 time=20.705 ms
84 bytes from 192.168.10.10 icmp_seq=17 ttl=255 time=14.314 ms
84 bytes from 192.168.10.10 icmp_seq=18 ttl=255 time=12.114 ms
84 bytes from 192.168.10.10 icmp_seq=19 ttl=255 time=19.732 ms
84 bytes from 192.168.10.10 icmp_seq=20 ttl=255 time=17.282 ms
84 bytes from 192.168.10.10 icmp_seq=21 ttl=255 time=15.373 ms
84 bytes from 192.168.10.10 icmp_seq=22 ttl=255 time=16.911 ms
84 bytes from 192.168.10.10 icmp_seq=23 ttl=255 time=13.631 ms
84 bytes from 192.168.10.10 icmp_seq=24 ttl=255 time=21.128 ms
84 bytes from 192.168.10.10 icmp_seq=25 ttl=255 time=17.089 ms
```

FIGURE 4.6 – Ping continu avant la défaillance d'un lien EtherChannel

Étape 3 : Simulation de défaillance d'un lien

Un lien membre de l'EtherChannel a été désactivé avec la commande `shutdown` sur l'interface `e0/0` afin de simuler une panne.



```
CSWL3-01>en
CSWL3-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CSWL3-01(config)#int port-channel1
CSWL3-01(config-if)#shut
CSWL3-01(config-if)#end
CSWL3-01#wr
*Oct 13 16:56:56.974: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Oct 13 16:56:56.977: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to administratively down
*Oct 13 16:56:56.980: %LINK-5-CHANGED: Interface Port-channel1, changed state to administratively down
*Oct 13 16:56:57.235: %SYS-5-CONFIG_I: Configured from console by console
*Oct 13 16:56:57.974: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
CSWL3-01#wr
```

FIGURE 4.7 – Désactivation d'un lien membre de l'EtherChannel

Étape 4 : Vérification de l'état du port-channel après désactivation

Après la mise hors service d'un lien membre, la commande `show etherchannel summary` a été exécutée afin de confirmer que l'interface concernée est bien désactivée tout en maintenant l'état opérationnel du port-channel.

```
VLAN10
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
Copyright (c) 2021, Alain Degreffe (alain.degreffe@eve-ng.net)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version for EVE-NG.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
VPCS : 192.168.10.12 255.255.255.0 gateway 192.168.10.1

VPCS> ping 192.168.10.10 -c 50

84 bytes from 192.168.10.10 icmp_seq=1 ttl=255 time=4.812 ms
84 bytes from 192.168.10.10 icmp_seq=2 ttl=255 time=18.105 ms
84 bytes from 192.168.10.10 icmp_seq=3 ttl=255 time=18.895 ms
84 bytes from 192.168.10.10 icmp_seq=4 ttl=255 time=26.155 ms
84 bytes from 192.168.10.10 icmp_seq=5 ttl=255 time=18.972 ms
84 bytes from 192.168.10.10 icmp_seq=6 ttl=255 time=13.553 ms
84 bytes from 192.168.10.10 icmp_seq=7 ttl=255 time=12.666 ms
192.168.10.10 icmp_seq=8 timeout
192.168.10.10 icmp_seq=9 timeout
192.168.10.10 icmp_seq=10 timeout
192.168.10.10 icmp_seq=11 timeout
192.168.10.10 icmp_seq=12 timeout
84 bytes from 192.168.10.10 icmp_seq=13 ttl=255 time=22.013 ms
84 bytes from 192.168.10.10 icmp_seq=14 ttl=255 time=11.131 ms
84 bytes from 192.168.10.10 icmp_seq=15 ttl=255 time=23.105 ms
84 bytes from 192.168.10.10 icmp_seq=16 ttl=255 time=20.705 ms
84 bytes from 192.168.10.10 icmp_seq=17 ttl=255 time=14.314 ms
84 bytes from 192.168.10.10 icmp_seq=18 ttl=255 time=12.114 ms
84 bytes from 192.168.10.10 icmp_seq=19 ttl=255 time=19.732 ms
84 bytes from 192.168.10.10 icmp_seq=20 ttl=255 time=17.282 ms
84 bytes from 192.168.10.10 icmp_seq=21 ttl=255 time=15.373 ms
84 bytes from 192.168.10.10 icmp_seq=22 ttl=255 time=16.911 ms
84 bytes from 192.168.10.10 icmp_seq=23 ttl=255 time=13.631 ms
84 bytes from 192.168.10.10 icmp_seq=24 ttl=255 time=21.128 ms
84 bytes from 192.168.10.10 icmp_seq=25 ttl=255 time=17.089 ms
```

FIGURE 4.8 – Vérification de l'état du port-channel après la désactivation d'un lien

Étape 5 : Vérification de la continuité du service

Pendant la désactivation, le ping a continué sans interruption notable, démontrant la tolérance aux pannes du port-channel.


```

CSWL3-01
CSWL3-01(config)#int port-channel1
CSWL3-01(config-if)#shut
CSWL3-01(config-if)#exi
CSWL3-01(config)#exi
*Oct 13 17:56:22.982: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to a
administratively down
*Oct 13 17:56:22.987: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to a
administratively down
*Oct 13 17:56:22.987: %LINK-5-CHANGED: Interface Port-channel1, changed state to
administratively down
*Oct 13 17:56:23.984: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to down
*Oct 13 17:56:23.987: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
2, changed state to down
*Oct 13 17:56:23.987: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-chann
ell, changed state to down
CSWL3-01(config)#exi
CSWL3-01#wr
*Oct 13 17:56:25.208: %SYS-5-CONFIG_I: Configured from console by console
CSWL3-01#wr
Building configuration...
Compressed configuration from 3744 bytes to 1765 bytes[OK]
CSWL3-01#wr
*Oct 13 17:56:27.598: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/1 TDR=0, TRC=0
CSWL3-01#sh spanning-tree mst

##### MST0      vlans mapped: 1-9,11-19,21-29,31-39,41-49,51-59,61-4094
Bridge            address aabb.cc00.1000 priority 32768 (32768 sysid 0)
Root              this switch for the CIST
Operational        hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured         hello time 2 , forward delay 15, max age 20, max hops 20

Interface         Role Sts Cost      Prio.Nbr Type
-----
Et1/3              Desg FWD 2000000 128.8   Shr
Et2/0              Desg FWD 2000000 128.9   Shr
Et2/1              Desg FWD 2000000 128.10  Shr
Et2/2              Desg FWD 2000000 128.11  Shr
Et2/3              Desg FWD 2000000 128.12  Shr
Po5                Desg FWD 1000000 128.65  Shr
Po4                Desg FWD 1000000 128.66  Shr

##### MST1      vlans mapped: 10,20,30
Bridge            address aabb.cc00.1000 priority 24577 (24576 sysid 1)
Root              this switch for MST1

Interface         Role Sts Cost      Prio.Nbr Type
-----
Po5                Desg FWD 1000000 128.65  Shr

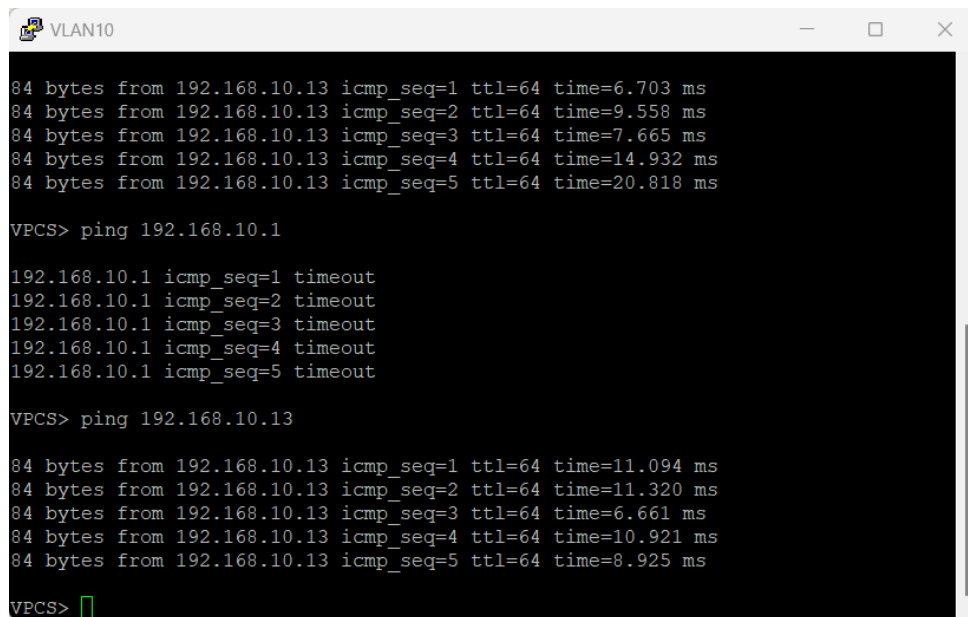
```

FIGURE 4.9 – Ping continu pendant la désactivation d'un lien EtherChannel

Cette capture illustre le comportement du ping continu pendant le test de résilience. Une perte momentanée de quelques paquets a été observée lors de la désactivation du lien, suivie d'une reprise immédiate, ce qui confirme la tolérance aux pannes du port-channel.

Étape 6 : Rétablissement du lien

Le lien précédemment désactivé a été réactivé avec la commande `no shutdown`, permettant de restaurer la configuration initiale du port-channel.



```
VLAN10
84 bytes from 192.168.10.13 icmp_seq=1 ttl=64 time=6.703 ms
84 bytes from 192.168.10.13 icmp_seq=2 ttl=64 time=9.558 ms
84 bytes from 192.168.10.13 icmp_seq=3 ttl=64 time=7.665 ms
84 bytes from 192.168.10.13 icmp_seq=4 ttl=64 time=14.932 ms
84 bytes from 192.168.10.13 icmp_seq=5 ttl=64 time=20.818 ms

VPCS> ping 192.168.10.1

192.168.10.1 icmp_seq=1 timeout
192.168.10.1 icmp_seq=2 timeout
192.168.10.1 icmp_seq=3 timeout
192.168.10.1 icmp_seq=4 timeout
192.168.10.1 icmp_seq=5 timeout

VPCS> ping 192.168.10.13

84 bytes from 192.168.10.13 icmp_seq=1 ttl=64 time=11.094 ms
84 bytes from 192.168.10.13 icmp_seq=2 ttl=64 time=11.320 ms
84 bytes from 192.168.10.13 icmp_seq=3 ttl=64 time=6.661 ms
84 bytes from 192.168.10.13 icmp_seq=4 ttl=64 time=10.921 ms
84 bytes from 192.168.10.13 icmp_seq=5 ttl=64 time=8.925 ms

VPCS> █
```

FIGURE 4.10 – Rétablissement du lien EtherChannel

4.3 Tests MST (Multiple Spanning Tree)

Ce test permet de vérifier la configuration des instances MST et d'évaluer la capacité du protocole à maintenir la connectivité réseau en cas de défaillance d'un lien.

Étape 1 : Vérification des instances MST configurées

```
CSWL3-01

*Oct 13 16:30:51.633: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/1 TDR=0, TRC=0
CSWL3-01>en
CSWL3-01#sh spanning-tree mst

##### MST0      vlans mapped: 1-9,11-19,21-29,31-39,41-49,51-59,61-4094
Bridge          address aabb.cc00.1000 priority      32768 (32768 sysid 0)
Root            this switch for the CIST
Operational     hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured      hello time 2 , forward delay 15, max age 20, max hops 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Et1/3          Desg FWD 2000000 128.8   Shr
Et2/0          Desg FWD 2000000 128.9   Shr
Et2/1          Desg FWD 2000000 128.10  Shr
Et2/2          Desg FWD 2000000 128.11  Shr
Et2/3          Desg FWD 2000000 128.12  Shr
Po1            Desg FWD 1000000 128.65  Shr
Po4            Desg FWD 1000000 128.66  Shr
Po5            Desg FWD 1000000 128.67  Shr

