

**Ecole Supérieure Privée des Technologies et de
l'Ingénierie**

Rapport de Projet de sécurité Réseaux

Conception et mise en place de la Solution VPN- MPLS

Réalisé par : Raslen Othmani
Issam ben hamad

Encadré par : Mr Hdiji TAREK

Table des matières

Introduction générale	1
1 Conception et Mise en place de la Solution VPN-MPLS	3
1.1 Introduction	4
1.2 Technologie de Service VPN-MPLS	4
1.2.1 Le protocole VPN (Virtual Private Network)	5
1.3 Le protocole MPLS	6
1.4 Le protocole OSPF	7
1.5 Le protocole BGP	8
1.6 Architecture de la solution VPN-MPLS	8
1.7 Environnement de travail (GNS3 et VMware)	10
1.7.1 VMware workstation	10
1.7.2 GNS3	11
1.8 Topologie de l'université TEKUP	11
1.9 Mise en place de VPN-MPLS	12
1.9.1 Configuration de base de l'adressage de chaque Interface	12
1.9.2 Configuration des protocoles de routage	13
1.9.3 Configuration de MPLS	16
1.9.4 LFIB	18
1.9.5 Binding	19
1.9.6 Mise en place des VPN	20
1.9.7 table de routage	21
1.9.8 Validation et test de la connexion	22
1.10 Conclusion	23
2 Conception et mise en place de la solution de réseau LAN Etendu Tekup	24
2.1 Introduction	25
2.2 Architecture de réseau LAN étendu de Tekup	25
2.3 Conception de la Solution LAN	26
2.4 Description de la Solution Redondante de LAN	26
2.5 Mise en place de la Solution de LAN Redondante	28
2.6 Siège	28
2.6.1 Création de VLAN	28
2.6.2 Lien entre Switch Layer 2 et Switch Layer3 "Federateur". sont des Trunks tel que Native Vlan 20	29
2.6.3 Sécurité des appareils :	30
2.6.4 IP address Management de VLAN 20	33
2.6.5 Service DHCP	33

2.6.6	Redondance HSRP	34
2.6.7	Ethernet Channel mode TRUNK	35
2.7	Branch 1	37
2.7.1	Création de VLAN	37
2.7.2	Assignation de PC au VLAN	37
2.7.3	Lien entre Switch et routeur CE-Branch1	38
2.7.4	Routage Inter-VLAN	39
2.7.5	@IPManagement de Swich Layer2 (Sw3) de VLAN101	40
2.7.6	Service DHCP au niveau Router CE-Branch1	41
2.7.7	Sécurité des appareils	42
2.8	Branch 2	43
2.8.1	Création de VLAN	43
2.8.2	Assignation de PC au VLAN	44
2.8.3	Lien entre Switch et routeur CE-Branch2	45
2.8.4	Routage Inter-VLAN	46
2.8.5	adresse IP Management de Switch Layer2 (Sw4) de VLAN103	47
2.8.6	Service DHCP au niveau Router CE-Branch2	47
2.8.7	Sécurité des appareils	48
2.9	Test et Validation des Services de la Solution Redondante	49
2.10	Conclusion	50
3	Conception et mise en place de la Solution de Monitoring et Sécurité	
	AAA	51
3.1	Introduction	52
3.2	Choix de la Solution Monitoring	53
3.3	Model de fonctionnement de la Solution Monitoring	53
3.4	Mise en place de la Solution Monitoring	54
3.5	Test et Validation de la Solution Monitoring	58
3.5.1	Surveillance des Périphériques avec Nagios Core	59
3.6	Description de la Solution AAA	59
3.7	Mise en place de la Solution de sécurité AAA de Tekup	60
3.8	Test et Validation des Services de la solution de sécurité AAA	67
3.9	conclusion	67
3.10	Conclusion general	69

Table des figures

1.1	Université TEK-UP	4
1.2	Architecture de la solution VPN-MPLS	6
1.3	Architecture de la solution VPN-MPLS	10
1.4	Gns3 vm	10
1.5	GNS3	11
1.6	Core de notre réseau	12
1.7	Adressage de PE1	12
1.8	Adressage de PE2	13
1.9	Adressage de P1	13
1.10	Adressage de P2	13
1.11	table de Voisinage OSPF de PE1	13
1.12	table de Voisinage OSPF de PE2	14
1.13	table de Voisinage OSPF de P1	14
1.14	table de Voisinage OSPF de P2	14
1.15	table de routage OSPF de PE1	14
1.16	table de routage OSPF de PE2	15
1.17	table de routage OSPF de P1	15
1.18	table de routage OSPF de P2	15
1.19	Configuration de MPLS de PE1	16
1.20	Configuration de MPLS de PE2	16
1.21	Configuration de MPLS de P1	17
1.22	Configuration de MPLS de P2	17
1.23	vérification de la LFIB de PE1	18
1.24	vérification de la LFIB de PE2	18
1.25	vérification de la LFIB de P1	19
1.26	vérification de la LFIB de P2	19
1.27	affichage des bindings des labels MPLS récupérés par LDP de PE1	19
1.28	affichage des bindings des labels MPLS récupérés par LDP de PE2	20
1.29	affichage des bindings des labels MPLS récupérés par LDP de P1	20
1.30	Affichage Instance BGP de PE1	21
1.31	Affichage Instance BGP de PE2	21
1.32	Affichage la table de routage de VRF de VPN Customer1 et VPN Customer2 de PE1	22
1.33	ping CE11 TO CE12	23
1.34	ping CE21 TO CE22	23
2.35	Architecture de Partie 2	25
2.36	VLAN 10 : data1	28
2.37	VLAN 15 : data2	29
2.38	Vlan 20 : management	29
2.39	Mode Trunk entre layer2 et layer3	30

2.40	Mode Trunk entre sw4 et pc 3	31
2.41	show interfaces trunk federateur 1	31
2.42	show interfaces trunk federateur 2	32
2.43	Passwords CE11	32
2.44	Passwords CE21	32
2.45	Passwords CE22	33
2.46	Passwords Federateur1	33
2.47	Passwords Federateur2	34
2.48	Service dhcp federateur1	34
2.49	Standby fed1	35
2.50	Ethernet channel mode trunk federateur 1	35
2.51	Ethernet channel mode trunk federateur 1	36
2.52	Ethernet channel mode trunk federateur 2	36
2.53	Ethernet channel mode trunk federateur 2	37
2.54	show Vlan	37
2.55	Affectation du port	38
2.56	Config trunk de switch sw3 et routeur ce-Branch1	38
2.57	routage Inter-vlan	39
2.58	IPManagement de Swich Layer2 (Sw3) de VLAN101	40
2.59	config service dhcp au niveau routeur CE-Branch1	41
2.60	ip dhcp de pc4	41
2.61	password ce12	42
2.62	password sw3	43
2.63	creation de vlan 103 et 104	44
2.64	Affectation de port	44
2.65	Mode trunk sw4	45
2.66	routage Inter-vlan	46
2.67	IP Management de Switch Layer2 (Sw4) de VLAN103	47
2.68	Service DHCP au niveau Router CE-Branch2	47
2.69	password ce22	48
2.70	password sw4	48
2.71	Redondance HSRP sur le fédérateur 1	49
2.72	Redondance HSRP sur le fédérateur 2	49
2.73	Configuration DHCP réussie sur le PC1	49
2.74	Vérification de la connexion entre PC1 et PC2	49
2.75	Vérification de la connexion entre PC3 et PC4	50
2.76	Tracé de route vers PC2 depuis PC1	50
2.77	Tracé de route vers PC4 depuis PC3	50
3.78	Architecture de Partie 3	52
3.79	Logo de Nagios Core	53
3.80	Configuration de MySQL	56
3.81	Interface de configuration de connexion	57
3.82	Authentication au Nagios Cores	58
3.83	Interface Web de Nagios Core	58
3.84	Vérification de la connexion entre nagios et le federateur1	59
3.85	Surveillance des Périphériques avec Nagios Core	59
3.86	mise en place server AAA en siege2	62
3.87	mise en place server AAA en SW2	62
3.88	mise en place server AAA en Federateur 2	63

3.89	mise en place server AAA en siege1	63
3.90	mise en place server AAA en Branch1	64
3.91	mise en place server AAA en Branche2	64
3.92	mise en place server AAA en SW4	65
3.93	mise en place server AAA en SW1	65
3.94	mise en place server AAA en Federateur1	66
3.95	mise en place server AAA en SW3	66
3.96	Vérification de la connexion entre radius et le federateur2	67
3.97	Vérification de la connexion entre radius et le federateur2	67
3.98	Vérification de la connexion entre radius et le federateur2	67

Introduction générale

La mise en place d'une infrastructure réseau efficace est cruciale pour répondre aux exigences croissantes de connectivité, de performance et de sécurité dans le monde des télécommunications. Dans ce contexte, le déploiement d'une architecture IP/MPLS (Internet Protocol/Multiprotocol Label Switching) occupe une place prépondérante en offrant une solution robuste pour la gestion de flux de données à travers des réseaux étendus.

Ce rapport vise à présenter en détail la maquette de configuration du modèle Backbone IP/MPLS, une étape cruciale dans la conception et la mise en œuvre d'une infrastructure réseau de haute qualité. L'objectif principal est de fournir une vision holistique de la configuration du backbone IP/MPLS, en mettant l'accent sur les éléments essentiels tels que les équipements, les protocoles, les politiques de routage, la gestion de la qualité de service (QoS) et les mécanismes de sécurité.

Nous explorerons les différentes couches de la pile protocolaire, en mettant en lumière l'intégration harmonieuse de l'IP et du MPLS pour améliorer l'efficacité du routage et la gestion du trafic. L'accent sera également mis sur les aspects liés à la scalabilité, à la résilience et à la flexibilité de l'infrastructure, en mettant en œuvre des techniques avancées telles que la distribution de label, la convergence rapide des liaisons et la gestion proactive des incidents.

En outre, ce rapport mettra en évidence les meilleures pratiques de configuration pour garantir une exploitation optimale du réseau, en prenant en compte les exigences spécifiques liées à la connectivité, à la disponibilité des services et à la sécurité des données. Les scénarios de cas d'utilisation et les exemples concrets faciliteront la compréhension des concepts abordés, offrant ainsi une ressource complète pour les professionnels chargés de la conception et de la maintenance des réseaux IP/MPLS.

En conclusion, la maquette de configuration du modèle Backbone IP/MPLS est essentielle pour établir un fondement solide et fiable dans le domaine des réseaux de télécommunications. Ce rapport vise à fournir une orientation approfondie pour la mise en place

d'une infrastructure robuste, flexible et performante, répondant ainsi aux besoins actuels et futurs des opérateurs de réseaux.

chapitre 1

Conception et Mise en place de la Solution VPN-MPLS

1.1 Introduction

La création du Service VPN-MPLS à l'université TEK-UP marque une avancée essentielle pour assurer une connectivité sécurisée, stable et efficace entre les divers sites éloignés. Ce segment examine en détail les divers éléments de cette solution, couvrant la technologie fondamentale, les aspects pratiques du déploiement ainsi que l'architecture et la configuration du réseau.



FIGURE 1.1 – Université TEK-UP

1.2 Technologie de Service VPN-MPLS

La technologie VPN-MPLS repose sur l'affectation de labels MPLS aux paquets de données, permettant ainsi un routage efficace et une isolation des flux de trafic entre différents utilisateurs ou sites. Ce mécanisme de commutation de label offre une segmentation logique du réseau, garantissant que le trafic d'un VPN particulier reste isolé des autres, tout en optimisant les performances du réseau.

Cette section du rapport explorera en détail les mécanismes sous-jacents à la technologie de service VPN-MPLS, notamment la manière dont les labels MPLS sont utilisés pour définir des chemins spécifiques à travers le réseau, assurant ainsi la confidentialité des données et la cohérence des performances.

1.2.1 Le protocole VPN (Virtual Private Network)

Définition d'un Virtual Private Network (VPN)

Le réseau privé virtuel, ou Virtual Private Network (VPN), est un service destiné à protéger votre activité en ligne. Il renforce la sécurité de votre connexion internet lorsque vous vous trouvez dans un environnement non sécurisé. Un VPN offre également l'avantage de préserver votre confidentialité en ligne. Un atout pour les pirates informatiques qui souhaitent masquer leurs actes de malveillance. Découvrez tout ce que vous devez savoir sur le VPN et comment il peut vous être utile.

À quoi sert un réseau privé virtuel

Les utilisateurs d'un Virtual Private Network ont trois raisons majeures d'utiliser ce réseau privé virtuel.

Assurer la confidentialité des données sensibles pendant les connexions à internet Lorsque vous vous connectez à un site internet et que vous procédez à un achat en ligne, vos données sensibles peuvent être détournées et volées. En utilisant un service VPN, vos données sont cryptées. Le décryptage de vos informations ne peut être fait par un tiers qui ne possède pas la clé de chiffrement.

Préserver l'anonymat des utilisateurs Votre adresse IP représente votre carte d'identité en ligne. Tous les sites que vous consultez tracent votre IP, qui est directement liée à votre connexion internet. Il est donc très facile de suivre toute votre activité sur internet. En délivrant une adresse IP virtuelle, vous êtes intraçable. Un VPN vous offre l'anonymat dont vous avez besoin.

Attention cependant : si votre fournisseur d'accès internet n'a plus de visibilité sur vos différentes connexions, votre service VPN conserve un journal de logs. Vos données

restent stockées un temps sur les serveurs de votre fournisseur VPN.

Assurer la sécurité de votre connexion internet et de votre réseau Le VPN assure votre sécurité en ligne. Par exemple, il sécurise votre connexion internet si vous vous servez des réseaux Wi-Fi publics pour travailler ou non. Il détecte les intrusions non autorisées. Ainsi, le service interrompt tous vos programmes comme un mécanisme de défense lorsqu'il suspecte un trafic inhabituel. Cette fonctionnalité est d'ailleurs utilisée en entreprise. Les administrateurs peuvent également gérer les accès aux réseaux aux utilisateurs travaillant à distance.

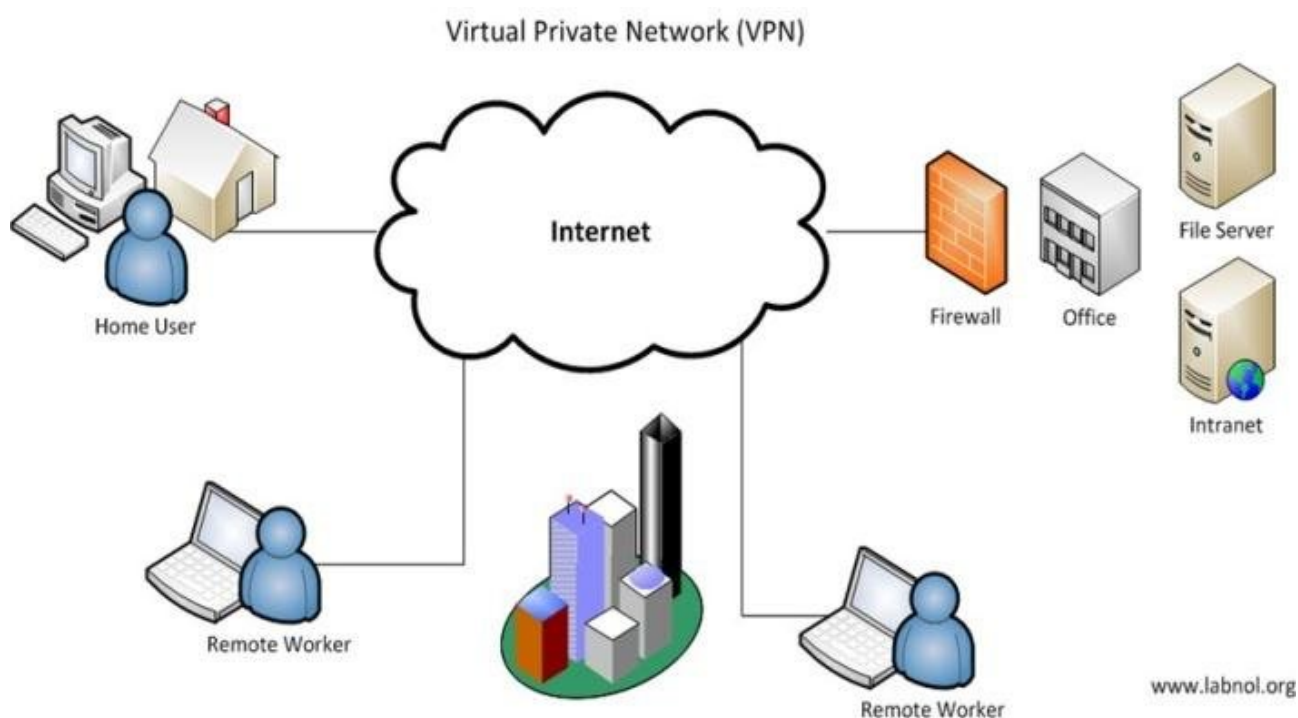


FIGURE 1.2 – Architecture de la solution VPN-MPLS

1.3 Le protocole MPLS

Multiprotocol Label Switching (MPLS) est un protocole de réseau de données utilisé pour diriger et acheminer le trafic de manière efficace à travers un réseau. Contrairement aux méthodes traditionnelles de routage IP qui examinent chaque paquet de données en fonction de son adresse IP, MPLS utilise des étiquettes (labels) pour identifier les chemins à travers le réseau. Ces étiquettes sont attribuées à chaque paquet de données à l'entrée du réseau et sont utilisées pour déterminer le chemin optimal vers sa destination, en évitant ainsi les recherches de routage complexes à chaque saut.