##### MST1      vlans mapped: 10,20,30
Bridge          address aabb.cc00.1000 priority      24577 (24576 sysid 1)
Root            this switch for MST1

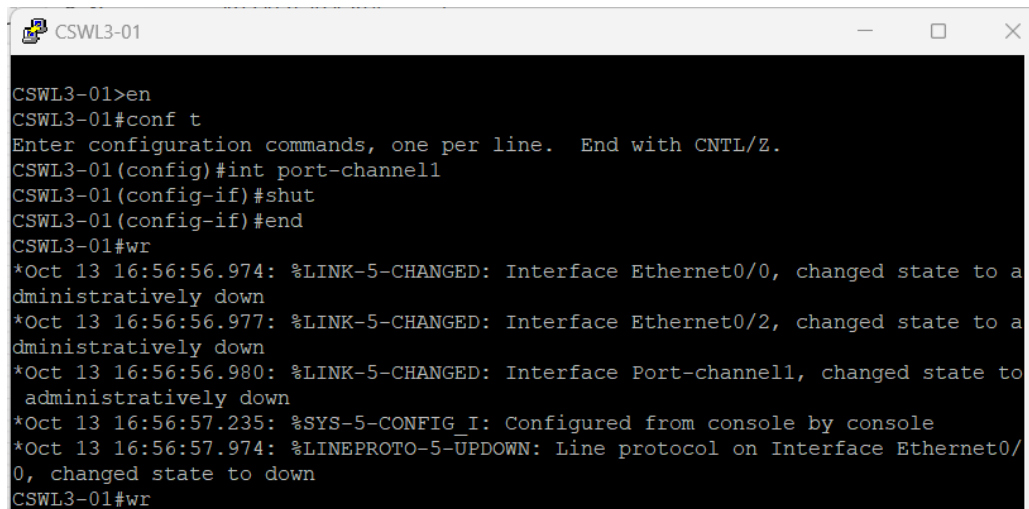
Interface      Role Sts Cost      Prio.Nbr Type
-----
Po1            Desg FWD 1000000 128.65  Shr
Po4            Desg FWD 1000000 128.66  Shr
Po5            Desg FWD 1000000 128.67  Shr

##### MST2      vlans mapped: 40,50,60
--More--
*Oct 13 16:31:51.733: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/1 TDR=0, TRC=0
Bridge          address aabb.cc00.1000 priority      28674 (28672 sysid 2)
Root            address aabb.cc00.2000 priority      24578 (24576 sysid 2)
                  port Po5 cost 1000000 rem hops 19

Interface      Role Sts Cost      Prio.Nbr Type
-----
Po1            Desg FWD 1000000 128.65  Shr
Po4            Desg FWD 1000000 128.66  Shr
Po5            Root FWD 1000000 128.67  Shr
```

FIGURE 4.11 – Affichage initial des instances MST configurées

Étape 2 : Simulation d'une défaillance de lien



```
CSWL3-01>en
CSWL3-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CSWL3-01(config)#int port-channel1
CSWL3-01(config-if)#shut
CSWL3-01(config-if)#end
CSWL3-01#wr
*Oct 13 16:56:56.974: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Oct 13 16:56:56.977: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to administratively down
*Oct 13 16:56:56.980: %LINK-5-CHANGED: Interface Port-channel1, changed state to administratively down
*Oct 13 16:56:57.235: %SYS-5-CONFIG_I: Configured from console by console
*Oct 13 16:56:57.974: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
CSWL3-01#wr
```

FIGURE 4.12 – Désactivation d'un lien pour tester la convergence MSTP

Cette action permet de vérifier la rapidité de réaction du protocole et l'absence de boucle après la perte d'un lien.

Étape 3 : Observation port-désactivation

La commande `show spanning-tree mst` a de nouveau été exécutée pour confirmer que le port concerné est passé en état blocking ou down.

```

CSWL3-01
CSWL3-01(config)#int port-channel1
CSWL3-01(config-if)#shut
CSWL3-01(config-if)#exi
CSWL3-01(config)#exi
*Oct 13 17:56:22.982: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to a
dministratively down
*Oct 13 17:56:22.987: %LINK-5-CHANGED: Interface Ethernet0/2, changed state to a
dministratively down
*Oct 13 17:56:22.987: %LINK-5-CHANGED: Interface Port-channel1, changed state to
administratively down
*Oct 13 17:56:23.984: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to down
*Oct 13 17:56:23.987: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
2, changed state to down
*Oct 13 17:56:23.987: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-chann
ell, changed state to down
CSWL3-01(config)#exi
CSWL3-01#wr
*Oct 13 17:56:25.208: %SYS-5-CONFIG_I: Configured from console by console
CSWL3-01#wr
Building configuration...
Compressed configuration from 3744 bytes to 1765 bytes[OK]
CSWL3-01#wr
*Oct 13 17:56:27.598: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/1 TDR=0, TRC=0
CSWL3-01#sh spanning-tree mst

##### MST0      vlans mapped: 1-9,11-19,21-29,31-39,41-49,51-59,61-4094
Bridge          address aabb.cc00.1000 priority      32768 (32768 sysid 0)
Root            this switch for the CIST
Operational     hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured      hello time 2 , forward delay 15, max age 20, max hops 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Et1/3          Desg FWD 2000000 128.8   Shr
Et2/0          Desg FWD 2000000 128.9   Shr
Et2/1          Desg FWD 2000000 128.10  Shr
Et2/2          Desg FWD 2000000 128.11  Shr
Et2/3          Desg FWD 2000000 128.12  Shr
Po5            Desg FWD 1000000 128.65  Shr
Po4            Desg FWD 1000000 128.66  Shr

##### MST1      vlans mapped: 10,20,30
Bridge          address aabb.cc00.1000 priority      24577 (24576 sysid 1)
Root            this switch for MST1

Interface      Role Sts Cost      Prio.Nbr Type
-----
Po5            Desg FWD 1000000 128.65  Shr

```

FIGURE 4.13 – État du MSTP après désactivation du lien

Étape 4 : Vérification de la connectivité

Un test de ping a été effectué entre deux VLANs pendant la défaillance et analysé via Wireshark afin de confirmer la continuité du trafic.

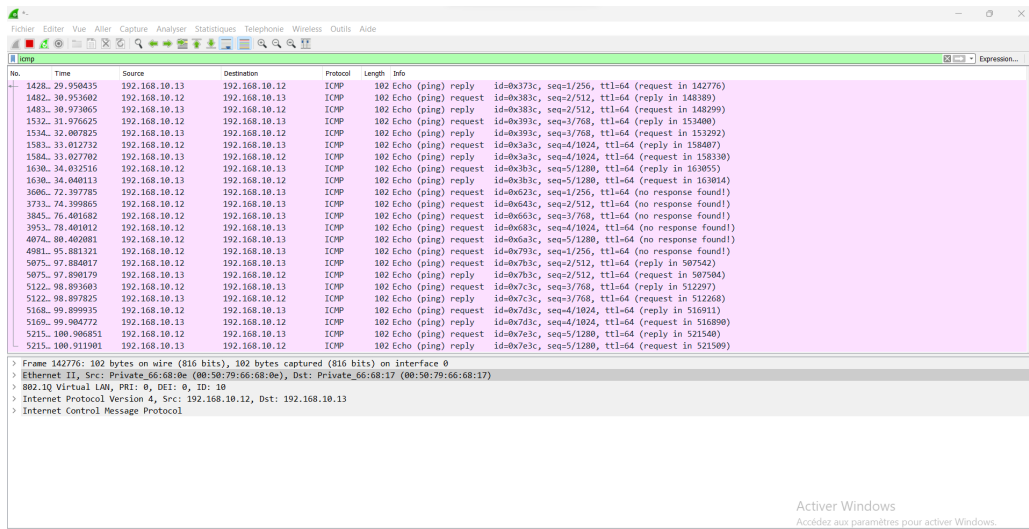


FIGURE 4.14 – Analyse du ping capturé par Wireshark lors de la convergence MSTP

Le ping capturé montre une courte interruption suivie d'une reprise immédiate, attestant de la rapidité de convergence et de la résilience du protocole MSTP.

4.4 Tests VRRP

Ces tests ont pour objectif de vérifier la configuration et la résilience du protocole VRRP, assurant la continuité du trafic entre les switches Core.

Étape 1 : Vérification des rôles VRRP

La commande `show vrrp bri` a été exécutée sur les deux switches Core afin d'identifier le rôle de chaque appareil (Master et Backup).

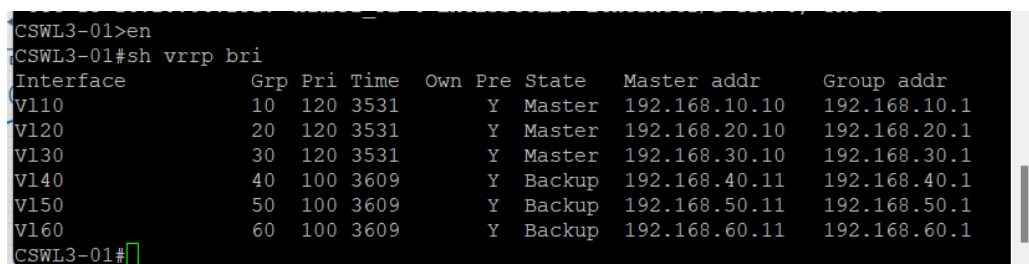


FIGURE 4.15 – Identification des rôles Master et Backup sur les switches Core1

```

CSWL3-02
CSWL3-02#sh vrrp bri
Interface      Grp Pri  Time   Own Pre State   Master addr   Group addr
Vl10           10  100 3609      Y Backup 192.168.10.10 192.168.10.1
Vl20           20  100 3609      Y Backup 192.168.20.10 192.168.20.1
Vl30           30  100 3609      Y Backup 192.168.30.10 192.168.30.1
Vl40           40  120 3531      Y Master 192.168.40.11 192.168.40.1
Vl50           50  120 3531      Y Master 192.168.50.11 192.168.50.1
Vl60           60  120 3531      Y Master 192.168.60.11 192.168.60.1
CSWL3-02#
*Oct 13 16:14:45.410: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/1 TDR=0, TRC=0
CSWL3-02#
*Oct 13 16:14:58.855: %VRRP-6-STATECHANGE: Vl10 Grp 10 state Backup -> Master
CSWL3-02#
*Oct 13 16:15:08.973: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 192.168.10.10
(Vlan10) is down: holding time expired

```

FIGURE 4.16 – Identification des rôles Master et Backup sur les switches Core2

Étape 2 : Test de basculement VRRP

Un ping a été lancé depuis un PC connecté au réseau pour vérifier la connectivité. Ensuite, le routeur Master (CSWL3-01) a été désactivé afin de provoquer le basculement automatique vers le Backup, puis le ping a été relancé pour confirmer la continuité du trafic.

```

VLAN10
84 bytes from 192.168.10.13 icmp_seq=1 ttl=64 time=6.703 ms
84 bytes from 192.168.10.13 icmp_seq=2 ttl=64 time=9.558 ms
84 bytes from 192.168.10.13 icmp_seq=3 ttl=64 time=7.665 ms
84 bytes from 192.168.10.13 icmp_seq=4 ttl=64 time=14.932 ms
84 bytes from 192.168.10.13 icmp_seq=5 ttl=64 time=20.818 ms

VPCS> ping 192.168.10.1

192.168.10.1 icmp_seq=1 timeout
192.168.10.1 icmp_seq=2 timeout
192.168.10.1 icmp_seq=3 timeout
192.168.10.1 icmp_seq=4 timeout
192.168.10.1 icmp_seq=5 timeout

VPCS> ping 192.168.10.13

84 bytes from 192.168.10.13 icmp_seq=1 ttl=64 time=11.094 ms
84 bytes from 192.168.10.13 icmp_seq=2 ttl=64 time=11.320 ms
84 bytes from 192.168.10.13 icmp_seq=3 ttl=64 time=6.661 ms
84 bytes from 192.168.10.13 icmp_seq=4 ttl=64 time=10.921 ms
84 bytes from 192.168.10.13 icmp_seq=5 ttl=64 time=8.925 ms

VPCS>

```

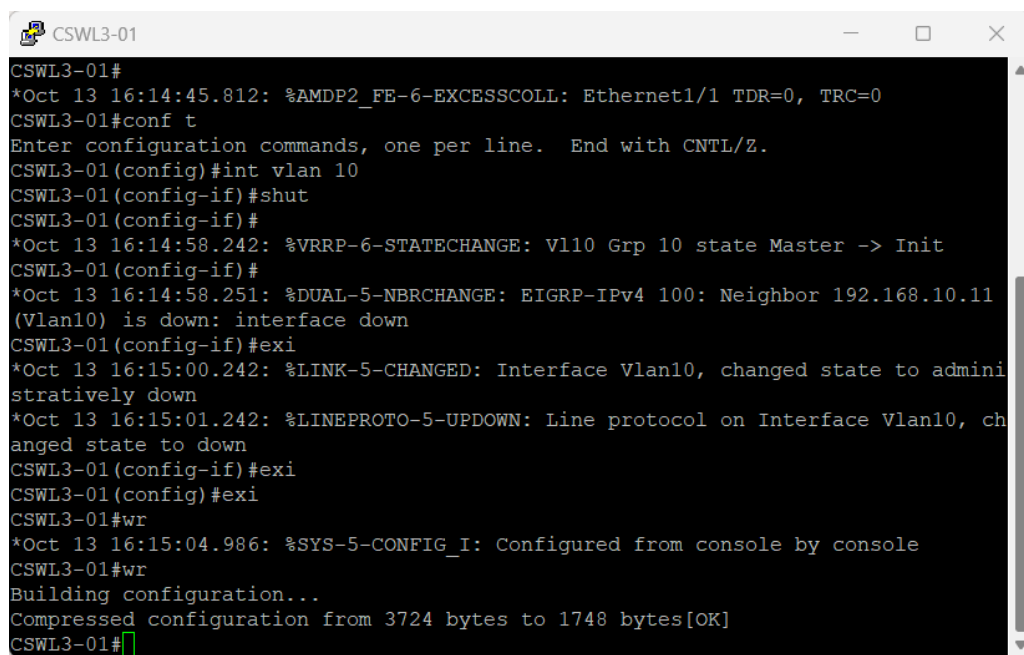
FIGURE 4.17 – Ping avant et après désactivation du Master pour tester le basculement VRRP

Étape 2 : Test de basculement VRRP

Objectif : Vérifier que le routeur Backup prend automatiquement le rôle de Master en cas de défaillance du Master, et que la continuité du trafic est assurée.

Procédure :

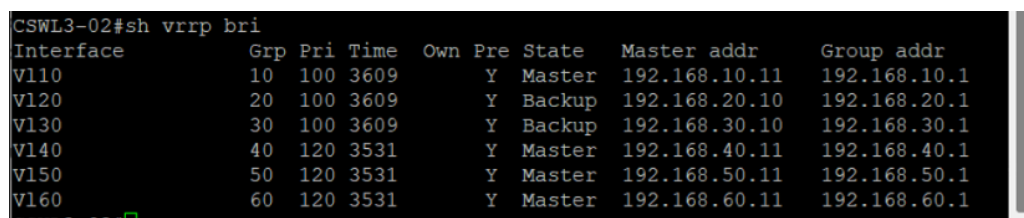
1. **Désactivation du Master (CSWL3-01)** Le routeur Master a été mis hors service ou son interface VRRP désactivée pour simuler une panne.



```
CSWL3-01#
*Oct 13 16:14:45.812: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/1 TDR=0, TRC=0
CSWL3-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CSWL3-01(config)#int vlan 10
CSWL3-01(config-if)#shut
CSWL3-01(config-if)#
*Oct 13 16:14:58.242: %VRRP-6-STATECHANGE: V110 Grp 10 state Master -> Init
CSWL3-01(config-if)#
*Oct 13 16:14:58.251: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 192.168.10.11
(Vlan10) is down: interface down
CSWL3-01(config-if)#exi
*Oct 13 16:15:00.242: %LINK-5-CHANGED: Interface Vlan10, changed state to admini
stratively down
*Oct 13 16:15:01.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, ch
anged state to down
CSWL3-01(config-if)#exi
CSWL3-01(config)#exi
CSWL3-01#wr
*Oct 13 16:15:04.986: %SYS-5-CONFIG_I: Configured from console by console
CSWL3-01#wr
Building configuration...
Compressed configuration from 3724 bytes to 1748 bytes[OK]
CSWL3-01#
```

FIGURE 4.18 – Désactivation du routeur Master CSWL3-01

2. **Basculement sur le Backup (CSWL3-02)** Après la désactivation du Master, le routeur Backup a automatiquement pris le rôle de Master. Un ping a été effectué depuis un PC pour vérifier que la connectivité réseau est restée opérationnelle.



```
CSWL3-02#sh vrrp bri
Interface      Grp Pri Time  Own Pre State  Master addr  Group addr
Vl10           10 100 3609      Y Master 192.168.10.11 192.168.10.1
Vl20           20 100 3609      Y Backup 192.168.20.10 192.168.20.1
Vl30           30 100 3609      Y Backup 192.168.30.10 192.168.30.1
Vl40           40 120 3531      Y Master 192.168.40.11 192.168.40.1
Vl50           50 120 3531      Y Master 192.168.50.11 192.168.50.1
Vl60           60 120 3531      Y Master 192.168.60.11 192.168.60.1
```

FIGURE 4.19 – Basculement automatique sur CSWL3-02 après défaillance du Master

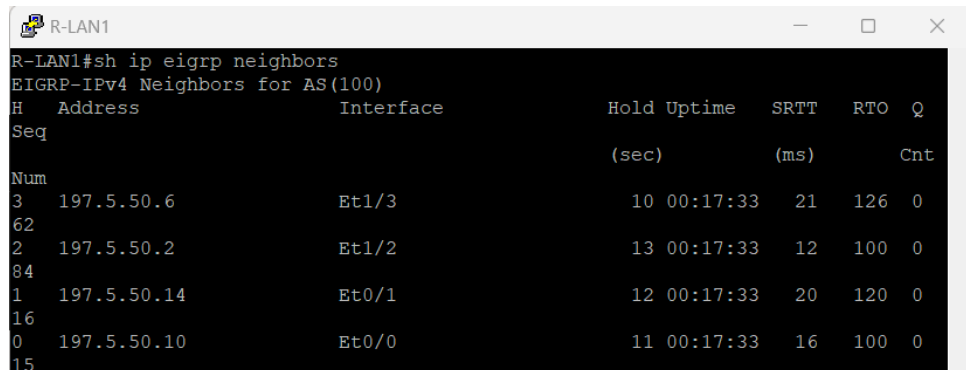
Le basculement s’est déroulé correctement, le Backup est devenu Master et le trafic réseau a été maintenu, confirmant la tolérance aux pannes de la configuration VRRP.

4.5 Tests EIGRP

Ces tests visent à vérifier la configuration et le bon fonctionnement du protocole EIGRP entre les trois routeurs, en évaluant l’établissement des voisinages, la convergence et la redondance des chemins.

Étape 1 : Vérification des voisinages EIGRP

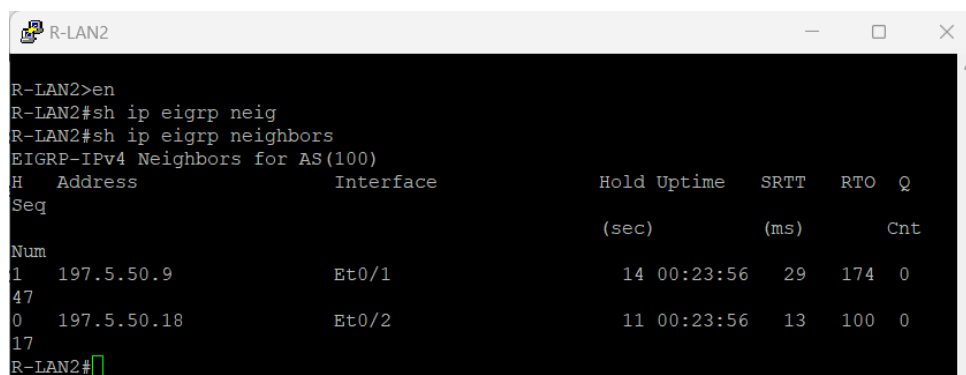
La commande `show ip eigrp neighbors` a été exécutée sur R-LAN1, R-LAN2 et R-LAN3 pour confirmer que tous les routeurs ont établi des voisinages EIGRP.



```
R-LAN1#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
```

H	Address	Interface	Hold	Uptime	SRTT	RTO	Q
Seq			(sec)		(ms)		Cnt
Num							
3	197.5.50.6	Et1/3	10	00:17:33	21	126	0
62							
2	197.5.50.2	Et1/2	13	00:17:33	12	100	0
84							
1	197.5.50.14	Et0/1	12	00:17:33	20	120	0
16							
0	197.5.50.10	Et0/0	11	00:17:33	16	100	0
15							

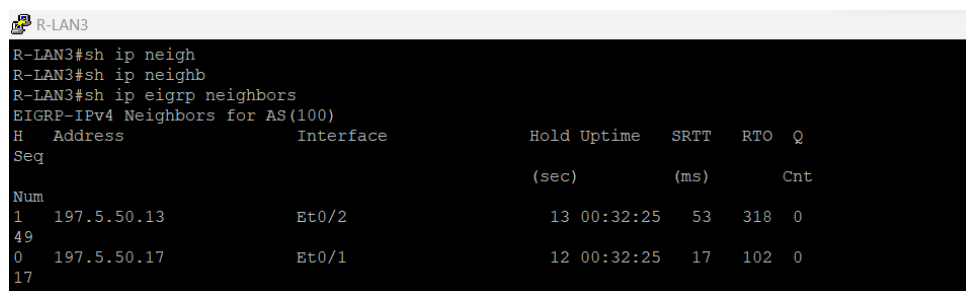
FIGURE 4.20 – Voisinages EIGRP sur R-LAN1



```
R-LAN2>en
R-LAN2#sh ip eigrp neig
R-LAN2#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
```

H	Address	Interface	Hold	Uptime	SRTT	RTO	Q
Seq			(sec)		(ms)		Cnt
Num							
1	197.5.50.9	Et0/1	14	00:23:56	29	174	0
47							
0	197.5.50.18	Et0/2	11	00:23:56	13	100	0
17							

FIGURE 4.21 – Voisinages EIGRP sur R-LAN2



```
R-LAN3#sh ip neigh
R-LAN3#sh ip neighb
R-LAN3#sh ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
```

H	Address	Interface	Hold	Uptime	SRTT	RTO	Q
Seq			(sec)		(ms)		Cnt
Num							
1	197.5.50.13	Et0/2	13	00:32:25	53	318	0
49							
0	197.5.50.17	Et0/1	12	00:32:25	17	102	0
17							

FIGURE 4.22 – Voisinages EIGRP sur R-LAN3

Étape 2 : Vérification des tables de routage EIGRP

La commande `show ip route eigrp` a été utilisée sur chaque routeur pour vérifier que toutes les routes apprises via EIGRP sont présentes et correctes.