MPLS offre plusieurs avantages, notamment une meilleure qualité de service (QoS), une ingénierie du trafic améliorée, une gestion efficace des réseaux privés virtuels (VPN), et une capacité à prendre en charge des services multiprotocoles. Il est couramment utilisé par les fournisseurs de services Internet (ISP) et dans les réseaux d'entreprise pour améliorer les performances et la fiabilité des communications.

1.4 Le protocole OSPF

Le protocole OSPF (Open Shortest Path First) est un protocole de routage interne utilisé dans les réseaux IP pour déterminer les meilleurs chemins entre les routeurs et, ainsi, acheminer le trafic de manière efficace. Il appartient à la famille des protocoles de routage à vecteur de lien et utilise l'algorithme Dijkstra pour calculer les chemins les plus courts vers toutes les destinations dans un réseau.

Contrairement aux protocoles de routage à vecteur de distance qui se basent sur des mises à jour périodiques de la table de routage, OSPF fonctionne en échangeant des messages de mise à jour de l'état des liens (LSA) entre les routeurs voisins. Ces messages contiennent des informations sur l'état des liens et les routes disponibles dans le réseau. Les routeurs utilisent ces informations pour construire une base de données topologique complète du réseau, à partir de laquelle ils calculent les chemins les plus courts vers toutes les destinations.

OSPF offre plusieurs avantages, notamment la convergence rapide du réseau en cas de modification de la topologie, la prise en charge de la hiérarchie de routage par zones, et la possibilité de définir des politiques de routage avancées. Il est largement utilisé dans les réseaux d'entreprise et les réseaux de fournisseurs de services Internet pour assurer un routage efficace et fiable du trafic IP.

1.5 Le protocole BGP

Le protocole BGP (Border Gateway Protocol) est un protocole de routage externe utilisé pour échanger des informations de routage entre différents systèmes autonomes (AS) sur Internet. Contrairement aux protocoles de routage interne comme OSPF ou EIGRP qui fonctionnent à l'intérieur d'un seul réseau, BGP est conçu pour gérer le trafic entre des réseaux distincts et souvent administrativement indépendants.

Dans un réseau BGP, les routeurs échangent des messages pour annoncer les préfixes IP qu'ils peuvent atteindre et pour apprendre les préfixes annoncés par d'autres routeurs. Ces annonces de préfixes sont utilisées pour construire la table de routage BGP, qui contient des informations sur la meilleure route vers chaque préfixe IP sur Internet. Contrairement aux protocoles de routage interne, BGP ne se base pas uniquement sur la distance ou le coût pour choisir la meilleure route, mais prend également en compte des politiques de routage définies par les opérateurs de réseau.

BGP est crucial pour le fonctionnement d'Internet car il permet aux réseaux individuels de se connecter les uns aux autres de manière transparente, tout en permettant aux opérateurs de réseau de contrôler le flux de trafic à travers leurs réseaux. Il est utilisé par les fournisseurs de services Internet, les grandes entreprises et les opérateurs de réseau pour gérer le routage du trafic IP à l'échelle mondiale.

1.6 Architecture de la solution VPN-MPLS

L'architecture d'une solution VPN-MPLS est généralement basée sur un ensemble de composants interconnectés qui permettent de créer un réseau privé virtuel (VPN) sécurisé en utilisant le protocole MPLS (Multiprotocol Label Switching). Voici une description générale de l'architecture typique d'une telle solution :

Routeurs MPLS (PE et P) : Les routeurs PE (Provider Edge) sont situés aux bords du réseau MPLS et interagissent directement avec les clients VPN. Ils sont responsables de l'encapsulation et du marquage des paquets entrants et sortants avec des étiquettes

MPLS. Les routeurs P (Provider) sont situés à l'intérieur du réseau MPLS et sont chargés de commuter les paquets en fonction des étiquettes MPLS sans avoir connaissance des détails des VPN.

Routeurs de Bord des Clients (CE) : Les routeurs CE sont situés au sein du réseau du client et sont connectés aux routeurs PE. Ils peuvent être des routeurs, des commutateurs ou des pare-feu. Les CE sont chargés de gérer la connectivité réseau locale du client et d'acheminer le trafic vers les routeurs PE via des protocoles de routage internes comme OSPF ou BGP.

Protocoles de Routage : Les protocoles de routage internes comme OSPF (Open Shortest Path First) ou BGP (Border Gateway Protocol) sont utilisés entre les routeurs CE et PE pour échanger des informations de routage. Ces protocoles permettent aux routeurs PE de découvrir les réseaux accessibles via les clients VPN et de mettre à jour leurs tables de routage en conséquence.

Étiquetage MPLS : Le cœur de l'architecture MPLS réside dans l'étiquetage des paquets. Les routeurs PE assignent des étiquettes MPLS à chaque paquet entrant en fonction de la destination et du VPN auquel il appartient. Ces étiquettes sont utilisées par les routeurs P pour acheminer le trafic vers sa destination sans avoir besoin de parcourir les tables de routage IP traditionnelles.

Tunnels VPN : Les tunnels VPN sont créés en encapsulant le trafic dans des étiquettes MPLS. Chaque VPN dispose de son propre tunnel dédié, ce qui permet d'isoler le trafic entre différents clients et de garantir la confidentialité et la sécurité des données.

Ensemble, ces composants forment une architecture robuste qui permet de fournir un réseau privé virtuel sécurisé et fiable utilisant la technologie MPLS.

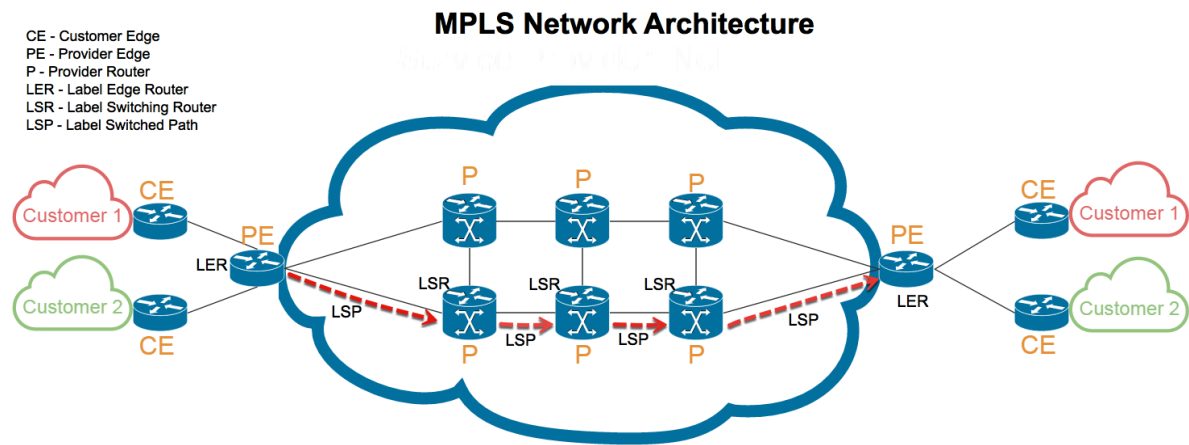


FIGURE 1.3 – Architecture de la solution VPN-MPLS

1.7 Environnement de travail (GNS3 et VMware)

1.7.1 VMware workstation

VMware workstation, est une plateforme de virtualisation de serveurs qui permet d'exécuter plusieurs machines virtuelles sur un seul matériel physique. Cela offre un moyen efficace de virtualiser des serveurs, des applications et des postes de travail. Pour la maquette IP/MPLS, VMware peut être utilisé pour héberger les machines virtuelles qui fonctionnent comme des serveurs MPLS, des serveurs de gestion, ou d'autres composants nécessaires à la configuration du réseau.

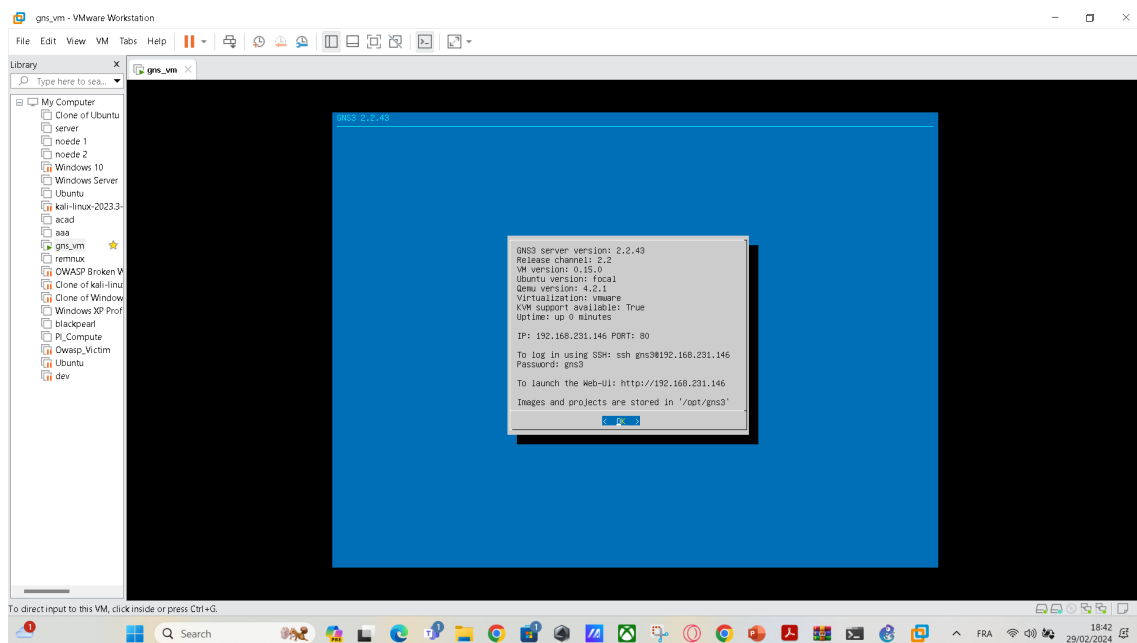


FIGURE 1.4 – Gns3 vm

1.7.2 GNS3

GNS3 est un simulateur de réseau graphique qui permet de modéliser des réseaux complexes en utilisant des images d'appareils réseau réels, tels que des routeurs et des commutateurs. Il prend en charge une variété de systèmes d'exploitation réseau, offrant ainsi une flexibilité pour concevoir des topologies réseau diverses. Dans le contexte de la maquette Backbone IP/MPLS, GNS3 peut être utilisé pour simuler les équipements réseau tels que les routeurs MPLS, les commutateurs, et les hôtes.

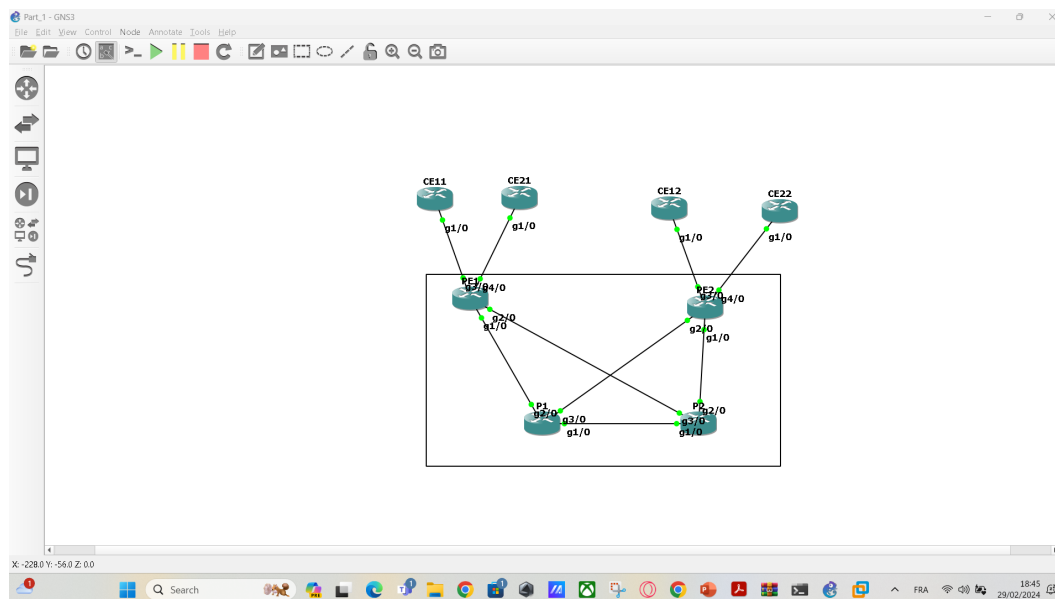


FIGURE 1.5 – GNS3

1.8 Topologie de l'université TEKUP

La topologie de l'université TEK-UP est soigneusement élaborée pour répondre aux exigences spécifiques de connectivité, de redondance, ainsi que pour garantir la disponibilité et la fiabilité du réseau.

L'architecture de la topologie de l'université TEK-UP repose sur un modèle en étoile étendue, où un réseau central (backbone) interconnecte plusieurs sites distants (P) et points d'accès aux utilisateurs (CE). Cette configuration offre une gestion centralisée du réseau tout en assurant une connectivité optimale entre les divers emplacements de l'université.

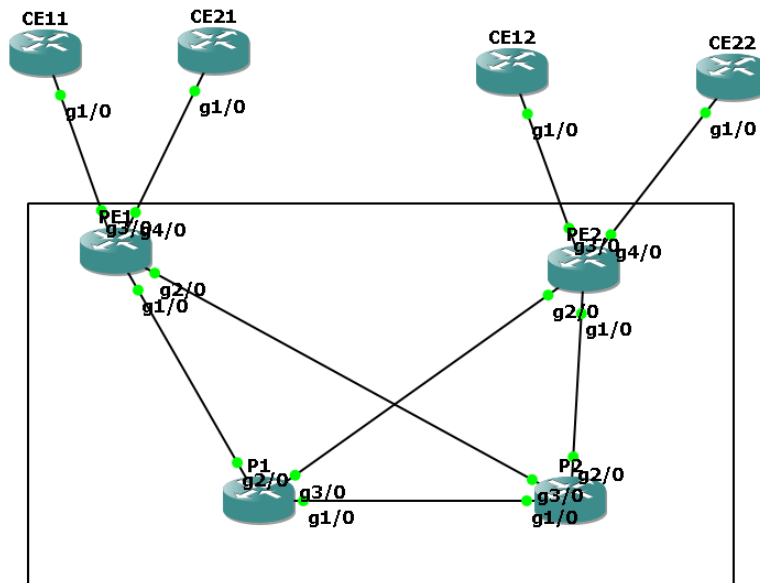


FIGURE 1.6 – Core de notre réseau

1.9 Mise en place de VPN-MPLS

1.9.1 Configuration de base de l'adressage de chaque Interface

Dans un premier temps, nous devons ajuster les différentes interfaces des routeurs à utiliser. Voici un exemple de configuration pour certaines interfaces du routeur PE1 , PE2 , P1 , P2

```

PE1#show ip int brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 unassigned      YES NVRAM   administratively down down
GigabitEthernet1/0 10.1.1.1       YES NVRAM   up          up
GigabitEthernet2/0 10.1.1.5       YES NVRAM   up          up
GigabitEthernet3/0 192.168.1.1    YES NVRAM   up          up
GigabitEthernet4/0 192.168.1.5    YES NVRAM   up          up
Loopback0       1.1.1.1        YES NVRAM   up          up
PE1#
  
```

FIGURE 1.7 – Adressage de PE1

```
PE2#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          unassigned      YES NVRAM    administratively down down
GigabitEthernet1/0       10.1.1.9        YES NVRAM    up          up
GigabitEthernet2/0       10.1.1.13       YES NVRAM    up          up
GigabitEthernet3/0       192.168.1.9     YES NVRAM    up          up
GigabitEthernet4/0       192.168.1.13    YES NVRAM    up          up
Loopback0                 2.2.2.2         YES NVRAM    up          up
PE2#
```

FIGURE 1.8 – Adressage de PE2

```
P1#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          unassigned      YES NVRAM    administratively down down
GigabitEthernet1/0       10.1.1.21       YES NVRAM    up          up
GigabitEthernet2/0       10.1.1.2        YES NVRAM    up          up
GigabitEthernet3/0       10.1.1.14       YES NVRAM    up          up
Loopback0                 3.3.3.3         YES NVRAM    up          up
P1#
```

FIGURE 1.9 – Adressage de P1

```
P2#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          unassigned      YES NVRAM    administratively down down
GigabitEthernet1/0       10.1.1.22       YES NVRAM    up          up
GigabitEthernet2/0       10.1.1.10       YES NVRAM    up          up
GigabitEthernet3/0       10.1.1.6        YES NVRAM    up          up
Loopback0                 4.4.4.4         YES NVRAM    up          up
P2#
```