```

R-LAN1
R-LAN1>en
R-LAN1#sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        a - application route
        + - replicated route, % - next hop override

Gateway of last resort is not set

D    192.168.10.0/24 [90/281856] via 197.5.50.6, 00:17:01, Ethernet1/3
      [90/281856] via 197.5.50.2, 00:17:01, Ethernet1/2
D    192.168.20.0/24 [90/281856] via 197.5.50.6, 00:17:01, Ethernet1/3
      [90/281856] via 197.5.50.2, 00:17:01, Ethernet1/2
D    192.168.30.0/24 [90/281856] via 197.5.50.6, 00:17:01, Ethernet1/3
      [90/281856] via 197.5.50.2, 00:17:01, Ethernet1/2
D    192.168.40.0/24 [90/281856] via 197.5.50.6, 00:17:01, Ethernet1/3
      [90/281856] via 197.5.50.2, 00:17:01, Ethernet1/2
D    192.168.50.0/24 [90/281856] via 197.5.50.6, 00:17:01, Ethernet1/3
      [90/281856] via 197.5.50.2, 00:17:01, Ethernet1/2
D    192.168.60.0/24 [90/281856] via 197.5.50.6, 00:17:01, Ethernet1/3
      [90/281856] via 197.5.50.2, 00:17:01, Ethernet1/2
D    192.168.100.0/24 [90/307200] via 197.5.50.10, 00:16:59, Ethernet0/0
D    192.168.200.0/24 [90/307200] via 197.5.50.14, 00:16:59, Ethernet0/1
      197.5.50.0/24 is variably subnetted, 9 subnets, 2 masks
D    197.5.50.16/30 [90/307200] via 197.5.50.14, 00:17:01, Ethernet0/1
      [90/307200] via 197.5.50.10, 00:17:01, Ethernet0/0
R-LAN1#

```

FIGURE 4.23 – Table de routage EIGRP sur R-LAN1

```

R-LAN2
R-LAN2#sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        a - application route
        + - replicated route, % - next hop override

Gateway of last resort is not set

D    192.168.10.0/24 [90/307456] via 197.5.50.9, 00:24:56, Ethernet0/1
D    192.168.20.0/24 [90/307456] via 197.5.50.9, 00:24:56, Ethernet0/1
D    192.168.30.0/24 [90/307456] via 197.5.50.9, 00:24:56, Ethernet0/1
D    192.168.40.0/24 [90/307456] via 197.5.50.9, 00:24:56, Ethernet0/1
D    192.168.50.0/24 [90/307456] via 197.5.50.9, 00:24:56, Ethernet0/1
D    192.168.60.0/24 [90/307456] via 197.5.50.9, 00:24:56, Ethernet0/1
D    192.168.200.0/24 [90/307200] via 197.5.50.18, 00:24:56, Ethernet0/2
      197.5.50.0/24 is variably subnetted, 7 subnets, 2 masks
D    197.5.50.0/30 [90/307200] via 197.5.50.9, 00:24:56, Ethernet0/1
D    197.5.50.4/30 [90/307200] via 197.5.50.9, 00:24:56, Ethernet0/1
D    197.5.50.12/30 [90/307200] via 197.5.50.18, 00:24:56, Ethernet0/2
      [90/307200] via 197.5.50.9, 00:24:56, Ethernet0/1
R-LAN2#

```

FIGURE 4.24 – Table de routage EIGRP sur R-LAN2

```
R-LAN3
R-LAN3>en
R-LAN3#sh ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        a - application route
        + - replicated route, % - next hop override

Gateway of last resort is not set

D        192.168.10.0/24 [90/307456] via 197.5.50.13, 00:26:32, Ethernet0/2
D        192.168.20.0/24 [90/307456] via 197.5.50.13, 00:26:32, Ethernet0/2
D        192.168.30.0/24 [90/307456] via 197.5.50.13, 00:26:32, Ethernet0/2
D        192.168.40.0/24 [90/307456] via 197.5.50.13, 00:26:32, Ethernet0/2
D        192.168.50.0/24 [90/307456] via 197.5.50.13, 00:26:32, Ethernet0/2
D        192.168.60.0/24 [90/307456] via 197.5.50.13, 00:26:32, Ethernet0/2
D        192.168.100.0/24 [90/307200] via 197.5.50.17, 00:26:32, Ethernet0/1
        197.5.50.0/24 is variably subnetted, 7 subnets, 2 masks
D          197.5.50.0/30 [90/307200] via 197.5.50.13, 00:26:32, Ethernet0/2
D          197.5.50.4/30 [90/307200] via 197.5.50.13, 00:26:32, Ethernet0/2
D          197.5.50.8/30 [90/307200] via 197.5.50.17, 00:26:32, Ethernet0/1
                        [90/307200] via 197.5.50.13, 00:26:32, Ethernet0/2
R-LAN3#
R-LAN3#
```

FIGURE 4.25 – Table de routage EIGRP sur R-LAN3

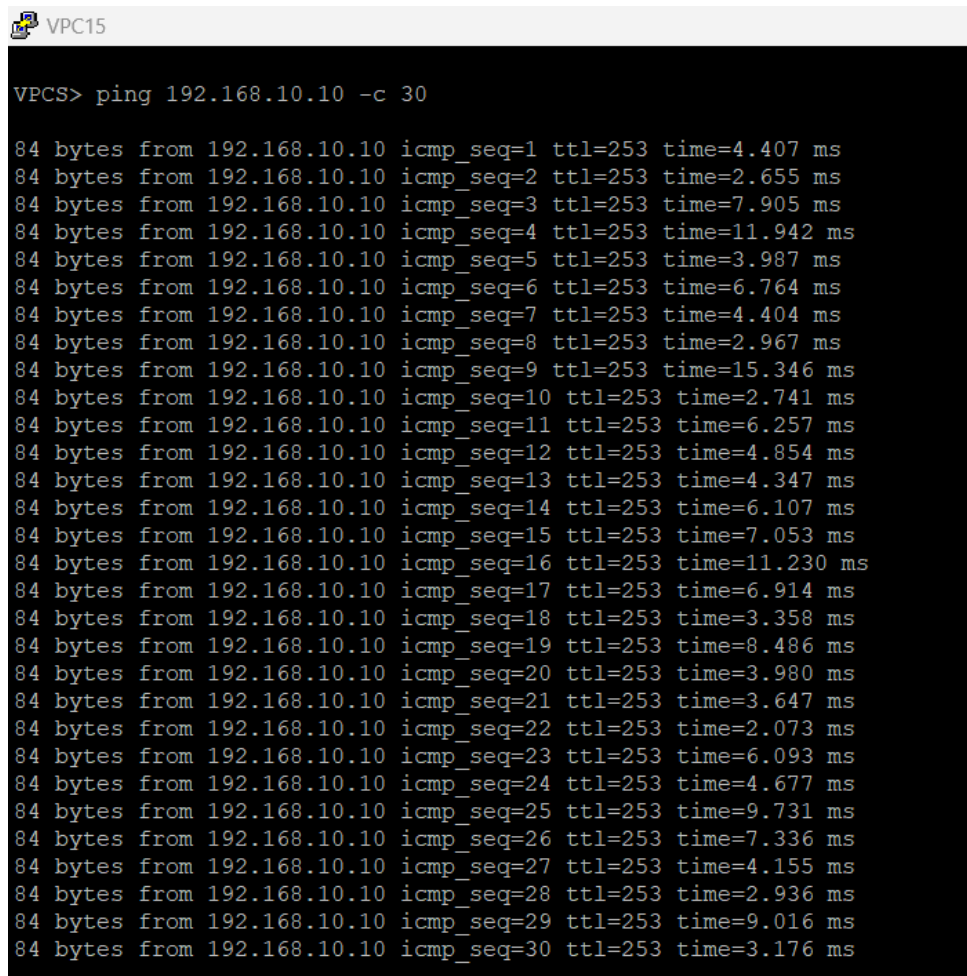
Étape 3 : Test de convergence

Une interface sur R-LAN2 a été désactivée pour simuler une panne. La convergence EIGRP a été observée et un ping a été lancé pour vérifier la continuité du trafic.

```
R-LAN2
R-LAN2>en
R-LAN2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-LAN2(config)#int e0/1
R-LAN2(config-if)#shut
R-LAN2(config-if)#en
*Oct 13 19:42:52.836: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 197.5.50.9 (Ethernet0/1) is down: interface down
R-LAN2(config-if)#end
R-LAN2#wr
Building configuration...

*Oct 13 19:42:54.835: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
*Oct 13 19:42:54.903: %SYS-5-CONFIG_I: Configured from console by console
*Oct 13 19:42:55.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down[OK]
R-LAN2#
```

FIGURE 4.26 – désactivation d’une interface sur R-LAN2



```
VPC15
VPCS> ping 192.168.10.10 -c 30

84 bytes from 192.168.10.10 icmp_seq=1 ttl=253 time=4.407 ms
84 bytes from 192.168.10.10 icmp_seq=2 ttl=253 time=2.655 ms
84 bytes from 192.168.10.10 icmp_seq=3 ttl=253 time=7.905 ms
84 bytes from 192.168.10.10 icmp_seq=4 ttl=253 time=11.942 ms
84 bytes from 192.168.10.10 icmp_seq=5 ttl=253 time=3.987 ms
84 bytes from 192.168.10.10 icmp_seq=6 ttl=253 time=6.764 ms
84 bytes from 192.168.10.10 icmp_seq=7 ttl=253 time=4.404 ms
84 bytes from 192.168.10.10 icmp_seq=8 ttl=253 time=2.967 ms
84 bytes from 192.168.10.10 icmp_seq=9 ttl=253 time=15.346 ms
84 bytes from 192.168.10.10 icmp_seq=10 ttl=253 time=2.741 ms
84 bytes from 192.168.10.10 icmp_seq=11 ttl=253 time=6.257 ms
84 bytes from 192.168.10.10 icmp_seq=12 ttl=253 time=4.854 ms
84 bytes from 192.168.10.10 icmp_seq=13 ttl=253 time=4.347 ms
84 bytes from 192.168.10.10 icmp_seq=14 ttl=253 time=6.107 ms
84 bytes from 192.168.10.10 icmp_seq=15 ttl=253 time=7.053 ms
84 bytes from 192.168.10.10 icmp_seq=16 ttl=253 time=11.230 ms
84 bytes from 192.168.10.10 icmp_seq=17 ttl=253 time=6.914 ms
84 bytes from 192.168.10.10 icmp_seq=18 ttl=253 time=3.358 ms
84 bytes from 192.168.10.10 icmp_seq=19 ttl=253 time=8.486 ms
84 bytes from 192.168.10.10 icmp_seq=20 ttl=253 time=3.980 ms
84 bytes from 192.168.10.10 icmp_seq=21 ttl=253 time=3.647 ms
84 bytes from 192.168.10.10 icmp_seq=22 ttl=253 time=2.073 ms
84 bytes from 192.168.10.10 icmp_seq=23 ttl=253 time=6.093 ms
84 bytes from 192.168.10.10 icmp_seq=24 ttl=253 time=4.677 ms
84 bytes from 192.168.10.10 icmp_seq=25 ttl=253 time=9.731 ms
84 bytes from 192.168.10.10 icmp_seq=26 ttl=253 time=7.336 ms
84 bytes from 192.168.10.10 icmp_seq=27 ttl=253 time=4.155 ms
84 bytes from 192.168.10.10 icmp_seq=28 ttl=253 time=2.936 ms
84 bytes from 192.168.10.10 icmp_seq=29 ttl=253 time=9.016 ms
84 bytes from 192.168.10.10 icmp_seq=30 ttl=253 time=3.176 ms
```

FIGURE 4.27 – Ping continu pendant la désactivation du lien sur R-LAN2

Étape 4 : Vérification de la redondance

Les chemins alternatifs configurés ont été testés afin de confirmer que le protocole EIGRP redirige correctement le trafic en cas de panne d'un lien principal.

```

R-LAN1
R-LAN1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

D    192.168.10.0/24 [90/281856] via 197.5.50.6, 00:03:27, Ethernet1/3
      [90/281856] via 197.5.50.2, 00:03:27, Ethernet1/2
D    192.168.20.0/24 [90/281856] via 197.5.50.6, 00:03:27, Ethernet1/3
      [90/281856] via 197.5.50.2, 00:03:27, Ethernet1/2
D    192.168.30.0/24 [90/281856] via 197.5.50.6, 00:03:27, Ethernet1/3
      [90/281856] via 197.5.50.2, 00:03:27, Ethernet1/2
D    192.168.40.0/24 [90/281856] via 197.5.50.6, 00:03:27, Ethernet1/3
      [90/281856] via 197.5.50.2, 00:03:27, Ethernet1/2
D    192.168.50.0/24 [90/281856] via 197.5.50.6, 00:03:27, Ethernet1/3
      [90/281856] via 197.5.50.2, 00:03:27, Ethernet1/2
D    192.168.60.0/24 [90/281856] via 197.5.50.6, 00:03:27, Ethernet1/3
      [90/281856] via 197.5.50.2, 00:03:27, Ethernet1/2
D    192.168.100.0/24 [90/332800] via 197.5.50.14, 00:02:39, Ethernet0/1
D    192.168.200.0/24 [90/307200] via 197.5.50.14, 01:02:39, Ethernet0/1
      197.5.50.0/24 is variably subnetted, 9 subnets, 2 masks
C    197.5.50.0/30 is directly connected, Ethernet1/2
L    197.5.50.1/32 is directly connected, Ethernet1/2
C    197.5.50.4/30 is directly connected, Ethernet1/3
L    197.5.50.5/32 is directly connected, Ethernet1/3
C    197.5.50.8/30 is directly connected, Ethernet0/0
L    197.5.50.9/32 is directly connected, Ethernet0/0
C    197.5.50.12/30 is directly connected, Ethernet0/1
L    197.5.50.13/32 is directly connected, Ethernet0/1
D    197.5.50.16/30 [90/307200] via 197.5.50.14, 00:02:39, Ethernet0/1
R-LAN1#
R-LAN1#

```

FIGURE 4.28 – Chemins alternatifs et redondance EIGRP

Conclusion

Les tests réalisés dans l'environnement **EVE-NG** ont validé le bon fonctionnement de l'infrastructure réseau déployée. Les résultats confirment que la connectivité entre les **VLANs** est opérationnelle et que les mécanismes de redondance (**EtherChannel**, **VRRP**) assurent une continuité de service efficace lors de simulations de panne. Le protocole de routage **EIGRP** a démontré sa capacité à maintenir la connectivité via des chemins alternatifs, tandis que le **MSTP** garantit une topologie stable sans boucles. Cette validation complète atteste que l'architecture mise en place répond pleinement aux exigences de **performance**, de **résilience** et de **fiabilité** nécessaires pour un déploiement en environnement de production.

Annexe