FIGURE 1.10 – Adressage de P2

1.9.2 Configuration des protocoles de routage

En première étape, nous implémenterons le protocole OSPF sur l'ensemble des routeurs du réseau IP/MPLS, en prenant soin d'intégrer l'Area 0 dans la configuration. Ci-dessous, vous trouverez un exemple de configuration pour le routeur PE1 , PE2 , P1 , P2.

```
PE1#show ip ospf neighbor
Neighbor ID    Pri   State           Dead Time   Address        Interface
4.4.4.4        1     FULL/DR         00:00:37   10.1.1.6       GigabitEthernet2/0
3.3.3.3        1     FULL/DR         00:00:37   10.1.1.2       GigabitEthernet1/0
172.16.21.21   1     FULL/BDR        00:00:37   192.168.1.6    GigabitEthernet4/0
172.16.11.11   1     FULL/BDR        00:00:37   192.168.1.2    GigabitEthernet3/0
PE1#
```

FIGURE 1.11 – table de Voisinage OSPF de PE1

```
PE2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/DR	00:00:32	10.1.1.14	GigabitEthernet2/0
4.4.4.4	1	FULL/DR	00:00:32	10.1.1.10	GigabitEthernet1/0
172.16.22.22	1	FULL/BDR	00:00:32	192.168.1.14	GigabitEthernet4/0
172.16.12.12	1	FULL/BDR	00:00:32	192.168.1.10	GigabitEthernet3/0

```
PE2#
```

FIGURE 1.12 – table de Voisinage OSPF de PE2

```
P1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
4.4.4.4	1	FULL/DR	00:00:33	10.1.1.22	GigabitEthernet1/0
2.2.2.2	1	FULL/BDR	00:00:33	10.1.1.13	GigabitEthernet3/0
1.1.1.1	1	FULL/BDR	00:00:33	10.1.1.1	GigabitEthernet2/0

```
P1#
```

FIGURE 1.13 – table de Voisinage OSPF de P1

```
P2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	1	FULL/BDR	00:00:30	10.1.1.21	GigabitEthernet1/0
2.2.2.2	1	FULL/BDR	00:00:30	10.1.1.9	GigabitEthernet2/0
1.1.1.1	1	FULL/BDR	00:00:30	10.1.1.5	GigabitEthernet3/0

```
P2#
```

FIGURE 1.14 – table de Voisinage OSPF de P2

```
PE1#show ip route ospf
```

```

  2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/3] via 10.1.1.6, 00:06:19, GigabitEthernet2/0
        [110/3] via 10.1.1.2, 00:06:19, GigabitEthernet1/0
  3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/2] via 10.1.1.2, 00:06:19, GigabitEthernet1/0
  4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/2] via 10.1.1.6, 00:06:19, GigabitEthernet2/0
 10.0.0.0/30 is subnetted, 5 subnets
O       10.1.1.8 [110/2] via 10.1.1.6, 00:06:19, GigabitEthernet2/0
O       10.1.1.12 [110/2] via 10.1.1.2, 00:06:19, GigabitEthernet1/0
O       10.1.1.20 [110/2] via 10.1.1.6, 00:06:19, GigabitEthernet2/0
        [110/2] via 10.1.1.2, 00:06:19, GigabitEthernet1/0
PE1#
```

FIGURE 1.15 – table de routage OSPF de PE1

```

[110/2] via 10.1.1.10, 00:06:19, GigabitEthernet1/0
PE2#show ip route ospf
  1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/3] via 10.1.1.14, 00:06:32, GigabitEthernet2/0
        [110/3] via 10.1.1.10, 00:06:32, GigabitEthernet1/0
  3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/2] via 10.1.1.14, 00:06:32, GigabitEthernet2/0
  4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/2] via 10.1.1.10, 00:06:32, GigabitEthernet1/0
 10.0.0.0/30 is subnetted, 5 subnets
O       10.1.1.0 [110/2] via 10.1.1.14, 00:06:32, GigabitEthernet2/0
O       10.1.1.4 [110/2] via 10.1.1.10, 00:06:32, GigabitEthernet1/0
O       10.1.1.20 [110/2] via 10.1.1.14, 00:06:32, GigabitEthernet2/0
        [110/2] via 10.1.1.10, 00:06:32, GigabitEthernet1/0
PE2#

```

FIGURE 1.16 – table de routage OSPF de PE2

```

P1#show ip route ospf
  1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/2] via 10.1.1.1, 00:06:17, GigabitEthernet2/0
  2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 10.1.1.13, 00:06:17, GigabitEthernet3/0
  4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/2] via 10.1.1.22, 00:06:17, GigabitEthernet1/0
 10.0.0.0/30 is subnetted, 5 subnets
O       10.1.1.8 [110/2] via 10.1.1.22, 00:06:17, GigabitEthernet1/0
        [110/2] via 10.1.1.13, 00:06:17, GigabitEthernet3/0
O       10.1.1.4 [110/2] via 10.1.1.22, 00:06:17, GigabitEthernet1/0
        [110/2] via 10.1.1.1, 00:06:17, GigabitEthernet2/0
P1#

```

FIGURE 1.17 – table de routage OSPF de P1

```

P2#show ip route ospf
  1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/2] via 10.1.1.5, 00:06:39, GigabitEthernet3/0
  2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 10.1.1.9, 00:06:39, GigabitEthernet2/0
  3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/2] via 10.1.1.21, 00:06:39, GigabitEthernet1/0
 10.0.0.0/30 is subnetted, 5 subnets
O       10.1.1.12 [110/2] via 10.1.1.21, 00:06:39, GigabitEthernet1/0
        [110/2] via 10.1.1.9, 00:06:39, GigabitEthernet2/0
O       10.1.1.0 [110/2] via 10.1.1.21, 00:06:39, GigabitEthernet1/0
        [110/2] via 10.1.1.5, 00:06:39, GigabitEthernet3/0
P2#

```

FIGURE 1.18 – table de routage OSPF de P2

1.9.3 Configuration de MPLS

Veillez trouver les configurations des autres routeurs dans l'annexe. En deuxième étape, nous veillons à activer le protocole MPLS sur tous les routeurs du Backbone, en prenant en considération les paramètres requis pour la commutation des labels. À titre illustratif, ci-dessous se trouve configuration pour le routeur PE1 , PE2 , P1 , P2. Ces commandes doivent être appliquées sur l'ensemble des routeurs appartenant au Backbone MPLS/IP.

```

PE1#Show mpls ldp neighbor
  Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 1.1.1.1:0
    TCP connection: 3.3.3.3.23252 - 1.1.1.1.646
    State: Oper; Msgs sent/rcvd: 27/27; Downstream
    Up time: 00:13:49
    LDP discovery sources:
      GigabitEthernet1/0, Src IP addr: 10.1.1.2
    Addresses bound to peer LDP Ident:
      10.1.1.21      3.3.3.3      10.1.1.2      10.1.1.14
  Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 1.1.1.1:0
    TCP connection: 4.4.4.4.51833 - 1.1.1.1.646
    State: Oper; Msgs sent/rcvd: 27/27; Downstream
    Up time: 00:13:49
    LDP discovery sources:
      GigabitEthernet2/0, Src IP addr: 10.1.1.6
    Addresses bound to peer LDP Ident:
      10.1.1.22      4.4.4.4      10.1.1.10     10.1.1.6
PE1#

```

FIGURE 1.19 – Configuration de MPLS de PE1

```

PE2#Show mpls ldp neighbor
  Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 2.2.2.2:0
    TCP connection: 4.4.4.4.15353 - 2.2.2.2.646
    State: Oper; Msgs sent/rcvd: 28/28; Downstream
    Up time: 00:14:00
    LDP discovery sources:
      GigabitEthernet1/0, Src IP addr: 10.1.1.10
    Addresses bound to peer LDP Ident:
      10.1.1.22      4.4.4.4      10.1.1.10     10.1.1.6
  Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 2.2.2.2:0
    TCP connection: 3.3.3.3.53802 - 2.2.2.2.646
    State: Oper; Msgs sent/rcvd: 28/28; Downstream
    Up time: 00:14:00
    LDP discovery sources:
      GigabitEthernet2/0, Src IP addr: 10.1.1.14
    Addresses bound to peer LDP Ident:
      10.1.1.21      3.3.3.3      10.1.1.2      10.1.1.14
PE2#

```

FIGURE 1.20 – Configuration de MPLS de PE2

```

P1#Show mpls ldp neighbor
  Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 3.3.3.3:0
    TCP connection: 4.4.4.4.63143 - 3.3.3.3.646
    State: Oper; Msgs sent/rcvd: 28/28; Downstream
    Up time: 00:14:03
    LDP discovery sources:
      GigabitEthernet1/0, Src IP addr: 10.1.1.22
    Addresses bound to peer LDP Ident:
      10.1.1.22      4.4.4.4      10.1.1.10      10.1.1.6
  Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 3.3.3.3:0
    TCP connection: 2.2.2.2.646 - 3.3.3.3.53802
    State: Oper; Msgs sent/rcvd: 28/28; Downstream
    Up time: 00:13:55
    LDP discovery sources:
      GigabitEthernet3/0, Src IP addr: 10.1.1.13
    Addresses bound to peer LDP Ident:
      10.1.1.9      2.2.2.2      10.1.1.13
  Peer LDP Ident: 1.1.1.1:0; Local LDP Ident 3.3.3.3:0
    TCP connection: 1.1.1.1.646 - 3.3.3.3.23252
    State: Oper; Msgs sent/rcvd: 27/28; Downstream
    Up time: 00:13:55
    LDP discovery sources:
      GigabitEthernet2/0, Src IP addr: 10.1.1.1
    Addresses bound to peer LDP Ident:
--More-- █

```

FIGURE 1.21 – Configuration de MPLS de P1

```

P2#Show mpls ldp neighbor
  Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 4.4.4.4:0
    TCP connection: 3.3.3.3.646 - 4.4.4.4.63143
    State: Oper; Msgs sent/rcvd: 28/28; Downstream
    Up time: 00:14:12
    LDP discovery sources:
      GigabitEthernet1/0, Src IP addr: 10.1.1.21
    Addresses bound to peer LDP Ident:
      10.1.1.21      3.3.3.3      10.1.1.2      10.1.1.14
  Peer LDP Ident: 1.1.1.1:0; Local LDP Ident 4.4.4.4:0
    TCP connection: 1.1.1.1.646 - 4.4.4.4.51833
    State: Oper; Msgs sent/rcvd: 27/27; Downstream
    Up time: 00:14:04
    LDP discovery sources:
      GigabitEthernet3/0, Src IP addr: 10.1.1.5
    Addresses bound to peer LDP Ident:
      10.1.1.1      1.1.1.1      10.1.1.5
  Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 4.4.4.4:0
    TCP connection: 2.2.2.2.646 - 4.4.4.4.15353
    State: Oper; Msgs sent/rcvd: 28/28; Downstream
    Up time: 00:14:04
    LDP discovery sources:
      GigabitEthernet2/0, Src IP addr: 10.1.1.9
    Addresses bound to peer LDP Ident:
--More-- █

```

FIGURE 1.22 – Configuration de MPLS de P2

1.9.4 LFIB

```

PE1#show mpls forwarding-table
Local  Outgoing  Prefix          Bytes tag  Outgoing     Next Hop
tag    tag or VC  or Tunnel Id    switched   interface
16     Pop tag    10.1.1.20/30    0          Gi2/0        10.1.1.6
      Pop tag    10.1.1.20/30    0          Gi1/0        10.1.1.2
17     Pop tag    10.1.1.12/30    0          Gi1/0        10.1.1.2
18     Pop tag    10.1.1.8/30     0          Gi2/0        10.1.1.6
19     20        2.2.2.2/32     0          Gi2/0        10.1.1.6
      20        2.2.2.2/32     0          Gi1/0        10.1.1.2
20     Pop tag    3.3.3.3/32     0          Gi1/0        10.1.1.2
21     Pop tag    4.4.4.4/32     0          Gi2/0        10.1.1.6
22     Untagged  172.16.11.11/32[V] \
      0          Gi3/0        192.168.1.2
23     Aggregate 192.168.1.0/30[V] 0
24     Untagged  172.16.21.21/32[V] \
      0          Gi4/0        192.168.1.6
25     Aggregate 192.168.1.4/30[V] 0
PE1#

```

FIGURE 1.23 – vérification de la LFIB de PE1

```

PE2#show mpls forwarding-table
Local  Outgoing  Prefix          Bytes tag  Outgoing     Next Hop
tag    tag or VC  or Tunnel Id    switched   interface
16     Pop tag    10.1.1.20/30    0          Gi2/0        10.1.1.14
      Pop tag    10.1.1.20/30    0          Gi1/0        10.1.1.10
17     Pop tag    10.1.1.4/30     0          Gi1/0        10.1.1.10
18     Pop tag    10.1.1.0/30     0          Gi2/0        10.1.1.14
19     Pop tag    3.3.3.3/32     0          Gi2/0        10.1.1.14
20     Pop tag    4.4.4.4/32     0          Gi1/0        10.1.1.10
21     19        1.1.1.1/32     0          Gi2/0        10.1.1.14
      19        1.1.1.1/32     0          Gi1/0        10.1.1.10
22     Untagged  172.16.12.12/32[V] \
      0          Gi3/0        192.168.1.10
23     Aggregate 192.168.1.8/30[V] 0
24     Untagged  172.16.22.22/32[V] \
      0          Gi4/0        192.168.1.14
25     Aggregate 192.168.1.12/30[V] \
      0
PE2#

```

FIGURE 1.24 – vérification de la LFIB de PE2


```
P1#Show mpls forwarding-table
Local   Outgoing   Prefix           Bytes tag  Outgoing     Next Hop
tag     tag or VC  or Tunnel Id     switched   interface
16      Pop tag    4.4.4.4/32       0          Gi1/0        10.1.1.22
17      Pop tag    10.1.1.4/30      0          Gi1/0        10.1.1.22
          Pop tag    10.1.1.4/30      0          Gi2/0        10.1.1.1
18      Pop tag    10.1.1.8/30      0          Gi1/0        10.1.1.22
          Pop tag    10.1.1.8/30      0          Gi3/0        10.1.1.13
19      Pop tag    1.1.1.1/32       2753       Gi2/0        10.1.1.1
20      Pop tag    2.2.2.2/32       3779       Gi3/0        10.1.1.13
P1#
```

FIGURE 1.25 – vérification de la LFIB de P1

```
P2#Show mpls forwarding-table
Local   Outgoing   Prefix           Bytes tag  Outgoing     Next Hop
tag     tag or VC  or Tunnel Id     switched   interface
16      Pop tag    3.3.3.3/32       0          Gi1/0        10.1.1.21
17      Pop tag    10.1.1.0/30      0          Gi1/0        10.1.1.21
          Pop tag    10.1.1.0/30      0          Gi3/0        10.1.1.5
18      Pop tag    10.1.1.12/30     0          Gi1/0        10.1.1.21
          Pop tag    10.1.1.12/30     0          Gi2/0        10.1.1.9
19      Pop tag    1.1.1.1/32       0          Gi3/0        10.1.1.5
20      Pop tag    2.2.2.2/32       0          Gi2/0        10.1.1.9
P2#
```

FIGURE 1.26 – vérification de la LFIB de P2

1.9.5 Binding

```
PE1#Show mpls ip binding
1.1.1.1/32
  in label:    imp-null
  out label:   19      lsr: 3.3.3.3:0
  out label:   19      lsr: 4.4.4.4:0
2.2.2.2/32
  in label:    19
  out label:   20      lsr: 3.3.3.3:0      inuse
  out label:   20      lsr: 4.4.4.4:0      inuse
3.3.3.3/32
  in label:    20
  out label:   imp-null lsr: 3.3.3.3:0      inuse
  out label:   16      lsr: 4.4.4.4:0
4.4.4.4/32
  in label:    21
  out label:   16      lsr: 3.3.3.3:0
  out label:   imp-null lsr: 4.4.4.4:0      inuse
10.1.1.0/30
  in label:    imp-null
  out label:   imp-null lsr: 3.3.3.3:0
  out label:   17      lsr: 4.4.4.4:0
10.1.1.4/30
  in label:    imp-null
  out label:   17      lsr: 3.3.3.3:0
--More--
```

FIGURE 1.27 – affichage des bindings des labels MPLS récupérés par LDP de PE1

```

PE2#show mpls ip binding
1.1.1.1/32
  in label:    21
  out label:   19      lsr: 4.4.4.4:0      inuse
  out label:   19      lsr: 3.3.3.3:0      inuse
2.2.2.2/32
  in label:    imp-null
  out label:   20      lsr: 4.4.4.4:0
  out label:   20      lsr: 3.3.3.3:0
3.3.3.3/32
  in label:    19
  out label:   16      lsr: 4.4.4.4:0
  out label:   imp-null lsr: 3.3.3.3:0      inuse
4.4.4.4/32
  in label:    20
  out label:   imp-null lsr: 4.4.4.4:0      inuse
  out label:   16      lsr: 3.3.3.3:0
10.1.1.0/30
  in label:    18
  out label:   17      lsr: 4.4.4.4:0
  out label:   imp-null lsr: 3.3.3.3:0      inuse
10.1.1.4/30
  in label:    17
  out label:   imp-null lsr: 4.4.4.4:0      inuse
--More--

```

FIGURE 1.28 – affichage des bindings des labels MPLS récupérés par LDP de PE2

```

P1#show mpls ip binding
1.1.1.1/32
  in label:    19
  out label:   imp-null lsr: 1.1.1.1:0      inuse
  out label:   19      lsr: 4.4.4.4:0
  out label:   21      lsr: 2.2.2.2:0
2.2.2.2/32
  in label:    20
  out label:   imp-null lsr: 2.2.2.2:0      inuse
  out label:   19      lsr: 1.1.1.1:0
  out label:   20      lsr: 4.4.4.4:0
3.3.3.3/32
  in label:    imp-null
  out label:   16      lsr: 4.4.4.4:0
  out label:   19      lsr: 2.2.2.2:0
  out label:   20      lsr: 1.1.1.1:0
4.4.4.4/32
  in label:    16
  out label:   imp-null lsr: 4.4.4.4:0      inuse
  out label:   20      lsr: 2.2.2.2:0
  out label:   21      lsr: 1.1.1.1:0
10.1.1.0/30
  in label:    imp-null
  out label:   17      lsr: 4.4.4.4:0
--More--

```

FIGURE 1.29 – affichage des bindings des labels MPLS récupérés par LDP de P1

1.9.6 Mise en place des VPN

Dans l'étape suivante, nous nous attèlerons à la configuration de VRF (Virtual Routing and Forwarding).