1. Installation de VMware Workstation Pro

Étape 1

L'installateur de VMware Workstation Pro est téléchargé depuis le site officiel et exécuté pour lancer le processus d'installation, comme indiqué dans la figure 1.

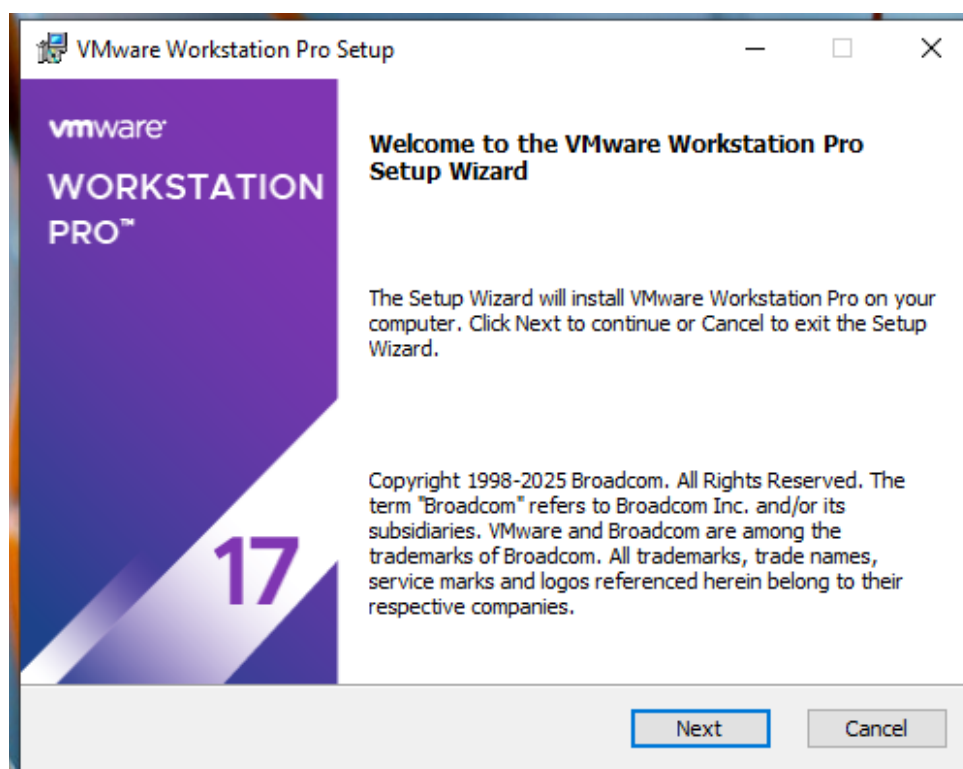


FIGURE 1 – Lancement de l'installation de VMware Workstation Pro

Étape 2

L'installation standard est sélectionnée, le processus est lancé et finalisé, puis VMware Workstation Pro est démarré pour vérifier le bon fonctionnement, comme le montre la figure 2.

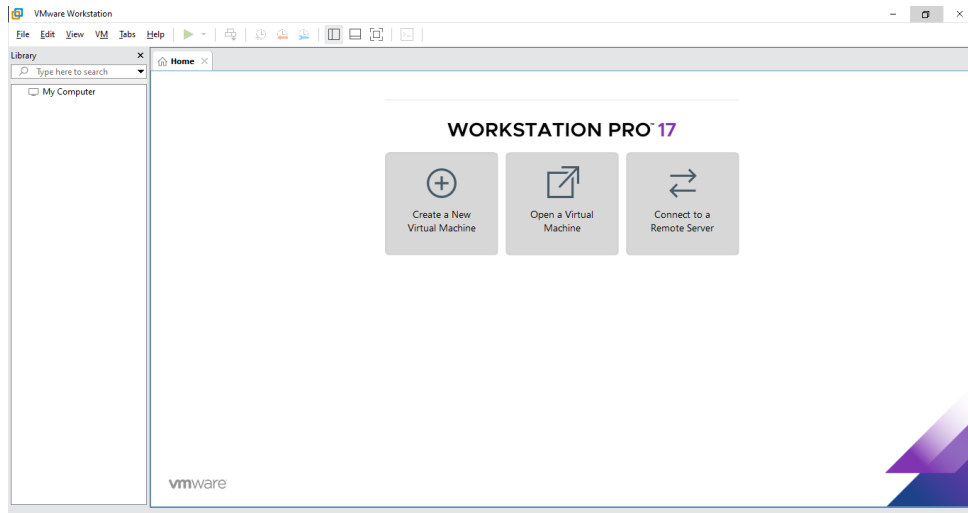


FIGURE 2 – Installation et configuration finale de VMware Workstation Pro

2. Intégration de l'image ISO d'EVE-NG sous VMware

Étape 1

Une nouvelle machine virtuelle est créée dans VMware Workstation Pro et les ressources matérielles de la machine sont configurées, en attribuant la mémoire RAM, le nombre de processeurs et l'espace disque nécessaires, comme le montre la figure 3.

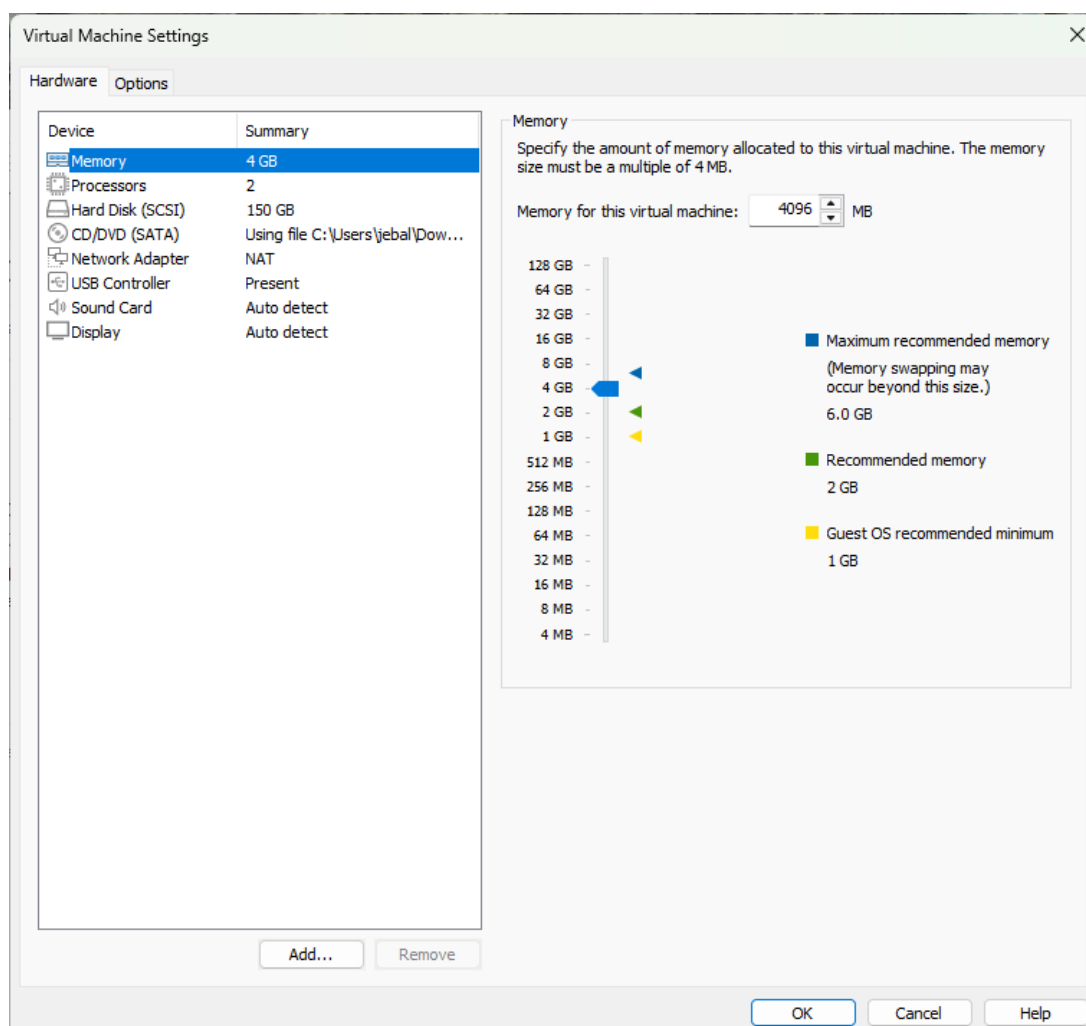


FIGURE 3 – Configuration des ressources matérielles de la VM

Étape 2

L'image ISO officielle de EVE-NG est sélectionnée comme support d'installation, comme l'illustre la figure 4.

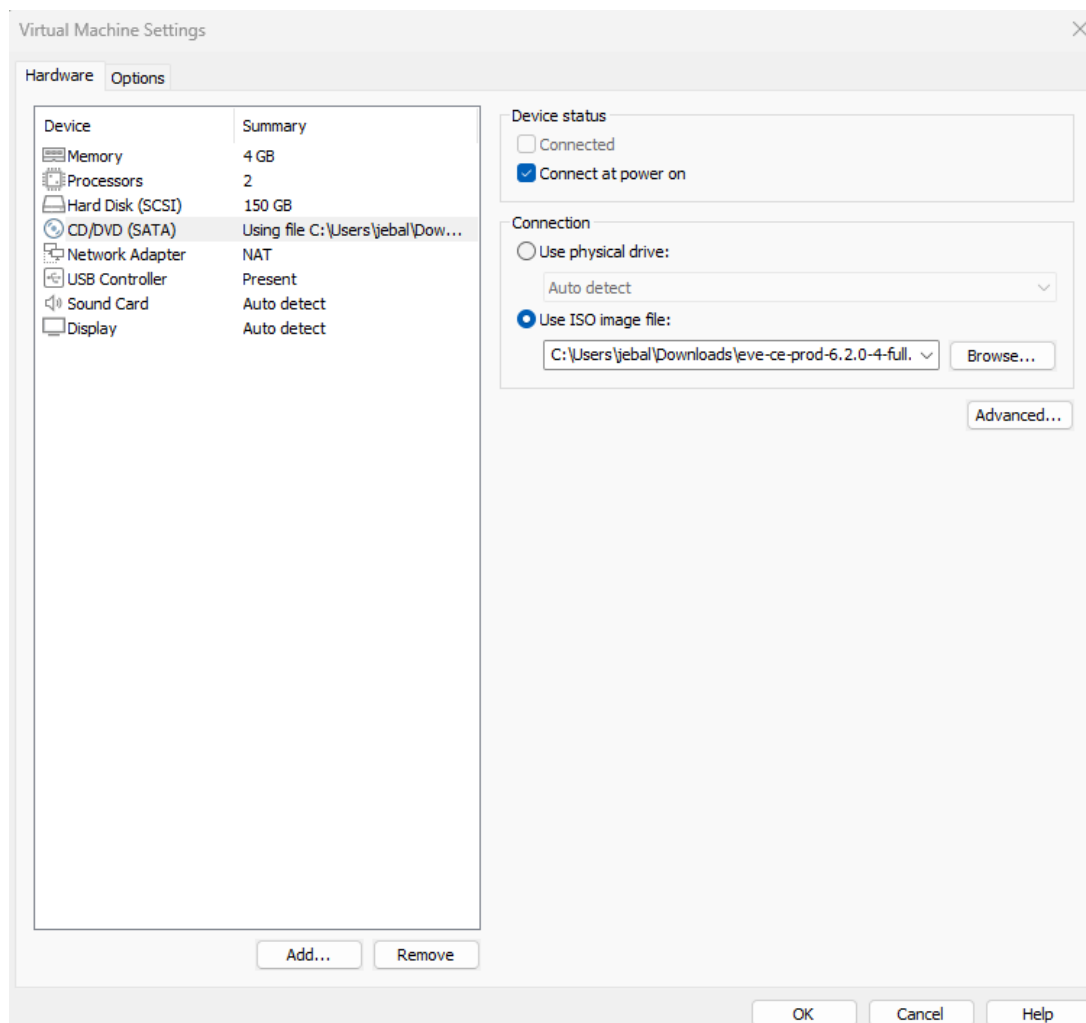


FIGURE 4 – Création de la machine virtuelle et choix de l’image ISO

Étape 3

Après le démarrage de la machine virtuelle, l’installation de EVE-NG est lancée et l’assistant d’installation apparaît, comme illustré dans la figure 5.

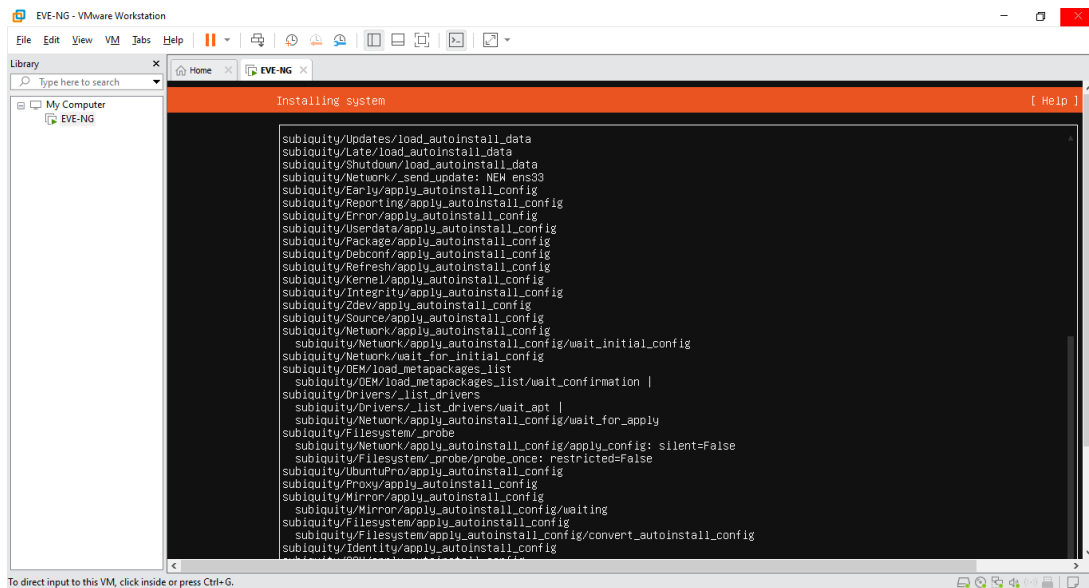


FIGURE 5 – Lancement de l'installation de EVE-NG

Étape 4

L'assistant guide l'utilisateur dans la configuration des paramètres initiaux, en commençant par la sélection de la langue (figure 6).

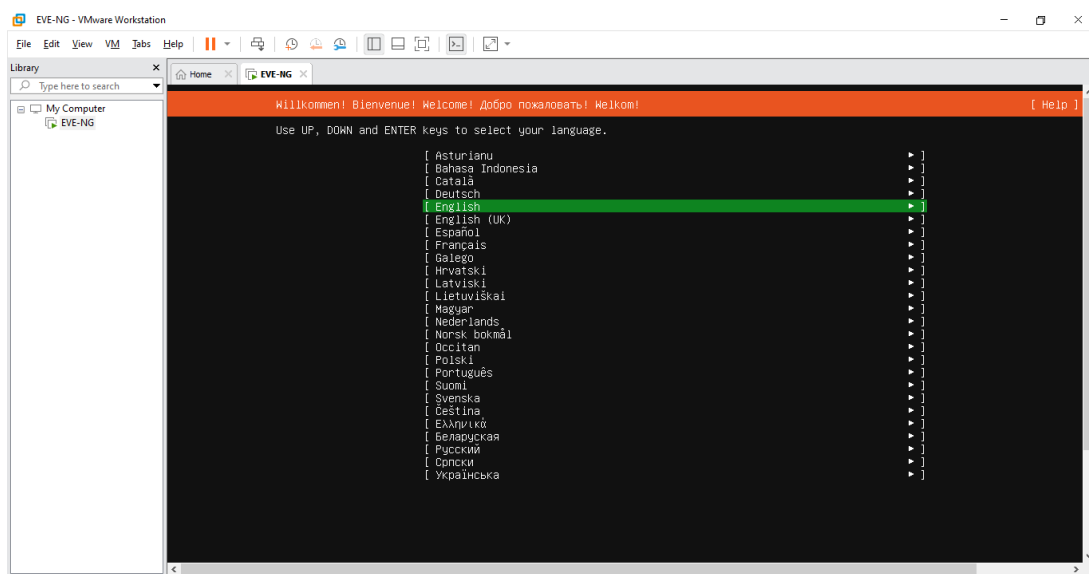


FIGURE 6 – Choix de la langue d'installation

Étape 5

Ensuite, le mot de passe administrateur est défini pour sécuriser l'accès à la plateforme (figure 7).

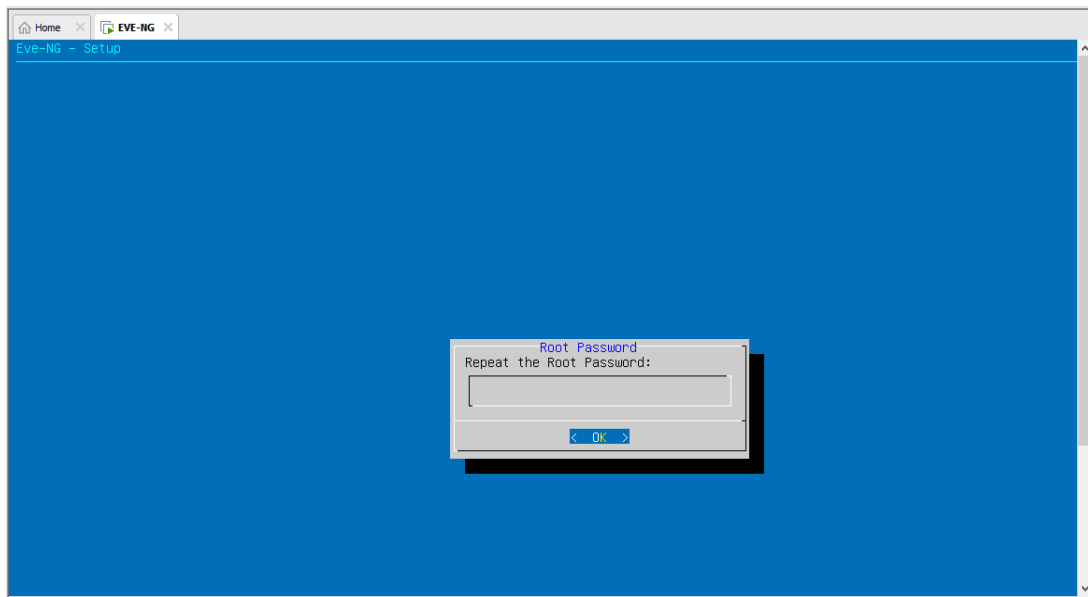


FIGURE 7 – Définition du mot de passe administrateur

Étape 6

Enfin, la configuration réseau est effectuée. L'adresse IP peut être obtenue via DHCP ou attribuée manuellement en mode statique, comme le montre la figure 8.

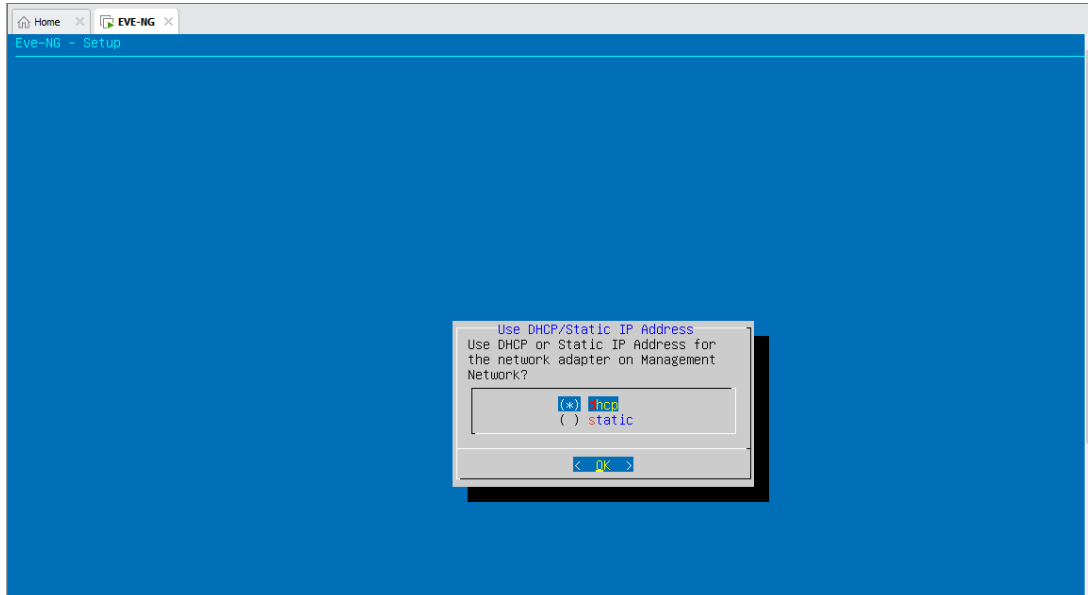


FIGURE 8 – Attribution de l'adresse IP via DHCP

Étape 7

À la fin du processus d'installation, la machine redémarre automatiquement et EVE-NG est prêt à être utilisé, comme indiqué dans la figure 9.

```
Eve-ng (default root password is 'eve')
Use http://192.168.30.128/

WARNING: neither Intel VT-x or AMD-V found

eve-ng login: [ 20.937976] cloud-init[2006]: Cloud-init v. 23.3.3-0ubuntu0~22.04.1 running 'modules:final' at Thu, 09 Oct 2025 20:47:07 +0000. Up 20.80 second
s.
[ 21.029664] cloud-init[2006]: Cloud-init v. 23.3.3-0ubuntu0~22.04.1 finished at Thu, 09 Oct 2025 20:47:07 +0000. DataSource DataSourceNone. Up 21.02 seconds
[ 21.032338] cloud-init[2006]: 2025-10-09 20:47:07,677 - cc_final_message.py[WARNING]: Used fallback datasource
```

FIGURE 9 – Adresse IP attribuée après installation

3. Installation de WinSCP

Étape 1

Le fichier d'installation de WinSCP est téléchargé depuis le site officiel puis exécuté, comme montré dans la figure 10.

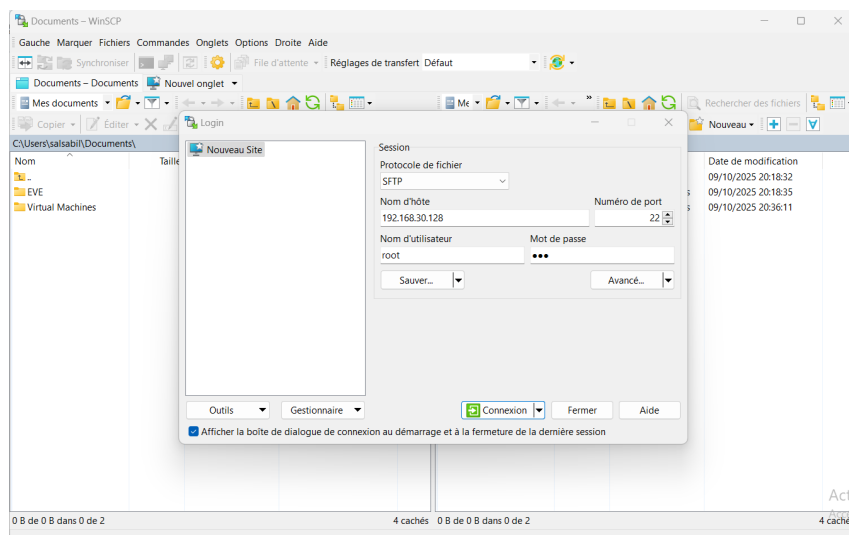


FIGURE 10 – Lancement de l'installation de WinSCP

Étape 2

L'installation standard est choisie, le processus est finalisé et l'application est ouverte pour vérifier son bon fonctionnement, comme illustré dans la figure 11.

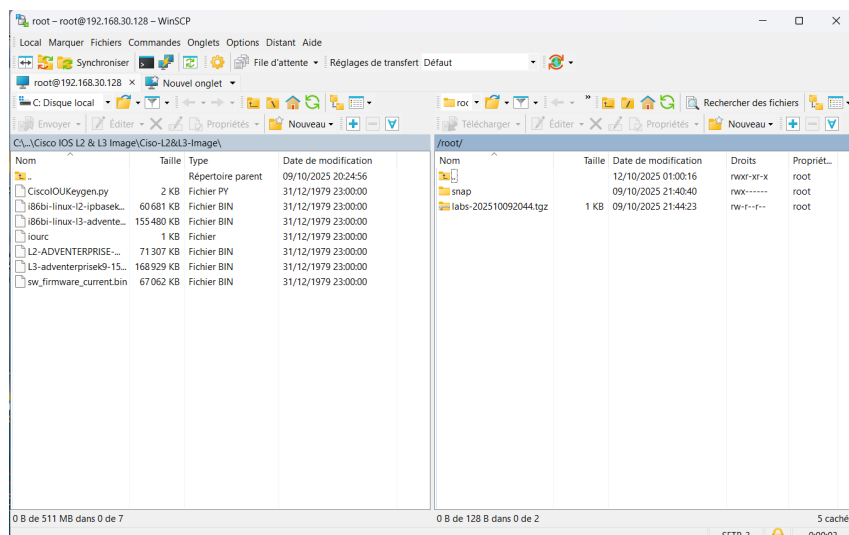


FIGURE 11 – Interface de WinSCP après installation

4. Installation et utilisation de PuTTY

Étape 1

PuTTY est installé automatiquement avec le client-side EVE-NG, ou peut être téléchargé séparément depuis le site officiel, comme montré dans la figure 12.

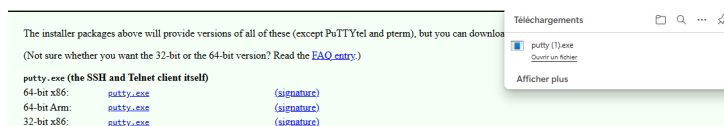


FIGURE 12 – Installation de PuTTY

Étape 2

Une connexion SSH est établie avec la machine EVE-NG en saisissant l'adresse IP et le port 22, comme indiqué dans la figure 13.

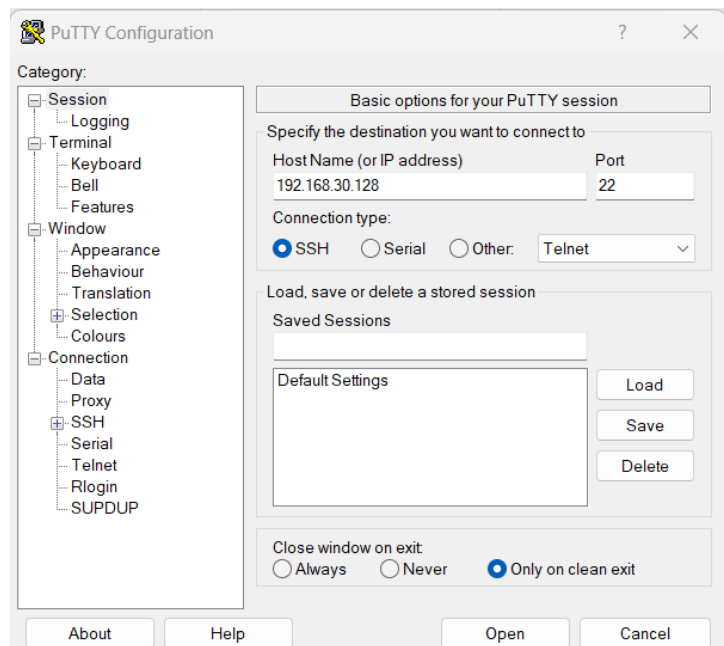


FIGURE 13 – Connexion SSH à EVE-NG avec PuTTY

Étape 3

La console de PuTTY permet ensuite d'exécuter les commandes Linux nécessaires à la gestion des images Cisco et à la configuration de l'environnement, comme illustré dans la figure 14.

```

root@eve-ng: ~
login as: root
root@192.168.30.128's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.7.5-eveng-6-ksm+ x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of lun. 20 oct. 2025 12:01:35 UTC

System load:  0.35302734375    Processes:            266
Usage of /:   8.7% of 145.12GB Users logged in:             0
Memory usage: 26%             IPv4 address for pnet0: 192.168.30.128
Swap usage:   0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

La maintenance de sécurité étendue pour Applications n'est pas activée.