```

PE1#Show ip bgp vpnv4 vrf VPN_Customer1
BGP table version is 17, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network                Next Hop           Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf VPN_Customer1)
*> 172.16.11.11/32 192.168.1.2             2         32768 ?
*>i172.16.12.12/32 2.2.2.2                 2        100    0 ?
*> 192.168.1.0/30   0.0.0.0                 0         32768 ?
*>i192.168.1.8/30  2.2.2.2                 0        100    0 ?
PE1#Show ip bgp vpnv4 vrf VPN_Customer2
BGP table version is 17, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network                Next Hop           Metric LocPrf Weight Path
Route Distinguisher: 100:2 (default for vrf VPN_Customer2)
*> 172.16.21.21/32 192.168.1.6             2         32768 ?
*>i172.16.22.22/32 2.2.2.2                 2        100    0 ?
*> 192.168.1.4/30   0.0.0.0                 0         32768 ?
*>i192.168.1.12/30 2.2.2.2                 0        100    0 ?
PE1#

```

FIGURE 1.30 – Affichage Instance BGP de PE1

```

PE2#Show ip bgp vpnv4 vrf VPN_Customer1
BGP table version is 17, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network                Next Hop           Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf VPN_Customer1)
*>i172.16.11.11/32 1.1.1.1                 2        100    0 ?
*> 172.16.12.12/32 192.168.1.10            2         32768 ?
*>i192.168.1.0/30  1.1.1.1                 0        100    0 ?
*> 192.168.1.8/30   0.0.0.0                 0         32768 ?
PE2#Show ip bgp vpnv4 vrf VPN_Customer2
BGP table version is 17, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network                Next Hop           Metric LocPrf Weight Path
Route Distinguisher: 100:2 (default for vrf VPN_Customer2)
*>i172.16.21.21/32 1.1.1.1                 2        100    0 ?
*> 172.16.22.22/32 192.168.1.14            2         32768 ?
*>i192.168.1.4/30  1.1.1.1                 0        100    0 ?
*> 192.168.1.12/30 0.0.0.0                 0         32768 ?
PE2#

```

FIGURE 1.31 – Affichage Instance BGP de PE2

1.9.7 table de routage

```

PE1#Show ip route vrf VPN_Customer1

Routing Table: VPN_Customer1
Codes: 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

Gateway of last resort is not set

    172.16.0.0/32 is subnetted, 2 subnets
B       172.16.12.12 [200/2] via 2.2.2.2, 00:50:47
O       172.16.11.11 [110/2] via 192.168.1.2, 00:51:47, GigabitEthernet3/0
    192.168.1.0/30 is subnetted, 2 subnets
B       192.168.1.8 [200/0] via 2.2.2.2, 00:50:47
C       192.168.1.0 is directly connected, GigabitEthernet3/0
PE1#Show ip route vrf VPN_Customer2

Routing Table: VPN_Customer2
Codes: 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

Gateway of last resort is not set

    172.16.0.0/32 is subnetted, 2 subnets
B       172.16.22.22 [200/2] via 2.2.2.2, 00:50:50
O       172.16.21.21 [110/2] via 192.168.1.6, 00:51:51, GigabitEthernet4/0
    192.168.1.0/30 is subnetted, 2 subnets
B       192.168.1.12 [200/0] via 2.2.2.2, 00:50:50
C       192.168.1.4 is directly connected, GigabitEthernet4/0
PE1#

```

FIGURE 1.32 – Affichage la table de routage de VRF de VPN Customer1 et VPN Customer2 de PE1

1.9.8 Validation et test de la connexion

La dernière section du chapitre se concentre sur la validation et les tests de la connexion VPN-MPLS nouvellement établie. Des scénarios de test seront discutés pour évaluer la robustesse de la solution et s'assurer de sa conformité aux exigences préalablement définies. Pour vérifier la connexion entres les différents sites de clients, nous tapons la commande suivante au niveau CE11 , CE21 :

```
CE11#ping 172.16.12.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/121/132 ms
CE11#
```

FIGURE 1.33 – ping CE11 TO CE12

```
CE21#ping 172.16.22.22

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.22.22, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/120/140 ms
CE21#
```

FIGURE 1.34 – ping CE21 TO CE22

1.10 Conclusion

En résumé, ce chapitre a approfondi la mise en place de la solution VPN-MPLS. Nous avons exploré les tenants et les aboutissants de la technologie MPLS, détaillé l'architecture de la solution, présenté l'environnement de déploiement, et suivi les étapes nécessaires pour déployer le VPN-MPLS. Ces efforts nous ont permis d'établir des fondations solides. Les prochaines étapes consisteront à mener des tests exhaustifs pour garantir le bon fonctionnement de l'ensemble, avant de valider son intégration réussie dans l'infrastructure réseau planifiée.

chapitre 2

Conception et mise en place de la solution de réseau LAN Etendu Tekup

2.1 Introduction

La deuxième partie de ce rapport se concentre sur la configuration des VLANs, les modes de liaison trunk entre les commutateurs, ainsi que les mots de passe pour chaque routeur. Nous aborderons également la configuration des services DHCP et le protocole HSRP pour assurer une connectivité réseau robuste et sécurisée .

2.2 Architecture de réseau LAN étendu de Tekup

Cette architecture globale permet à l'université de fournir une connectivité réseau sécurisée et fiable à tous ses sites, tout en permettant une gestion efficace des ressources et des politiques de sécurité à l'échelle de l'ensemble du réseau.

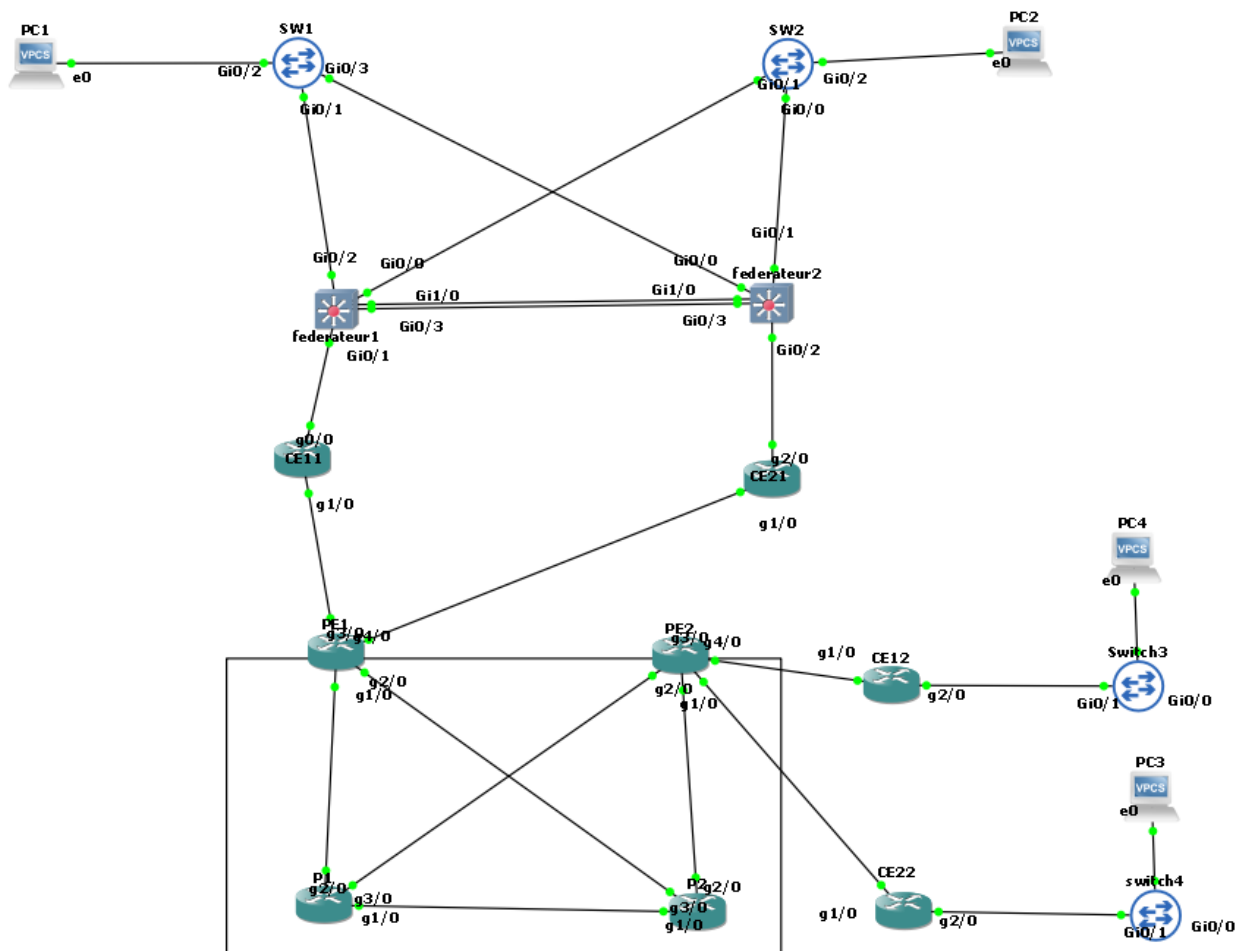


FIGURE 2.35 – Architecture de Partie 2

2.3 Conception de la Solution LAN

La conception de la solution de sécurité réseau pour l'université Tek-up a été minutieusement élaborée en fonction des besoins spécifiques de chaque site, y compris les deux sièges et les deux succursales. En suivant les directives énoncées dans la partie 2, nous avons développé une solution qui intègre les éléments suivants :

Le réseau de l'université Tek-up a été méticuleusement conçu pour répondre à ses besoins particuliers, en tenant compte de la connectivité entre ses deux sièges et deux succursales.

La solution comprend la mise en place de VLANs pour isoler les divers types de trafic, ainsi que des liaisons entre les commutateurs de couche 2 et de couche 3 afin d'assurer la connectivité entre les différents sites.

La gestion des identités est également prise en compte, avec la configuration de mots de passe conformes aux directives de sécurité.

Pour garantir la disponibilité du réseau, des mécanismes de redondance tels que HSRP ou VRRP ont été mis en œuvre.

Enfin, les canaux Ethernet ont été configurés en mode TRUNK pour permettre le transit du trafic entre les différents VLANs.

2.4 Description de la Solution Redondante de LAN

La mise en place d'une solution de redondance avec HSRP (Hot Standby Router Protocol) dans le réseau LAN étendu de Tekup est cruciale pour garantir une disponibilité élevée et une fiabilité accrue du réseau. Voici comment cette solution peut être intégrée :

- **Utilisation de plusieurs routeurs** : Tout d'abord, la solution implique l'utilisation de plusieurs routeurs au sein du réseau. Ces routeurs fonctionnent en tant que passerelles par défaut pour les périphériques du réseau, assurant ainsi une connectivité continue en cas de panne d'un routeur.

- **Configuration de HSRP** : Sur les routeurs, le protocole HSRP est configuré sur les interfaces qui servent de passerelles par défaut. HSRP permet de désigner un routeur actif et un ou plusieurs routeurs de secours (standby). Le routeur actif est responsable du transfert du trafic réseau normal, tandis que les routeurs de secours restent en veille, prêts à prendre le relais en cas de défaillance du routeur actif.

- **Élection du routeur actif** : Lorsqu'un groupe HSRP est configuré sur une interface, les routeurs se communiquent entre eux pour élire un routeur actif en fonction de leur priorité HSRP. Le routeur avec la priorité la plus élevée devient l'actif, tandis que les autres deviennent des routeurs de secours.

- **Surveillance des routes et basculement** : Les routeurs HSRP surveillent en permanence l'état de l'interface ainsi que la connectivité vers d'autres routeurs du réseau. Si le routeur actif devient indisponible (en raison d'une panne matérielle ou d'une défaillance du lien), un des routeurs de secours prend automatiquement le relais et devient le routeur actif, assurant ainsi une continuité de service transparente pour les périphériques du réseau.

- **Temps de basculement rapide** : L'un des avantages clés de HSRP est sa capacité à basculer rapidement vers un routeur de secours en cas de panne du routeur actif. Cela permet de minimiser l'impact sur les opérations réseau et d'assurer une disponibilité élevée des services.

En intégrant HSRP dans la solution de réseau LAN étendu de Tekup, l'entreprise peut garantir une redondance efficace au niveau de la passerelle par défaut, ce qui réduit les temps d'arrêt et améliore la résilience du réseau face aux pannes matérielles ou aux défaillances de lien.

Environnement de travail

Pour la configuration de notre solution, nous avons mis en place un environnement de travail bien défini, comprenant des équipements spécifiques et des logiciels adaptés. Voici un aperçu de cet environnement :

Équipements : Nous avons utilisé des switches de couche 3 Cisco 3640 pour configurer le réseau. Ces switches sont essentiels pour gérer de manière avancée le trafic et mettre en place la redondance au niveau du réseau LAN étendu. Nous avons utilisé le modèle de switch Cisco 3640 avec l'image logicielle c3640-a3jsmz.124-25d.bin pour cette configuration.

Pour les routeurs, nous avons opté pour les routeurs Cisco 7200 en raison de leur puissance de traitement élevée et de leur capacité à gérer le routage entre les différents réseaux. Ces routeurs sont cruciaux pour le routage entre les différents VLANs et pour assurer la connectivité entre les sites distants. Nous avons utilisé l'image logicielle c7200 pour ces routeurs.

En résumé, notre environnement de travail incluait des switches de couche 3 Cisco 3640

avec l'image logicielle c3640-a3js-mz.124-25d.bin, des routeurs Cisco 7200 avec l'image logicielle c7200. Nous avons également utilisé GNS3 comme plateforme de simulation réseau. Cette configuration nous a permis de concevoir, configurer et tester efficacement et en toute sécurité notre solution de réseau LAN étendu.

2.5 Mise en place de la Solution de LAN Redondante

Pour mettre en place la solution de LAN redondante pour Tek-up, nous suivrons un processus méthodique étape par étape pour configurer les commutateurs haute disponibilité, établir les liens de secours et activer les mécanismes de basculement automatique. Voici notre plan d'action détaillé :

2.6 Siège

2.6.1 Création de VLAN

Création des VLANs 10, 15 et 20 : Nous avons créé plusieurs VLAN au niveau les Switch Layer2 et Layer 3 pour isoler différents types de trafic et simplifier la gestion du réseau. Cela inclut : • VLAN 10 : DATA1 • VLAN 15 : DATA2 • VLAN 20 : Management Avec leurs plages d'adresses IP respectives 172.16.10.0/24, 172.16.15.0/24 et 172.16.20.0/24.

```
sw1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Gi0/0, Gi0/1, Gi0/3, Gi1/0 Gi1/1, Gi1/2, Gi1/3, Gi2/0 Gi2/1, Gi2/2, Gi2/3, Gi3/0 Gi3/1, Gi3/2, Gi3/3
10	data1	active	Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```
sw1#
```

FIGURE 2.36 – VLAN 10 : data1

```
sw2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Gi0/0, Gi0/1, Gi0/3, Gi1/0 Gi1/1, Gi1/2, Gi1/3, Gi2/0 Gi2/1, Gi2/2, Gi2/3, Gi3/0 Gi3/1, Gi3/2, Gi3/3
15	data2	active	Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```
sw2#
```

FIGURE 2.37 – VLAN 15 : data2

```
Switch>en
Switch>enable
Switch#ch
Switch#ch
Switch#conf
Switch#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int
Switch(config)#interface vlan 30
Switch(config-if)#
*Apr  4 00:55:50.061: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to down
Switch(config-if)#ip add
Switch(config-if)#ip address 192.168.1.45 255.255.255.252
Switch(config-if)#no sh
Switch(config-if)#no shutdown
Switch(config-if)#
```

FIGURE 2.38 – Vlan 20 : management

2.6.2 Lien entre Switch Layer 2 et Switch Layer3 "Federateur". sont des Trunks tel que Native Vlan 20

Nous avons configuré des liens de Trunk entre les commutateurs Layer 2 et les commutateurs Layer 3, avec le VLAN 20 Management comme VLAN native.