247 mises à jour peuvent être appliquées immédiatement.
158 de ces mises à jour sont des mises à jour de sécurité.
  
```

FIGURE 14 – Console de gestion de EVE-NG via PuTTY

Remarque : La différence de couleur observée dans la console PuTTY (texte blanc ou orange) résulte d'un paramétrage d'affichage propre à la plateforme EVE-NG. Ce phénomène, sans impact

sur le fonctionnement du réseau, a été identifié afin d'éviter toute confusion avec des captures d'écran externes ou non issues du projet.

5. Transfert des images Cisco IOL via WinSCP

Étape 1

Connexion à la machine EVE-NG à l'aide de l'adresse IP, du nom d'utilisateur et du mot de passe administrateur, comme indiqué dans la figure 15.

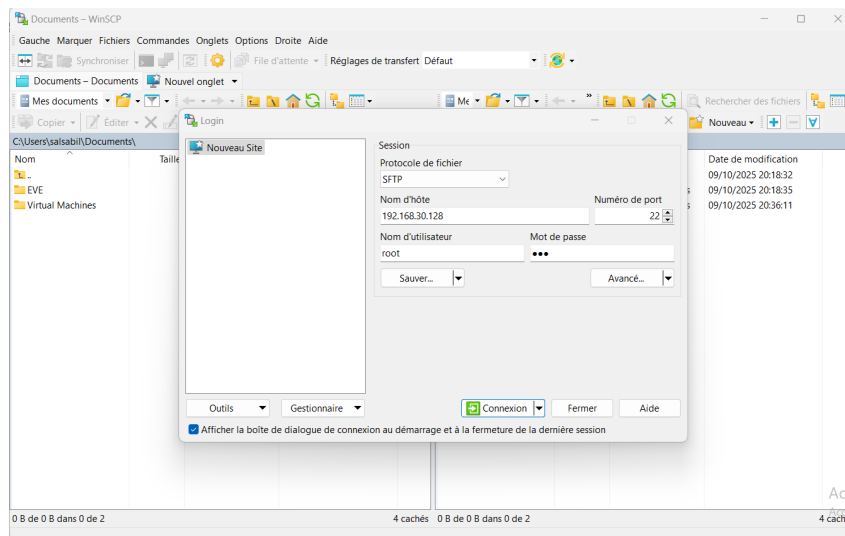


FIGURE 15 – Connexion à EVE-NG via WinSCP

Étape 2

Les fichiers binaires Cisco IOL sont transférés dans le répertoire `/opt/unetlab/addons/iol/bin`, comme illustré dans la figure 16.

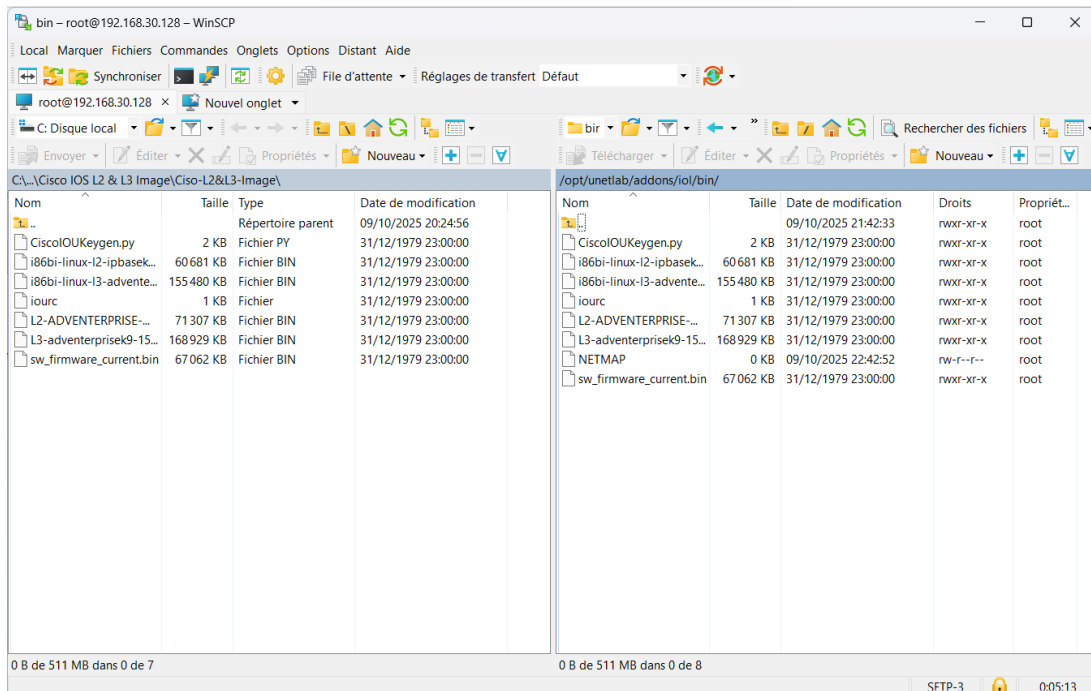


FIGURE 16 – Transfert des fichiers Cisco IOL vers EVE-NG

Étape 3

Une fois les fichiers copiés, les permissions sont configurées en exécutant les commandes appropriées sur la VM EVE-NG (via SSH ou console), comme indiqué dans la figure 17.

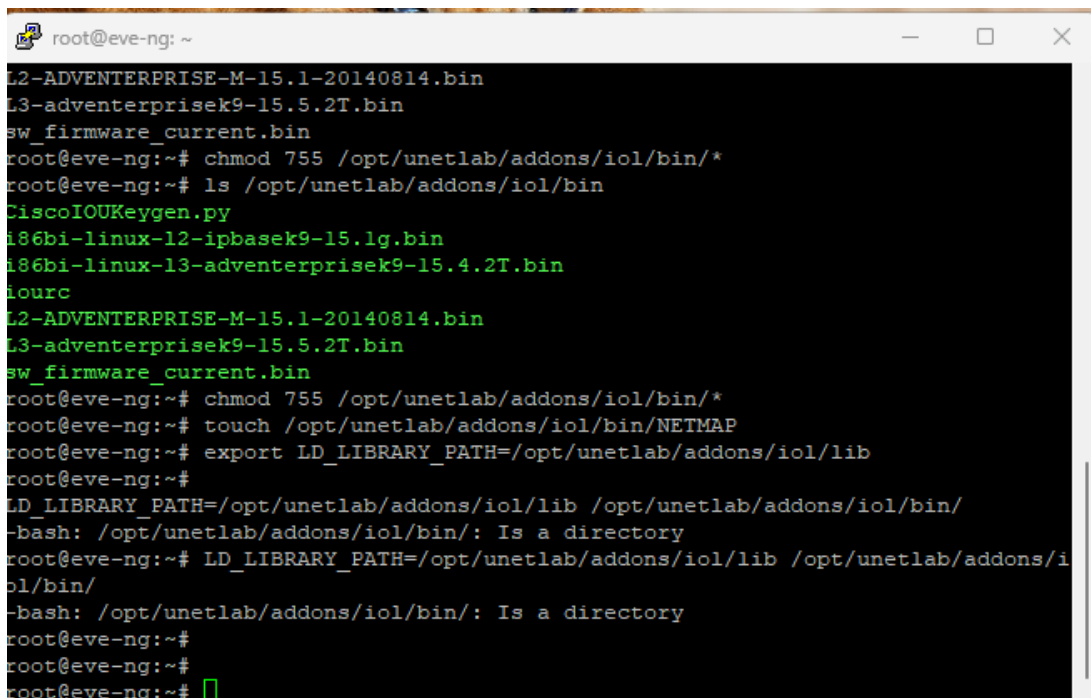


FIGURE 17 – Configuration des permissions pour les binaires Cisco IOL

6. Installation du client Windows (client-side EVE-NG)

Étape 1

Le package client-side est téléchargé depuis la documentation officielle EVE-NG. La page de téléchargement précise que l'installation inclut automatiquement les utilitaires nécessaires (PuTTY, Wireshark, VNC Viewer, etc.), comme indiqué dans la figure 18.

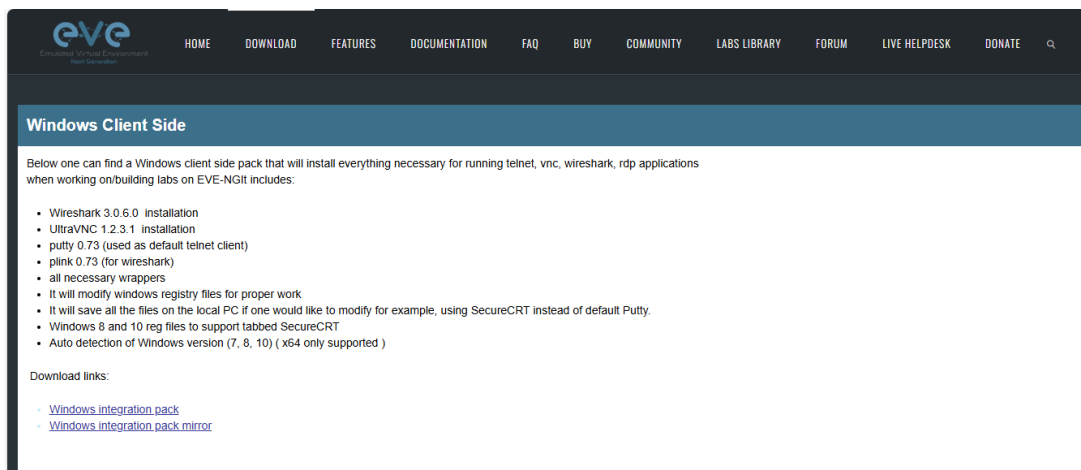


FIGURE 18 – Téléchargement du package client-side depuis la documentation officielle EVE-NG

Étape 2

Le fichier d'installation EVE-NG-Win-Client-Pack.exe est exécuté sur la machine Windows, déclenchant l'assistant d'installation comme montré dans la figure 19.

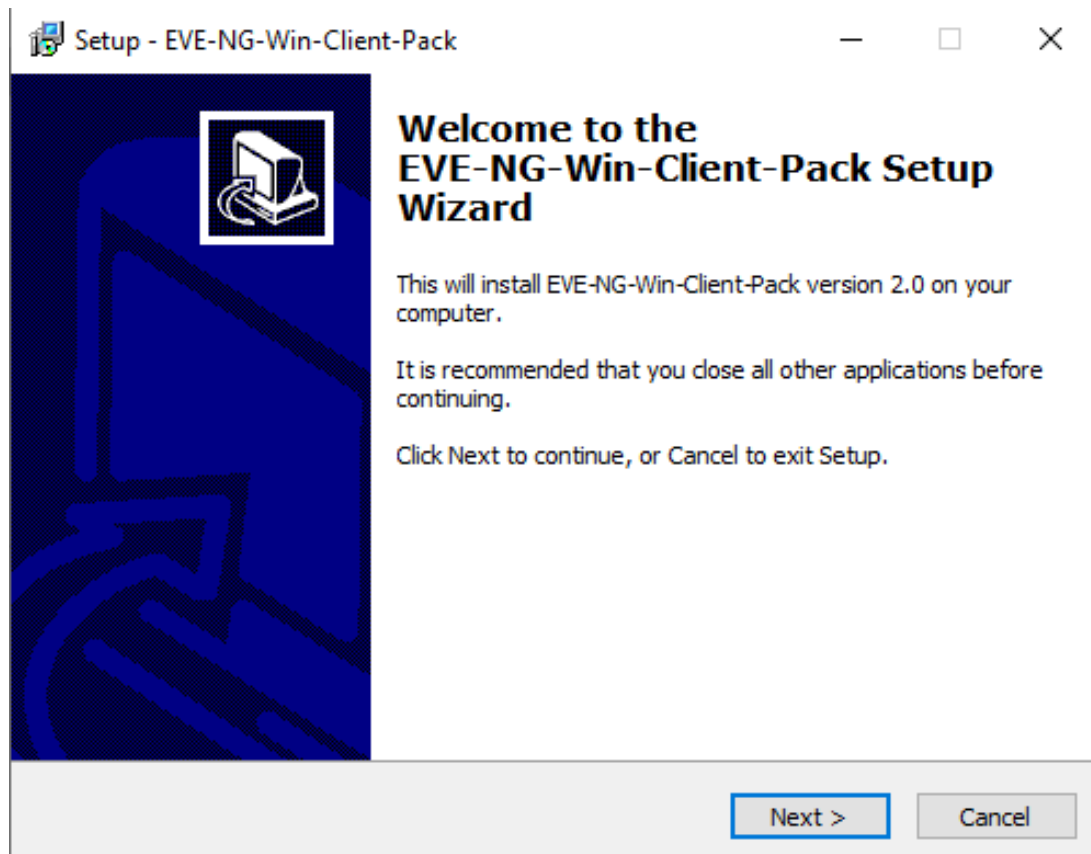


FIGURE 19 – Lancement de l'installation du package client-side sur Windows

Conclusion Générale

Ce projet a permis de concevoir et de déployer une infrastructure réseau hiérarchique moderne dans un environnement virtualisé. L'utilisation des plateformes EVE-NG et VMware Workstation Pro a facilité la mise en œuvre, la simulation et la validation d'une architecture complexe dans un cadre flexible et contrôlé.

L'intégration des protocoles EIGRP, VRRP, MSTP et EtherChannel a permis d'assurer la redondance, la résilience et la performance du réseau. Les tests de validation ont confirmé la stabilité des communications, la continuité du service et la rapidité de convergence des mécanismes déployés.

Les objectifs fixés ont été atteints. L'architecture proposée constitue une solution scalable, hautement disponible et fiable, démontrant l'efficacité des environnements virtualisés comme alternative économique et flexible aux infrastructures physiques traditionnelles.