```

Switch#
Switch#
Switch#
Switch#int
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int
Switch(config)#interface g0/0
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode access
Switch(config-if)#switchport mode access
Switch(config-if)#swit
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vlan 104
Switch(config-if)#exit
Switch(config)#int
Switch(config)#interface g0/1
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk en
Switch(config-if)#switchport trunk encapsulation do
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#sw
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk na
Switch(config-if)#switchport trunk native 103
Switch(config-if)#switchport trunk native 103
Switch(config-if)#end
Switch#wr
Building configuration...

*Apr  5 01:34:18.355: %SYS-5-CONFIG_I: Configured from console by consoleCompressed configuration from
8713 bytes to 1758 bytes[OK]
Switch#
*Apr  5 01:34:30.123: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait.
..
*Apr  5 01:34:31.113: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.

```

FIGURE 2.39 – Mode Trunk entre layer2 et layer3

2.6.3 Sécurité des appareils :

Mots de passe : — Un mot de passe console, un mot de passe VTY et un mot de passe enable seront configurés sur tous les routeurs et les switches Layer 2 et Layer 3. — Les mots de passe seront uniques pour chaque switch et conformes aux exigences de sécurité en vigueur. Gestion des accès : — L'accès aux switches sera restreint aux administrateurs réseau autorisés. — Les fonctionnalités de sécurité avancées des switches seront activées pour protéger le réseau contre les accès non autorisés.

```

Switch#
Switch#
Switch#
Switch#int
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int
Switch(config)#interface g0/0
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode access
Switch(config-if)#switchport mode access
Switch(config-if)#swit
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vlan 104
Switch(config-if)#exit
Switch(config)#int
Switch(config)#int
Switch(config)#interface g0/1
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk en
Switch(config-if)#switchport trunk encapsulation do
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#sw
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk na
Switch(config-if)#switchport trunk native 103
Switch(config-if)#switchport trunk native vlan 103
Switch(config-if)#end
Switch#wr
Building configuration...

*Apr  5 01:34:18.355: %SYS-5-CONFIG_I: Configured from console by consoleCompressed configuration from
3713 bytes to 1758 bytes[OK]
Switch#
*Apr  5 01:34:30.123: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait.
..
*Apr  5 01:34:31.113: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.

```

FIGURE 2.40 – Mode Trunk entre sw4 et pc 3

```

federateur1
federateur2
Translating "end"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
federateur1#
federateur1#
federateur1#
federateur1#
*Apr 15 09:54:42.982: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw2 GigabitEthernet0/1 (1).
federateur1#wr
Building configuration...
Compressed configuration from 3223 bytes to 1560 bytes
*Apr 15 09:54:50.255: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (20), with sw1 GigabitEthernet0/1 (1).[OK]
federateur1#
*Apr 15 09:54:54.245: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Apr 15 09:54:55.314: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
federateur1#sho
federateur1#show int
federateur1#show interfaces tr
federateur1#show interfaces trunk

Port:      Mode:      Encapsulation  Status  Native vlan
Gi0/0      on        802.1q         trunking  20
Gi0/1      on        802.1q         trunking  20
Gi0/2      on        802.1q         trunking  20

Port:      Vlans allowed on trunk
Gi0/0      10,15,20
Gi0/1      10,15,20
Gi0/2      10,15,20

Port:      Vlans allowed and active in management domain
Gi0/0      20
Gi0/1      20
Gi0/2      20

Port:      Vlans in spanning tree forwarding state and not pruned
Gi0/0      none
Gi0/1      20
Gi0/2      none

federateur1#
*Apr 15 09:55:24.542: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw2 GigabitEthernet0/1 (1).
*Apr 15 09:55:29.690: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (20), with sw1 GigabitEthernet0/1 (1).
*Apr 15 09:56:07.816: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw2 GigabitEthernet0/1 (1).
*Apr 15 09:56:12.372: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (20), with sw1 GigabitEthernet0/1 (1).
*Apr 15 09:56:53.334: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw2 GigabitEthernet0/1 (1).
*Apr 15 09:57:00.187: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (20), with sw1 GigabitEthernet0/1 (1).
*Apr 15 09:57:36.890: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw2 GigabitEthernet0/1 (1).
*Apr 15 09:57:42.075: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (20), with sw1 GigabitEthernet0/1 (1).

```

FIGURE 2.41 – show interfaces trunk federateur 1

```

Switch#
*Apr 15 09:59:22.576: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Building configuration...
Compressed configuration from 3115 bytes to 1524 bytes[OK]
Switch#
*Apr 15 09:59:32.655: %GRUB-5-CONFIG_WRITNG: GRUB configuration is being updated on disk. Please wait...show
*Apr 15 09:59:33.672: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully
Switch#
*Apr 15 09:59:35.602: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw1 GigabitEthernet0/3 (1).
% Type "show ?" for a list of subcommands
Switch#show tr
Switch#show tr
Switch#show trunk
Switch#show trunk in
Switch#show trunk int
Switch#show trunk inter
*Apr 15 09:59:56.182: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (20), with sw2 GigabitEthernet0/1 (1).
% Invalid input detected at '^' marker.

Switch#sho
Switch#show in
Switch#sh
Switch#show int
Switch#show interfaces tr
Switch#show interfaces trunk

Port      Mode      Encapsulation  Status        Native vlan
Gi0/0     on        802.1q         trunking      20
Gi0/1     on        802.1q         trunking      20

Port      Vlans allowed on trunk
Gi0/0     10,15,20
Gi0/1     10,15,20

Port      Vlans allowed and active in management domain
Gi0/0     20
Gi0/1     20

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/0     none
Gi0/1     none
Switch#
*Apr 15 10:00:23.584: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw1 GigabitEthernet0/3 (1).
*Apr 15 10:00:39.999: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (20), with sw2 GigabitEthernet0/0 (1).
*Apr 15 10:01:07.457: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw1 GigabitEthernet0/3 (1).

```

FIGURE 2.42 – show interfaces trunk federateur 2

```

CE11#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CE11(config)#usern
CE11(config)#username raslen sec
CE11(config)#username raslen secret issam
CE11(config)#line co
CE11(config)#line console 0
CE11(config-line)#login local
CE11(config-line)#exit
CE11(config)#line vty 0 4
CE11(config-line)#login local
CE11(config-line)#end
CE11#wr
Building configuration...
[OK]
CE11#
*Apr 15 11:32:55.883: %SYS-5-CONFIG_I: Configured from console by console
CE11#

```

FIGURE 2.43 – Passwords CE11

```

CE21#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CE21(config)#usern
CE21(config)#username rasslen sev
CE21(config)#username rasslen sev
CE21(config)#username rasslen sec
CE21(config)#username rasslen secret issam
CE21(config)#line co
CE21(config)#line console 0
CE21(config-line)#login local
CE21(config-line)#exit
CE21(config)#li
CE21(config)#lin
CE21(config)#line v
CE21(config)#line vty 0 4
CE21(config-line)#log
CE21(config-line)#logi
CE21(config-line)#login local
CE21(config-line)#
CE21(config-line)#exit
CE21(config)#end
CE21#wr
Building configuration...
[OK]
CE21#
*Apr 15 11:34:20.339: %SYS-5-CONFIG_I: Configured from console by console
CE21#

```

FIGURE 2.44 – Passwords CE21

```

E22(config)#enable sec
E22(config)#enable secret issam
E22(config)#line
E22(config)#line cons
E22(config)#line console 0
E22(config-line)#pass
E22(config-line)#password issam
E22(config-line)#login
E22(config-line)#exit
E22(config)#lin
E22(config)#line vty 0 15
E22(config-line)#pass
E22(config-line)#password issam
E22(config-line)#login
E22(config-line)#exit
E22(config)#en
E22(config)#exit
E22#wr
Building configuration...
OK]
E22#
Apr  5 02:46:42.151: %SYS-5-CONFIG_I: Configured from console by console
E22#

```

FIGURE 2.45 – Passwords CE22

```

federateur1(config)#username naslen secre
federateur1(config)#username naslen secret
*Apr 15 10:04:26.568: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (20), with sw1 GigabitEthernet0/1 (1).iss
federateur1(config)#username naslen secret issam
federateur1(config)#line co
federateur1(config)#line console 0
federateur1(config-line)#login local
federateur1(config-line)#exit
federateur1(config)#line vt
federateur1(config)#line vty 0 4
federateur1(config-line)#login local
federateur1(config-line)#exit
federateur1(config)#exit
federateur1#wr
Building configuration...
*Apr 15 10:04:43.329: %SYS-5-CONFIG_I: Configured from console by console

```

FIGURE 2.46 – Passwords Federateur1

2.6.4 IP address Management de VLAN 20

2.6.5 Service DHCP

Adresse IP de management des switches Layer 2 : — SW1 : 172.16.20.101/24 — SW2 : 172.16.20.102/24 Service DHCP : — Un serveur DHCP sera configuré sur les deux switches fédérateurs pour fournir des adresses IP aux périphériques des VLAN 10 et 15. — Les 10 premières adresses IP de chaque VLAN seront réservées pour une utilisation statique. Voici une exemple de configuration de service dhcp sur le fédérateur 1 :

```

federateur2(config)#hostname federateur2
federateur2(config)#usern
federateur2(config)#username raslen secret issam
federateur2(config)#li
federateur2(config)#lin
federateur2(config)#line co
federateur2(config)#line console 0
federateur2(config-line)#login local
federateur2(config-line)#exit
federateur2(config)#lin
federateur2(config)#line v
federateur2(config)#line vty ~
*Apr 15 10:05:28.204: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw1 GigabitEthernet0/3 (1).

% Invalid input detected at '^' marker.

federateur2(config)#line vty 0 4
federateur2(config-line)#login local
federateur2(config-line)#exit
federateur2(config)#exit
federateur2#wr
Building configuration...

*Apr 15 10:05:41.804: %SYS-5-CONFIG_I: Configured from console by consoleCompressed configuration from 3202 bytes to 1604 bytes
*Apr 15 10:05:45.641: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (20), with sw1 GigabitEthernet0/0 (1).[OK]
federateur2#
federateur2#

```

FIGURE 2.47 – Passwords Federateur2

```

federateur1(config)#ip routing
federateur1(config)#ip dhcp exclu
federateur1(config)#ip dhcp excluded-address 172.16.10.1 172.16.10.10
federateur1(config)#ip dhcp excluded-address 172.16.15.1 172.16.15.10
federateur1(config)#ip dhcp
federateur1(config)#ip dhcp po
federateur1(config)#ip dhcp pool vlan
*Apr 15 10:59:05.535: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (20), with pool vlan
*Apr 15 10:59:08.284: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw2 GigabitEthernet0/1 (1).
federateur1(dhcp-config)#exit
federateur1(config)#ip dhcp pool vlan10
^
% Invalid input detected at '^' marker.

federateur1(config)#ip dhcp pool vlan10
federateur1(dhcp-config)#network 172.16.10.0 255.255.255.0
federateur1(dhcp-config)#defa
federateur1(dhcp-config)#default-router 172.16.10.1
federateur1(dhcp-config)#doma
federateur1(dhcp-config)#domain-name Raslen.tn
federateur1(dhcp-config)#dns
federateur1(dhcp-config)#dns-server 8.8.8.8
*Apr 15 10:59:53.176: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (20), with sw1 GigabitEthernet0/1 (1).
federateur1(dhcp-config)#exit
federateur1(config)#ip dhcp pool vlan15
*Apr 15 11:00:02.337: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw2 GigabitEthernet0/1 (1).
federateur1(dhcp-config)#network 172.16.15.0 255.255.255.0
federateur1(dhcp-config)#default-router 172.16.15.1
federateur1(dhcp-config)#domain-name Raslen.tn
federateur1(dhcp-config)#dns-server 8.8.8.8
federateur1(dhcp-config)#exit
federateur1(config)#end
federateur1#

```

FIGURE 2.48 – Service dhcp federateur1

2.6.6 Redondance HSRP

Pour cette étape, nous avons mis en place HSRP pour assurer la redondance au niveau des passerelles par défaut pour les VLANs 10, 15 et 20, garantissant ainsi une disponibilité continue des services réseau en cas de défaillance de l'une des passerelles.


```

federateur1(config-if)#standby 15 priority 120
federateur1(config-if)#standby pre
federateur1(config-if)#standby preempt
federateur1(config-if)#exit
federateur1(config)#interface
federateur1(config)#interface vlan 20
federateur1(config-if)#stand
federateur1(config-if)#ip add
federateur1(config-if)#ip address 172.16.20.1
*Apr 15 11:04:56.876: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (20), with sw1 GigabitEthernet0/1 (
federateur1(config-if)#ip address 172.16.20.2 255.255.255.0
federateur1(config-if)#stand
federateur1(config-if)#standby 20 ip 172.16.20
*Apr 15 11:05:39.707: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw2 GigabitEthernet0/1 (1)
federateur1(config-if)#standby 20 ip 172.16.20.1
federateur1(config-if)#standby 20 prio
federateur1(config-if)#standby 20 priority 120
federateur1(config-if)#stand
federateur1(config-if)#standby pre
federateur1(config-if)#standby preempt
federateur1(config-if)#end
federateur1#copy
federateur1#copy
*Apr 15 11:05:42.062: %SYS-5-CONFIG_I: Configured from console by consoleru
federateur1#copy running-config st
federateur1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 4153 bytes to 2855 bytes[OK]
*Apr 15 11:05:36.873: %MSRP-5-STATECHANGE: Vlan20 Grp 20 state Standby -> Active
*Apr 15 11:05:37.397: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
federateur1#show
*Apr 15 11:05:38.686: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
federateur1#show sta
federateur1#show standby
*Apr 15 11:05:42.241: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (20), with sw1 GigabitEthernet0/1 (1)
federateur1#show standby bri
federateur1#show standby brief
P indicates configured to preempt.
Interface Grp Pri P State Active Standby Virtual IP
Vl10 10 120 Init unknown unknown 172.16.10.1
Vl15 15 120 Init unknown unknown 172.16.15.1
Vl20 20 120 Active local unknown 172.16.20.1
federateur1#
*Apr 15 11:05:55.943: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/0 (20), with sw2 GigabitEthernet0/1 (1)
*Apr 15 11:06:32.668: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (20), with sw1 GigabitEthernet0/1 (1)

```

FIGURE 2.49 – Standby fed1

2.6.7 Ethernet Channel mode TRUNK

Les canaux Ethernet ont été configurés en mode TRUNK pour autoriser les VLAN 10, 15, 20 et 30, avec la création spécifique du VLAN 30 sur les deux fédérateurs

```

Switch>enable
Switch#ch
Switch#ch
Switch#conf
Switch#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int
Switch(config)#interface vlan 30
Switch(config-if)#
*Apr 4 00:55:50.061: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to down
Switch(config-if)#ip add
Switch(config-if)#ip address 192.168.1.45 255.255.255.252
Switch(config-if)#no sh
Switch(config-if)#no shutdown
Switch(config-if)#
*Apr 4 00:56:45.459: %LINK-3-UPDOWN: Interface Vlan30, changed state to down
Switch(config-if)#exit
Switch(config)#int
Switch(config)#
Switch(config)#Switch(config-if)#
^
% Invalid input detected at '^' marker.
Switch(config)#
Switch(config)#Switch(config-if)#
^
% Invalid input detected at '^' marker.
Switch(config)#abitEthernet 0/0 , gigabitEthernet 1/0 , gigabitEthernet 0/3
Switch(config-if-range)#cha
Switch(config-if-range)#channel-gr
Switch(config-if-range)#channel-group 1 mod ?
active Enable LACP unconditionally
auto Enable PAGP only if a PAGP device is detected
desirable Enable PAGP unconditionally
on Enable Etherchannel only
passive Enable LACP only if a LACP device is detected
Switch(config-if-range)#channel-group 1 mode ?
active Enable LACP unconditionally
auto Enable PAGP only if a PAGP device is detected
desirable Enable PAGP unconditionally
on Enable Etherchannel only
passive Enable LACP only if a LACP device is detected
Switch(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1
Switch(config-if-range)#
*Apr 4 01:05:39.052: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
*Apr 4 01:05:40.052: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
Switch(config-if-range)#shu
Switch(config-if-range)#shutdown

```

FIGURE 2.50 – Ethernet channel mode trunk federateur 1

```
Switch#
*Apr  4 01:06:31.270: %SYS-5-CONFIG_I: Configured from console by console
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int
Switch(config)#interface por
Switch(config)#interface port ch
Switch(config)#interface port
Switch(config)#interface port-
Switch(config)#interface port-channel 1
Switch(config-if)#swi
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk enc
Switch(config-if)#switchport trunk encapsulation do
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#swit
Switch(config-if)#switchm
Switch(config-if)#switch mo
Switch(config-if)#switchp
Switch(config-if)#switchport tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#swit
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk all
Switch(config-if)#switchport trunk allowed v
Switch(config-if)#switchport trunk allowed vlan 10,15,20,30
Switch(config-if)#exit
Switch(config)#%abittEthernet 0/0 , gigabitEthernet 1/0 , gigabitEthernet 0/3
Switch(config-if-range)#no sh
Switch(config-if-range)#no shutdown
Switch(config-if-range)#end
*Apr  4 01:08:21.130: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
*Apr  4 01:08:21.257: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Apr  4 01:08:21.378: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*Apr  4 01:08:21.493: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed state to up
*Apr  4 01:08:22.134: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
Switch#
*Apr  4 01:08:22.257: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
*Apr  4 01:08:22.385: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
*Apr  4 01:08:22.496: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/3, changed state to up
*Apr  4 01:08:22.904: %SYS-5-CONFIG_I: Configured from console by console
*Apr  4 01:08:24.385: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
*Apr  4 01:08:25.385: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
Switch#wr
Building configuration...
Compressed configuration from 3775 bytes to 1829 bytes[OK]
Switch#
*Apr  4 01:08:39.422: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait.
..
```

FIGURE 2.51 – Ethernet channel mode trunk federateur 1

```
federateur2
federateur2(config-if-range)#shutdown
federateur2(config-if-range)#
*Apr  4 01:18:28.410: %SEC-5-COMPATIBLE: Gi0/3 is compatible with port-channel members
*Apr  4 01:18:28.420: %SEC-5-COMPATIBLE: Gi1/0 is compatible with port-channel members
*Apr  4 01:18:30.315: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
*Apr  4 01:18:30.370: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down
*Apr  4 01:18:30.406: %LINK-3-UPDOWN: Interface Port-channel1, changed state to down
federateur2(config-if-range)#exit
*Apr  4 01:18:30.449: %LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to administratively down
*Apr  4 01:18:30.499: %LINK-5-CHANGED: Interface GigabitEthernet0/3, changed state to administratively down
*Apr  4 01:18:31.317: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
*Apr  4 01:18:31.370: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
*Apr  4 01:18:31.408: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to down
federateur2(config)#exit
federateur2(config)#exit
federateur2#
*Apr  4 01:18:36.414: %SYS-5-CONFIG_I: Configured from console by console
federateur2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
federateur2(config)#int
federateur2(config)#interface por
federateur2(config)#interface port-ch
federateur2(config)#interface port-channel 1
federateur2(config-if)#swi
federateur2(config-if)#switchport port tr
federateur2(config-if)#switchport port tr
federateur2(config-if)#switchport trunk enc
federateur2(config-if)#switchport trunk encapsulation do
federateur2(config-if)#switchport trunk encapsulation dot1q
federateur2(config-if)#swit
federateur2(config-if)#switchport mo
federateur2(config-if)#switchport mode tr
federateur2(config-if)#switchport mode trunk
federateur2(config-if)#swi
federateur2(config-if)#switchport tr
federateur2(config-if)#switchport trunk al
federateur2(config-if)#switchport trunk allowed vlan 10,15,20,30
federateur2(config-if)#exit
federateur2(config)#%abittEthernet 1/0 , gigabitEthernet 0/3
federateur2(config-if-range)#no sh
federateur2(config-if-range)#no shutdown
federateur2(config-if-range)#end
federateur2#
*Apr  4 01:20:57.961: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Apr  4 01:20:58.081: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Apr  4 01:20:58.237: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*Apr  4 01:20:58.359: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed state to up
*Apr  4 01:20:58.470: %SYS-5-CONFIG_I: Configured from console by console
*Apr  4 01:20:58.961: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

FIGURE 2.52 – Ethernet channel mode trunk federateur 2

```

federateur2>en
federateur2#enable
federateur2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
federateur2(config)#int
federateur2(config)#interface vlan 30
federateur2(config-if)#
*Apr  4 01:14:27.552: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to down
federateur2(config-if)#ip address 192.168.1.45 255.255.255.252
federateur2(config-if)#ip address 192.168.1.46 255.255.255.252
federateur2(config-if)#no sh
federateur2(config-if)#no shutdown
federateur2(config-if)#
*Apr  4 01:15:29.737: %LINK-3-UPDOWN: Interface Vlan30, changed state to down
federateur2(config-if)#exit
federateur2(config)#set 0/0 , gigabitEthernet 1/0 , gigabitEthernet 0/3
federateur2(config-if-range)#ch
federateur2(config-if-range)#channel-gr
federateur2(config-if-range)#channel-group mode 1 ?
% Unrecognized command
federateur2(config-if-range)#channel-group mode ?
% Unrecognized command
federateur2(config-if-range)#channel-group mode channel-group 1 mod ?
% Unrecognized command
federateur2(config-if-range)#channel-group mode channel-group 1 mod
% Invalid input detected at '^' marker.
federateur2(config-if-range)#channel-group 1 mod ?
active      Enable LACP unconditionally
auto        Enable PAgp only if a PAgp device is detected
desirable   Enable PAgp unconditionally
on          Enable Etherchannel only
passive     Enable LACP only if a LACP device is detected
federateur2(config-if-range)#channel-group 1 mod
% Incomplete command.
federateur2(config-if-range)#chan
federateur2(config-if-range)#channel-gr
federateur2(config-if-range)#channel-group 1 mo
federateur2(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1
federateur2(config-if-range)#
*Apr  4 01:17:51.131: %EC-5-CANNOT_BUNDLE2: Gi1/0 is not compatible with Gi0/0 and will be suspended (trunk mode of Gi1/0 is trunk, Gi0/0 is access)
*Apr  4 01:17:51.155: %EC-5-CANNOT_BUNDLE2: Gi0/3 is not compatible with Gi0/0 and will be suspended (trunk mode of Gi0/3 is trunk, Gi0/0 is access)
*Apr  4 01:17:52.130: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to down
*Apr  4 01:17:52.150: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/3, changed state to down
*Apr  4 01:17:53.052: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
*Apr  4 01:17:54.052: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
federateur2(config-if-range)#sh
federateur2(config-if-range)#shutdown

```

FIGURE 2.53 – Ethernet channel mode trunk federateur 2

2.7 Branch 1

2.7.1 Création de VLAN

Nous avons créé deux VLANs sur le commutateur Layer 2 (SW3) de Branch1 pour isoler le trafic de gestion et de données.

```

SW3#show vlan brief

```

VLAN	Name	Status	Ports
1	default	active	Gi0/1, Gi0/2, Gi0/3, Gi1/0 Gi1/1, Gi1/2, Gi1/3, Gi2/0 Gi2/1, Gi2/2, Gi2/3, Gi3/0
101	management	active	
102	data	active	
103	VLAN0103	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```

SW3#

```

FIGURE 2.54 – show Vlan

2.7.2 Assignation de PC au VLAN

Nous avons assigné le PC3 au VLAN 102 pour le trafic de données.

```

SW3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#int g0/0
SW3(config-if)#swi
SW3(config-if)#switchport mo
SW3(config-if)#switchport mode acc
SW3(config-if)#switchport mode access
SW3(config-if)#swit
SW3(config-if)#switchport acc
SW3(config-if)#switchport access vlan
SW3(config-if)#switchport access vlan 102
SW3(config-if)#end
SW3#show
*Apr 23 03:03:46.486: %SYS-5-CONFIG_I: Configured from console by console
% Type "show ?" for a list of subcommands
SW3#show vlan br
SW3#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Gi0/1, Gi0/2, Gi0/3, Gi1/0
                                           Gi1/1, Gi1/2, Gi1/3, Gi2/0
                                           Gi2/1, Gi2/2, Gi2/3, Gi3/0
101  management              active
102  data                     active    Gi0/0
103  VLAN0103                 active
1002 fddi-default             act/unsup
1003 token-ring-default     act/unsup
1004 fddinet-default         act/unsup
1005 trnet-default          act/unsup
SW3#

```

FIGURE 2.55 – Affectation du port

2.7.3 Lien entre Switch et routeur CE-Branch1

Nous avons configuré un lien TRUNK avec VLAN natif 101 entre le commutateur Switch3 et le routeur CE-Branch1.

```

SW3(config)#int g0/1
SW3(config-if)#switcp
SW3(config-if)#switchport tr
SW3(config-if)#switchport trunk enc
SW3(config-if)#switchport trunk encapsulation do
SW3(config-if)#switchport trunk encapsulation dot1q
SW3(config-if)#swit
SW3(config-if)#switchport mod
SW3(config-if)#switchport mode tr
SW3(config-if)#switchport mode trunk
SW3(config-if)#swit
SW3(config-if)#switchport tru
SW3(config-if)#switchport trunk nat
SW3(config-if)#switchport trunk native v
SW3(config-if)#switchport trunk native vlan 101
SW3(config-if)#swit
SW3(config-if)#switchport tr
SW3(config-if)#switchport trunk akk
SW3(config-if)#switchport trunk ll
SW3(config-if)#switchport trunkal
SW3(config-if)#switchport trunk all
SW3(config-if)#switchport trunk allowed vl
SW3(config-if)#switchport trunk allowed vlan 102,103
SW3(config-if)#end
SW3#wr
Building configuration...

*Apr 23 03:08:58.102: %SYS-5-CONFIG_I: Configured from console by consoleCompressed configuration from 3791 bytes to 1847 bytes[OK]
*Apr 23 03:09:07.778: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Apr 23 03:09:08.795: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
SW3#
SW3#show tr
SW3#show int
SW3#show interfaces tr
SW3#show interfaces trunk

Port      Mode      Encapsulation  Status        Native vlan
Gi0/1     on        802.1q         trunking      101

Port      Vlans allowed on trunk
Gi0/1     102-103

Port      Vlans allowed and active in management domain
Gi0/1     102-103

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/1     102-103
SW3#

```

FIGURE 2.56 – Config trunk de switch sw3 et routeur ce-Branch1

2.7.4 Routage Inter-VLAN

Nous avons créé des sous-interfaces sur le routeur CE-Branch1 pour permettre le routage entre les VLANs 101 et 102.

```
E12#conf t
Enter configuration commands, one per line. End with CNTL/Z.
E12(config)#in
E12(config)#interface g2/0
E12(config-if)#no sh
E12(config-if)#no shutdown
E12(config-if)#int
E12(config-if)#int
*Apr  5 02:08:54.435: %LINK-3-UPDOWN: Interface GigabitEthernet2/0, changed state to up
E12(config-if)#int
*Apr  5 02:08:54.435: %ENTITY_ALARM-6-INFO: CLEAR INFO Gi2/0 Physical Port Administrative State Down
*Apr  5 02:08:55.435: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to up
E12(config-if)#inter
E12(config-if)#interface g2/0.101
E12(config-subif)#enc
E12(config-subif)#encapsulation d
E12(config-subif)#encapsulation dot1Q 101
E12(config-subif)#ip add
E12(config-subif)#ip address 172.16.101.3 255.255.255.0
E12(config-subif)#exit
E12(config)#int
E12(config)#interface g2/0.101
E12(config-subif)#encapsulation dot1Q 101
E12(config-subif)#ip address 172.16.101.1 255.255.255.0
E12(config-subif)#exit
E12(config)#int
E12(config)#interface g2/0.102
E12(config-subif)#enc
E12(config-subif)#encapsulation do
E12(config-subif)#encapsulation dot1Q 102
E12(config-subif)#ip add
E12(config-subif)#ip address 172.16.102.1 255.255.255.0
E12(config-subif)#exit
E12(config)#exit
E12#wr
*Apr  5 02:11:10.703: %SYS-5-CONFIG_I: Configured from console by console
E12#wr
Building configuration...
[OK]
E12#
```

FIGURE 2.57 – routage Inter-vlan

2.7.5 @IPManagement de Swich Layer2 (Sw3) de VLAN101

Nous avons attribué une adresse IP de gestion au commutateur Layer 2 de VLAN 101.

```
% Ambiguous command: "e"
SW3(config)#in
SW3(config)#interface vlan 101
SW3(config-if)#ip add
SW3(config-if)#ip address 172.16.101.100 255.255.255.0
SW3(config-if)#exit
SW3(config)#wr
SW3(config)#^
% Invalid input detected at '^' marker.

SW3(config)#exit
SW3#w
*Apr  5 01:12:43.152: %SYS-5-CONFIG_I: Configured from console by consoler
Building configuration...
█
```

FIGURE 2.58 – IPManagement de Swich Layer2 (Sw3) de VLAN101

2.7.6 Service DHCP au niveau Router CE-Branch1

Nous avons configuré le service DHCP sur le routeur CE-Branch1 pour le VLAN 102, en réservant les 10 premières adresses IP.

```
User Access Verification

Password:
CE12#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CE12(config)#ip dhc
CE12(config)#ip dhcp ex
CE12(config)#ip dhcp excluded-address 172.16.102.1 172.16.102.10
CE12(config)#ip dh
CE12(config)#ip dhcp po
CE12(config)#ip dhcp pool vl
CE12(config)#ip dhcp pool vla
CE12(config)#ip dhcp pool vlan102
CE12(dhcp-config)#net
CE12(dhcp-config)#netw
CE12(dhcp-config)#network 172.16.102.0 255.255.255.0
CE12(dhcp-config)#def
CE12(dhcp-config)#default-router 172.16.102.1
CE12(dhcp-config)#end
CE12#wr
Building configuration...
[OK]
CE12#
*Apr 22 11:59:24.387: %SYS-5-CONFIG_I: Configured from console by console
```

FIGURE 2.59 – config service dhcp au niveau routeur CE-Branch1



```
Welcome to Virtual PC Simulator, version 0.8.3
Dedicated to Daling.
Build time: Sep 9 2023 11:15:00
Copyright (c) 2007-2015, Paul Neng (mirnshi@gmail.com)
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.

Press '?' to get help.

Executing the startup file

PC4> ip dhcp
DDORA IP 172.16.102.11/24 GW 172.16.102.1
PC4>
```

FIGURE 2.60 – ip dhcp de pc4

2.7.7 Sécurité des appareils

Nous avons configuré les mots de passe de console, de VTY et d'activation conformément aux directives de sécurité spécifiques, renforçant ainsi la sécurité des appareils réseau.

```

CE12#
CE12#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CE12(config)#in
CE12(config)#interface g2/0
CE12(config-if)#no sh
CE12(config-if)#no shutdown
CE12(config-if)#int
CE12(config-if)#int
*Apr  5 02:08:54.435: %LINK-3-UPDOWN: Interface GigabitEthernet2/0, changed state to up
CE12(config-if)#int
*Apr  5 02:08:54.435: %ENTITY_ALARM-6-INFO: CLEAR INFO Gi2/0 Physical Port Administrative State Down
*Apr  5 02:08:55.435: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to up
CE12(config-if)#inter
CE12(config-if)#interface g2/0.101
CE12(config-subif)#enc
CE12(config-subif)#encapsulation d
CE12(config-subif)#encapsulation dot1Q 101
CE12(config-subif)#ip add
CE12(config-subif)#ip address 172.16.101.3 255.255.255.0
CE12(config-subif)#exit
CE12(config)#int
CE12(config)#interface g2/0.101
CE12(config-subif)#encapsulation dot1Q 101
CE12(config-subif)#ip address 172.16.101.1 255.255.255.0
CE12(config-subif)#exit
CE12(config)#int
CE12(config)#interface g2/0.102
CE12(config-subif)#enc
CE12(config-subif)#encapsulation do
CE12(config-subif)#encapsulation dot1Q 102
CE12(config-subif)#ip add
CE12(config-subif)#ip address 172.16.102.1 255.255.255.0
CE12(config-subif)#exit
CE12(config)#exit
CE12#wr
*Apr  5 02:11:10.703: %SYS-5-CONFIG_I: Configured from console by console
CE12#wr
Building configuration...
[OK]
CE12#
CE12#
CE12#
CE12#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CE12(config)#ip ad
CE12(config)#ip dh
CE12(config)#ip dhcp ex
CE12(config)#ip dhcp excluded-address 172.16.102.1 172.16.102.10
CE12(config)#ip dh
CE12(config)#ip dhcp pool vlan 102
CE12(config)#ip dhcp pool ^
% Invalid input detected at '^' marker.

CE12(config)#ip dhcp pool vlan102
CE12(dhcp-config)#net
CE12(dhcp-config)#net 172.16.102.0

```

FIGURE 2.61 – password ce12


```
SW3>en
SW3>enable
Password:
SW3#co
SW3#conf
SW3#configure t
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#vlan 103
SW3(config-vlan)#exit
SW3(config)#
SW3(config)#
SW3(config)#en
SW3(config)#ena
SW3(config)#enable sec
SW3(config)#enable secret issam
The enable secret you have chosen is the same as your enable password.
This is not recommended. Re-enter the enable secret.

SW3(config)#lin
SW3(config)#line co
SW3(config)#line console 0
SW3(config-line)#passo
SW3(config-line)#pass
SW3(config-line)#password issam
SW3(config-line)#lo
SW3(config-line)#log
SW3(config-line)#login
SW3(config-line)#exit
SW3(config)#li
SW3(config)#line vty 0 15
SW3(config-line)#pass
SW3(config-line)#password issam
SW3(config-line)#login
SW3(config-line)#end
SW3#
*Apr  5 01:27:01.119: %SYS-5-CONFIG_I: Configured from console by console
SW3#wr
Building configuration...
█
```

FIGURE 2.62 – password sw3

2.8 Branch 2

2.8.1 Création de VLAN

Nous avons créé deux VLANs sur le commutateur Layer 2 (SW4) de Branch2 pour isoler le trafic de gestion et de données.

```

switch4
Switch>en
Switch>enable
Password:
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 103
Switch(config-vlan)#name manag
Switch(config-vlan)#name management
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#int
Switch(config)#interface vlan 103
Switch(config-if)#ip add
Switch(config-if)#ip address
*Apr  5 01:29:12.856: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan103, changed state to down
% Incomplete command.

Switch(config-if)#ip address 172.16.103.4 255.255.255.0
Switch(config-if)#exit
Switch(config)#vlan 104
Switch(config-vlan)#name data
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#int
Switch(config)#interface vlan 104
Switch(config-if)#
*Apr  5 01:30:01.335: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan104, changed state to down*
^
% Invalid input detected at '^' marker.

Switch(config-if)#ip add
Switch(config-if)#ip address 172.16.104.4 255.255.255.0
Switch(config-if)#exit
Switch(config)#exit
Switch#wr
Building configuration...

```

FIGURE 2.63 – creation de vlan 103 et 104

2.8.2 Assignation de PC au VLAN

Nous avons assigné le PC4 au VLAN 104 pour le trafic de données.

```

SW4(config-if)#sw
SW4(config-if)#switchport mo
SW4(config-if)#switchport mode ac
SW4(config-if)#switchport mode access
SW4(config-if)#swi
SW4(config-if)#switchport ac
SW4(config-if)#switchport access vl
SW4(config-if)#switchport access vlan 104
SW4(config-if)#end
SW4#wr
Building configuration...

*Apr 23 03:22:48.495: %SYS-5-CONFIG_I: Configured from console by consoleCompressed configuration from 3767 bytes to 1814 bytes[OK]
*Apr 23 03:22:58.897: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
SW4#
SW4#
*Apr 23 03:22:59.930: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
SW4#sho
SW4#sho v
SW4#show v
SW4#show vl
SW4#show vlan br
SW4#show vlan brief

```

VLAN	Name	Status	Ports
1	default	active	Gi0/2, Gi0/3, Gi1/0, Gi1/1 Gi1/2, Gi1/3, Gi2/0, Gi2/1 Gi2/2, Gi2/3, Gi3/0, Gi3/1 Gi3/2, Gi3/3
102	VLAN0102	active	
103	management	active	
104	data	active	Gi0/0
1002	fdi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdinet-default	act/unsup	
1005	trnet-default	act/unsup	

```

SW4#

```

FIGURE 2.64 – Affectation de port

2.8.3 Lien entre Switch et routeur CE-Branch2

Nous avons configuré un lien TRUNK avec VLAN natif 103 entre le commutateur Switch4 et le routeur CE-Branch2.

```
Switch#
Switch#
Switch#
Switch#int
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int
Switch(config)#interface g0/0
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode acces
Switch(config-if)#switchport mode access
Switch(config-if)#swit
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vlan 104
Switch(config-if)#exit
Switch(config)#int
Switch(config)#interface g0/1
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk en
Switch(config-if)#switchport trunk encapsulation do
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#sw
Switch(config-if)#switchport mo
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk na
Switch(config-if)#switchport trunk native 103
Switch(config-if)#switchport trunk native 103
Switch(config-if)#end
Switch#wr
Building configuration...

*Apr  5 01:34:18.355: %SYS-5-CONFIG_I: Configured from console by consoleCompressed configuration from
3713 bytes to 1758 bytes[OK]
Switch#
*Apr  5 01:34:30.123: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait.
..
*Apr  5 01:34:31.113: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.[]
```

FIGURE 2.65 – Mode trunk sw4

2.8.4 Routage Inter-VLAN

Nous avons créé des sous-interfaces sur le routeur CE-Branch1 pour permettre le routage entre les VLANs 103 et 104.

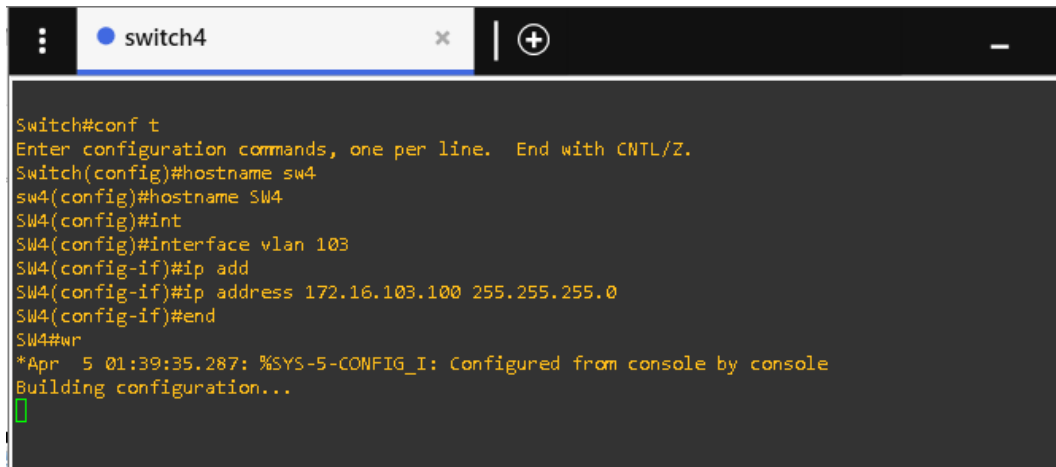
```
CE22#en
CE22#enable
CE22#con
CE22#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CE22(config)#int
CE22(config)#interface g0/0
^
% Invalid input detected at '^' marker.

CE22(config)#interface g2/0
CE22(config-if)#no
CE22(config-if)#no sh
CE22(config-if)#no shutdown
CE22(config-if)#
*Apr  5 02:38:52.459: %LINK-3-UPDOWN: Interface GigabitEthernet2/0, changed state to up
CE22(config-if)#int
CE22(config-if)#int
*Apr  5 02:38:52.459: %ENTITY_ALARM-6-INFO: CLEAR INFO Gi2/0 Physical Port Administrative State Down
*Apr  5 02:38:53.459: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0, changed state to up
CE22(config-if)#int
CE22(config-if)#interface g2/0.103
CE22(config-subif)#enc
CE22(config-subif)#encapsulation d
CE22(config-subif)#encapsulation dot1Q 103
CE22(config-subif)#ip add
CE22(config-subif)#ip address 172.16.103.1 255.255.255.0
CE22(config-subif)#exit
CE22(config)#int
CE22(config)#interface g2/0.104
CE22(config-subif)#enc
CE22(config-subif)#encapsulation d
CE22(config-subif)#encapsulation dot1Q 104
CE22(config-subif)#ip add
CE22(config-subif)#ip address 172.16.104.1 255.255.255.0
CE22(config-subif)#exit
CE22(config)#exit
CE22#wr
*Apr  5 02:40:24.507: %SYS-5-CONFIG_I: Configured from console by console
CE22#wr
Building configuration...
[OK]
CE22#
```

FIGURE 2.66 – routage Inter-vlan

2.8.5 adresse IP Management de Switch Layer2 (Sw4) de VLAN103

Nous avons attribué une adresse IP de gestion au commutateur Layer 2 de VLAN 103.

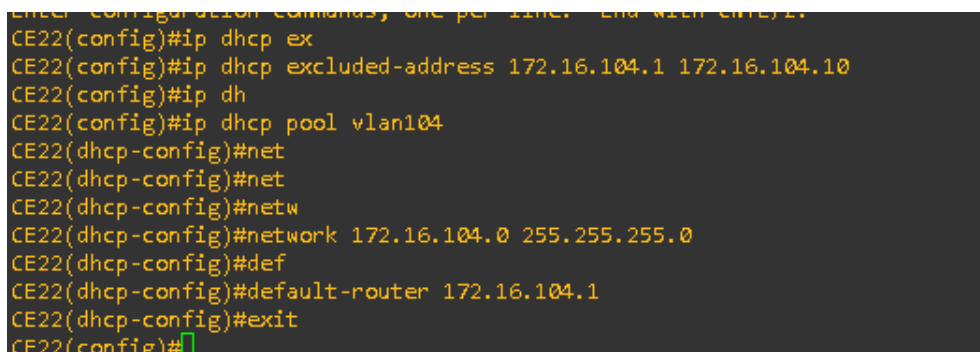


```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname sw4
sw4(config)#hostname SW4
SW4(config)#int
SW4(config)#interface vlan 103
SW4(config-if)#ip add
SW4(config-if)#ip address 172.16.103.100 255.255.255.0
SW4(config-if)#end
SW4#wr
*Apr  5 01:39:35.287: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...
[ ]
```

FIGURE 2.67 – IP Management de Switch Layer2 (Sw4) de VLAN103

2.8.6 Service DHCP au niveau Router CE-Branch2

Nous avons configuré le service DHCP sur le routeur CE-Branch2 pour le VLAN 104, en réservant les 10 premières adresses IP.



```
Enter configuration commands, one per line. End with CNTL/Z.
CE22(config)#ip dhcp ex
CE22(config)#ip dhcp excluded-address 172.16.104.1 172.16.104.10
CE22(config)#ip dh
CE22(config)#ip dhcp pool vlan104
CE22(dhcp-config)#net
CE22(dhcp-config)#net
CE22(dhcp-config)#netw
CE22(dhcp-config)#network 172.16.104.0 255.255.255.0
CE22(dhcp-config)#def
CE22(dhcp-config)#default-router 172.16.104.1
CE22(dhcp-config)#exit
CE22(config)#
```

FIGURE 2.68 – Service DHCP au niveau Router CE-Branch2

2.8.7 Sécurité des appareils

Nous avons configuré les mots de passe de console, de VTY et d'activation conformément aux directives de sécurité spécifiques, renforçant ainsi la sécurité des appareils réseau.

```
E22(config)#enable sec
E22(config)#enable secret issam
E22(config)#line
E22(config)#line cons
E22(config)#line console 0
E22(config-line)#pass
E22(config-line)#password issam
E22(config-line)#login
E22(config-line)#exit
E22(config)#lin
E22(config)#line vty 0 15
E22(config-line)#pass
E22(config-line)#password issam
E22(config-line)#login
E22(config-line)#exit
E22(config)#en
E22(config)#exit
E22#wr
Building configuration...
OK]
E22#
Apr  5 02:46:42.151: %SYS-5-CONFIG_I: Configured from console by console
E22#
```

FIGURE 2.69 – password ce22

```
switch4
SW4(config)#enab
SW4(config)#enable se
SW4(config)#enable secret issam
The enable secret you have chosen is the same as your enable password.
This is not recommended. Re-enter the enable secret.

SW4(config)#line co
SW4(config)#line console 0
SW4(config-line)#pass
SW4(config-line)#password issam
SW4(config-line)#login
SW4(config-line)#exit
SW4(config)#line vty 0 15
SW4(config-line)#password issam
SW4(config-line)#login
SW4(config-line)#exit
SW4(config)#wr
^
% Invalid input detected at '^' marker.

SW4(config)#exit
SW4#wr
Building configuration...
*Apr  5 01:45:47.784: %SYS-5-CONFIG_I: Configured from console by console
```

FIGURE 2.70 – password sw4

2.9 Test et Validation des Services de la Solution Redondante

Pour garantir l'efficacité de la solution redondante mise en place, nous avons réalisé plusieurs tests afin de valider le bon fonctionnement des services réseau et de nous assurer qu'ils répondaient aux exigences spécifiées dans notre projet.

```
Federateur1#sh standby brief
P indicates configured to preempt.
|
Interface  Grp Prio P State    Active        Standby        Virtual IP
Vl10       10  120 P Active   local         172.16.10.3    172.16.10.1
Vl15       15  120 P Active   local         172.16.15.3    172.16.15.1
Vl20       20  120 P Active   local         172.16.20.3    172.16.20.1
Federateur1#
```

FIGURE 2.71 – Redondance HSRP sur le fédérateur 1

```
Federateur2#sh standby brief
P indicates configured to preempt.
|
Interface  Grp Prio P State    Active        Standby        Virtual IP
Vl10       10  105 P Standby  172.16.10.2    local          172.16.10.1
Vl15       15  105 P Standby  172.16.15.2    local          172.16.15.1
Vl20       20  105 P Standby  172.16.20.2    local          172.16.20.1
Federateur2#
```

FIGURE 2.72 – Redondance HSRP sur le fédérateur 2

```
PC1> ip dhcp
DDORA IP 172.16.10.11/24 GW 172.16.10.1
```

FIGURE 2.73 – Configuration DHCP réussie sur le PC1

```
PC1> ping 172.16.15.11

84 bytes from 172.16.15.11 icmp_seq=1 ttl=63 time=427.036 ms
84 bytes from 172.16.15.11 icmp_seq=2 ttl=63 time=330.251 ms
84 bytes from 172.16.15.11 icmp_seq=3 ttl=63 time=205.647 ms
84 bytes from 172.16.15.11 icmp_seq=4 ttl=63 time=305.110 ms
84 bytes from 172.16.15.11 icmp_seq=5 ttl=63 time=351.306 ms
```

FIGURE 2.74 – Vérification de la connexion entre PC1 et PC2

```
PC3> ping 172.16.104.11

84 bytes from 172.16.104.11 icmp_seq=1 ttl=61 time=901.715 ms
84 bytes from 172.16.104.11 icmp_seq=2 ttl=61 time=942.921 ms
84 bytes from 172.16.104.11 icmp_seq=3 ttl=61 time=876.674 ms
84 bytes from 172.16.104.11 icmp_seq=4 ttl=61 time=799.774 ms
84 bytes from 172.16.104.11 icmp_seq=5 ttl=61 time=943.478 ms
```

FIGURE 2.75 – Vérification de la connexion entre PC3 et PC4

```
PC1> trace 172.16.15.11
trace to 172.16.15.11, 8 hops max, press Ctrl+C to stop
 1  172.16.10.2    180.935 ms  155.953 ms  317.361 ms
 2  172.16.15.3    320.944 ms
```

FIGURE 2.76 – Tracé de route vers PC2 depuis PC1

```
PC3> trace 172.16.104.11
trace to 172.16.104.11, 8 hops max, press Ctrl+C to stop
 1  172.16.102.1    253.574 ms  243.221 ms  305.594 ms
 2  192.168.1.9     347.698 ms  399.032 ms  557.614 ms
 3  192.168.1.14    569.530 ms  618.979 ms  612.508 ms
 4  *172.16.104.11  808.694 ms (ICMP type:3, code:3, D
```

FIGURE 2.77 – Tracé de route vers PC4 depuis PC3

2.10 Conclusion

En conclusion, la configuration des VLANs, des modes de liaison trunk, des mots de passe pour les routeurs, ainsi que la mise en place des services DHCP et du protocole HSRP sont des éléments essentiels pour garantir la stabilité, la sécurité et l'efficacité des réseaux IP/MPLS. En suivant les bonnes pratiques et en mettant en place ces configurations de manière appropriée, les organisations peuvent assurer une connectivité réseau fiable et résiliente pour répondre aux besoins croissants de leurs utilisateurs

chapitre 3

Conception et mise en place de la Solution de Monitoring et Sécurité AAA

3.1 Introduction

La troisieme partie de ce rapport concentre on Authentication, Authorization, and Accounting (AAA), crucial components in managing access to networks, systems, and resources. By carefully designing and deploying such a solution, organizations can bolster their security measures, effectively control access, and proactively monitor network activities for potential threats and vulnerabilities.

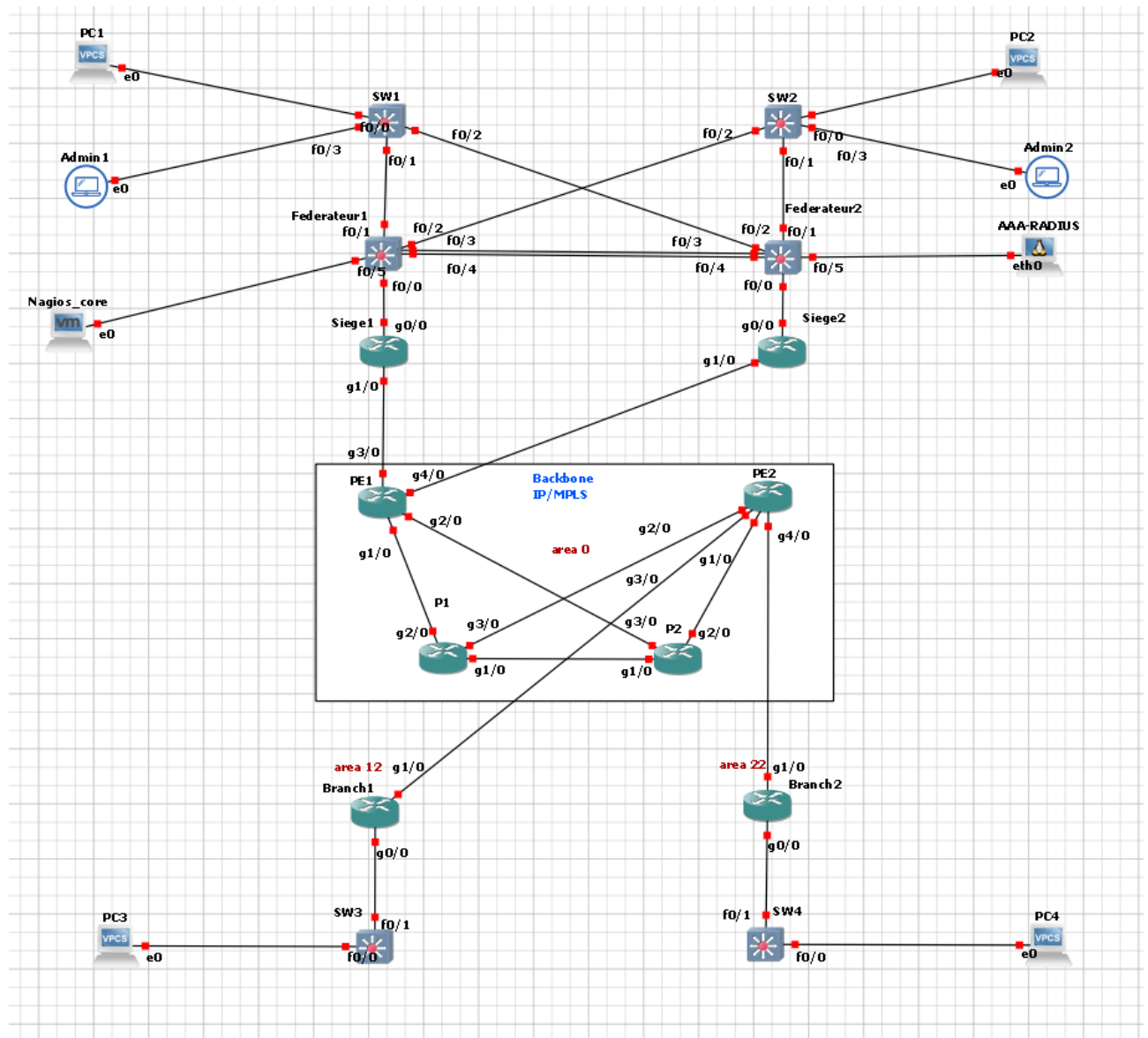


FIGURE 3.78 – Architecture de Partie 3

3.2 Choix de la Solution Monitoring

Le choix de Nagios Core comme solution de monitoring" représente une décision stratégique dans la gestion des infrastructures informatiques. Nagios Core est une plateforme de surveillance open-source reconnue pour sa flexibilité, sa fiabilité et sa capacité à surveiller un large éventail d'applications, de services et de périphériques.



FIGURE 3.79 – Logo de Nagios Core

3.3 Model de fonctionnement de la Solution Monitoring

Le modèle de fonctionnement de Nagios Core repose sur une architecture de surveillance distribuée et modulaire. Voici les principaux éléments de son fonctionnement :

- **Configuration** : Tout commence par la configuration. Les administrateurs définissent les services, les hôtes, et les commandes à surveiller dans des fichiers de configuration spécifiques. Cela inclut la définition des seuils de tolérance, des périodicités de vérification, des contacts d'alerte, etc.

- **Planification des vérifications** : Nagios Core planifie les vérifications en fonction des directives de configuration définies. Il exécute périodiquement des vérifications pour s'assurer que les services et les hôtes surveillés sont disponibles et répondent correctement.

- **Exécution des vérifications** : Nagios Core exécute les vérifications en utilisant des plugins spécifiques pour chaque type de service ou de périphérique surveillé. Ces plugins envoient des requêtes aux services ou périphériques surveillés et analysent les réponses pour détecter les problèmes.

- **Traitement des résultats** : Une fois les vérifications effectuées, Nagios Core traite les résultats et les compare aux seuils définis dans la configuration. Si une anomalie est

détectée, une alerte est déclenchée.

- **Gestion des alertes** : Nagios Core envoie des notifications d’alerte aux contacts spécifiés dans la configuration lorsque des problèmes sont détectés. Ces alertes peuvent être envoyées par e-mail, SMS, ou d’autres moyens définis par l’administrateur.

- **Visualisation des données** : Nagios Core offre des interfaces Web pour visualiser les données de surveillance, y compris les statuts actuels, les tendances historiques, et les rapports de performances.

- **Maintenance et ajustements** : Les administrateurs peuvent effectuer des ajustements à la configuration de surveillance, ajouter de nouveaux services à surveiller, ou modifier les seuils de tolérance en fonction des besoins changeants de l’infrastructure.

Ce modèle de fonctionnement permet à Nagios Core de surveiller de manière proactive les infrastructures informatiques, de détecter rapidement les problèmes potentiels, et d’alerter les équipes d’administration pour une intervention rapide, minimisant ainsi les temps d’arrêt et maximisant la disponibilité des services.

3.4 Mise en place de la Solution Monitoring

La mise en place de Nagios Core comme solution de monitoring implique plusieurs étapes clés :

Étape 1 : Installer les dépendances requises

Avant d’installer Nagios, nous devons installer les paquets requis. Ouvrez un terminal ou SSH sur votre serveur et exécutez les commandes suivantes :

```
sudo apt update
sudo apt install -y autoconf gcc libc6 make wget unzip apache2 php libapache2-
mod-php7.4 libgd-dev
```

Étape 2 : Créer un utilisateur et un groupe Nagios Nagios a besoin d’un utilisateur et d’un groupe dédiés pour fonctionner. Créez-les en utilisant les commandes suivantes :

```
sudo useradd nagios
sudo groupadd nagcmd
sudo usermod -a -G nagcmd nagios
```

Étape 3 : Télécharger et compiler Nagios

Ensuite, téléchargez la dernière version de Nagios sur le site officiel. Au moment de la rédaction, la dernière version est Nagios 4.4.6. Veuillez consulter le site officiel de Nagios pour la version la plus récente.

```
cd /tmp
wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz
tar xzf nagios-*.tar.gz
cd nagios-4.4.6
./configure --with-nagios-group=nagios --with-command-group=nagcmd
```

Étape 4 : Installer les binaires et le service Nagios Installez les fichiers binaires, les scripts d'initialisation et les exemples de fichiers de configuration avec les commandes suivantes :

```
sudo make install
sudo make install-init
sudo make install-config
sudo make install-commandmode
```

Étape 5 : Installer l'interface Web Nagios

Configurez l'interface web et créez un utilisateur administrateur appelé 'nagiosadmin' (vous pouvez modifier le nom d'utilisateur selon vos préférences). Vous serez invité à créer un mot de passe pour cet utilisateur :

```
sudo make install-webconf
sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Activer les modules Apache rewrite et cgi :

```
sudo a2enmod réécriture cgi
sudo systemctl restart apache2
```

Étape 6 : Installer les plugins Nagios

Les plugins Nagios sont essentiels pour la surveillance des services. Installez-les avec les commandes suivantes :

```

cd /tmp
wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
tar xzf nagios-plugins-*.tar.gz
cd nagios-plugins-2.3.3
./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl
make
sudo make install

```

Étape 7 : Vérifier la configuration de Nagios

Avant de démarrer Nagios, exécutez la commande suivante pour vérifier toute erreur de configuration :

```
sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

Étape 8 : Démarrer le service Nagios

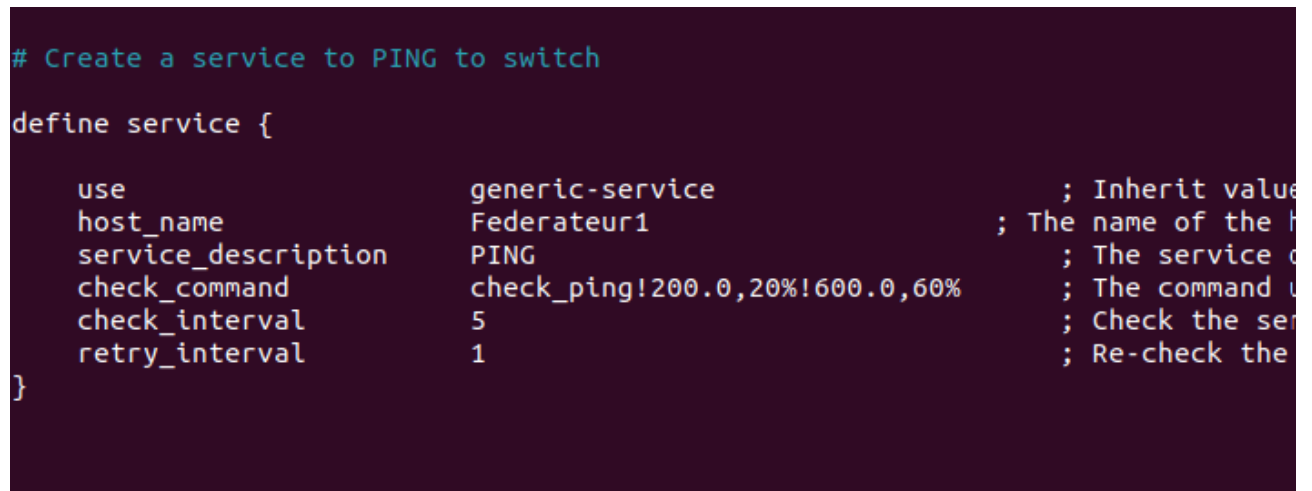
Maintenant, vous pouvez démarrer Nagios et l'activer pour l'exécuter au démarrage :

```

sudo systemctl start nagios.service
sudo systemctl enable nagios.service

```

Configuration de MySQL dans Nagios



```

# Create a service to PING to switch
define service {
    use                generic-service          ; Inherit values from the template
    host_name          Federateur1              ; The name of the host
    service_description PING                    ; The service description
    check_command       check_ping!200.0,20%!600.0,60% ; The command to run
    check_interval      5                       ; Check the service every 5 minutes
    retry_interval      1                       ; Re-check the service if it fails
}

```

FIGURE 3.80 – Configuration de MySQL

Authentication sur interface Web de Nagios Core

Avant d'accéder à l'interface web de Nagios Core, nous avons attribué une adresse IP 172.16.20.250/25 à notre serveur de gestion et de surveillance, avec une passerelle 172.16.20.1.

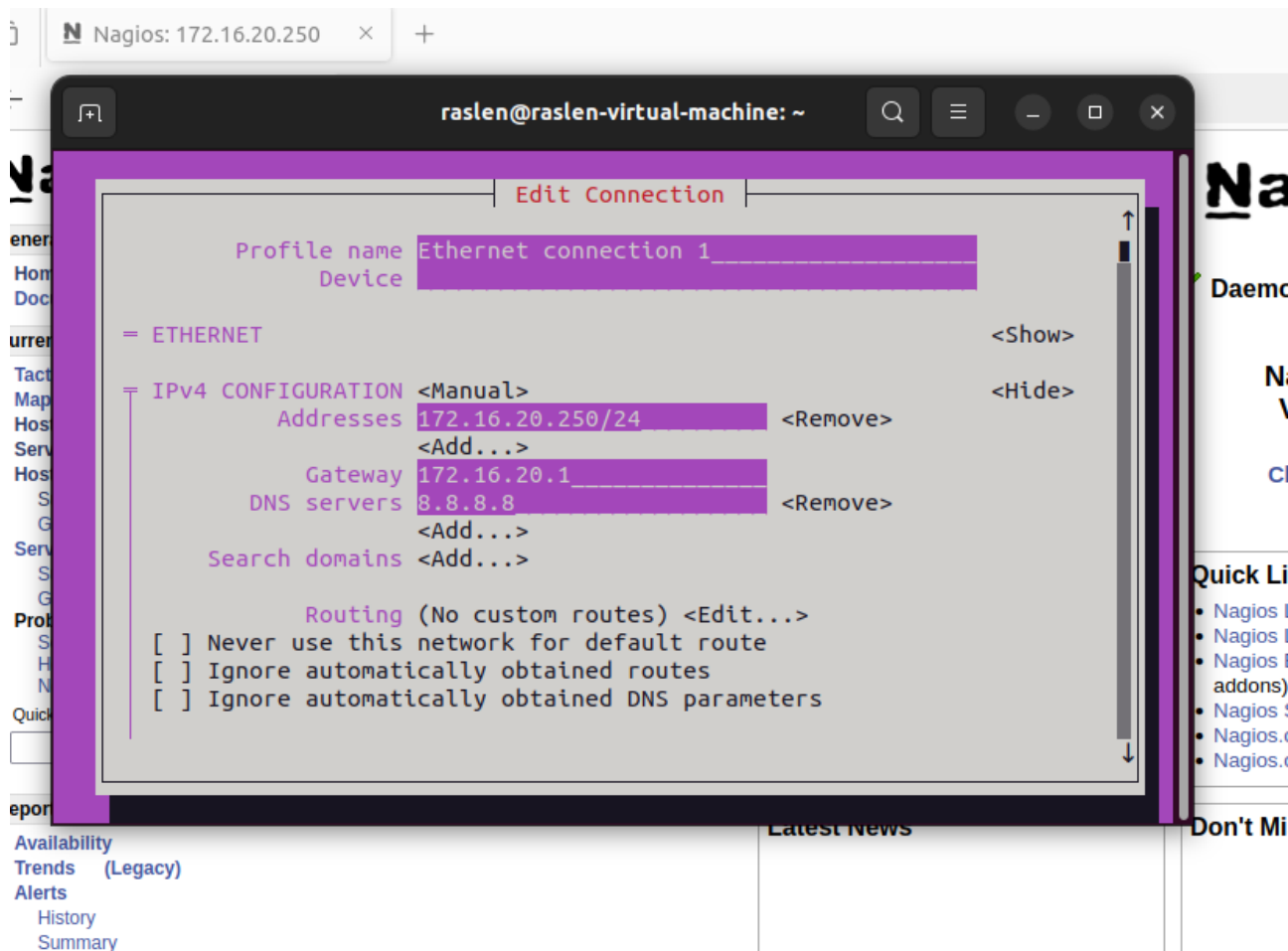


FIGURE 3.81 – Interface de configuration de connexion

Maintenant, nous pouvons accéder à l'interface Web de Nagios en naviguant vers <http://172.16.20.250/nagios> dans notre navigateur Web. Nous serons invités à entrer le nom d'utilisateur et le mot de passe que nous avons créé. Après une authentification réussie, vous obtiendrez l'accès au tableau de bord principal de Nagios.

Une fois l'authentification réussie, nous obtiendrons l'accès au tableau de bord principal de Nagios.

Ajout des routeurs et commutateurs sur dans Nagios

Nous avons ajouté CE11, CE12, CE21, CE22 et les SIX Switchs Layer 2 et Layer 3 sur Nagios Core

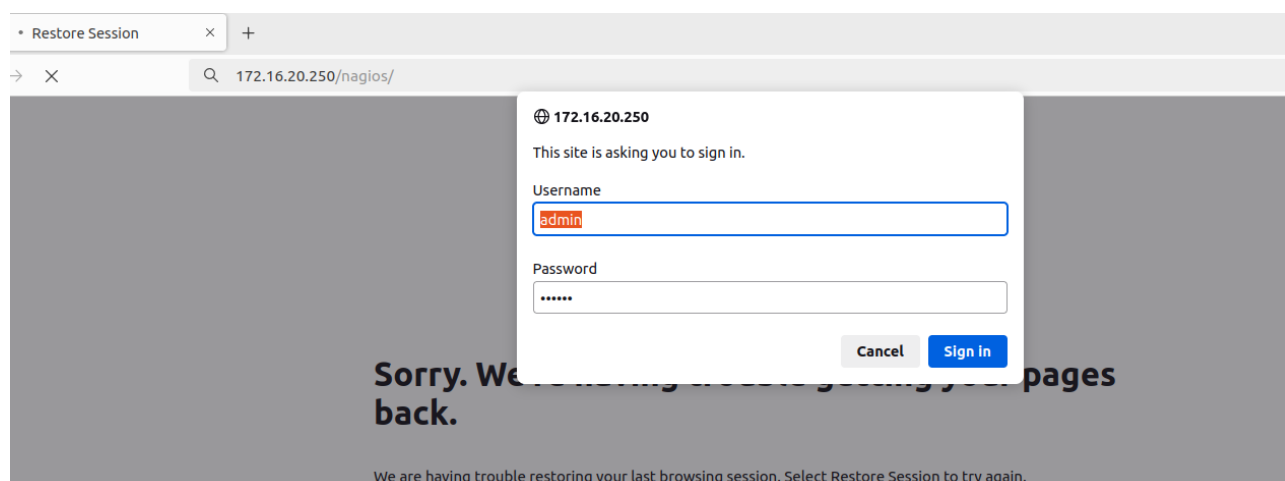


FIGURE 3.82 – Authentication au Nagios Cores

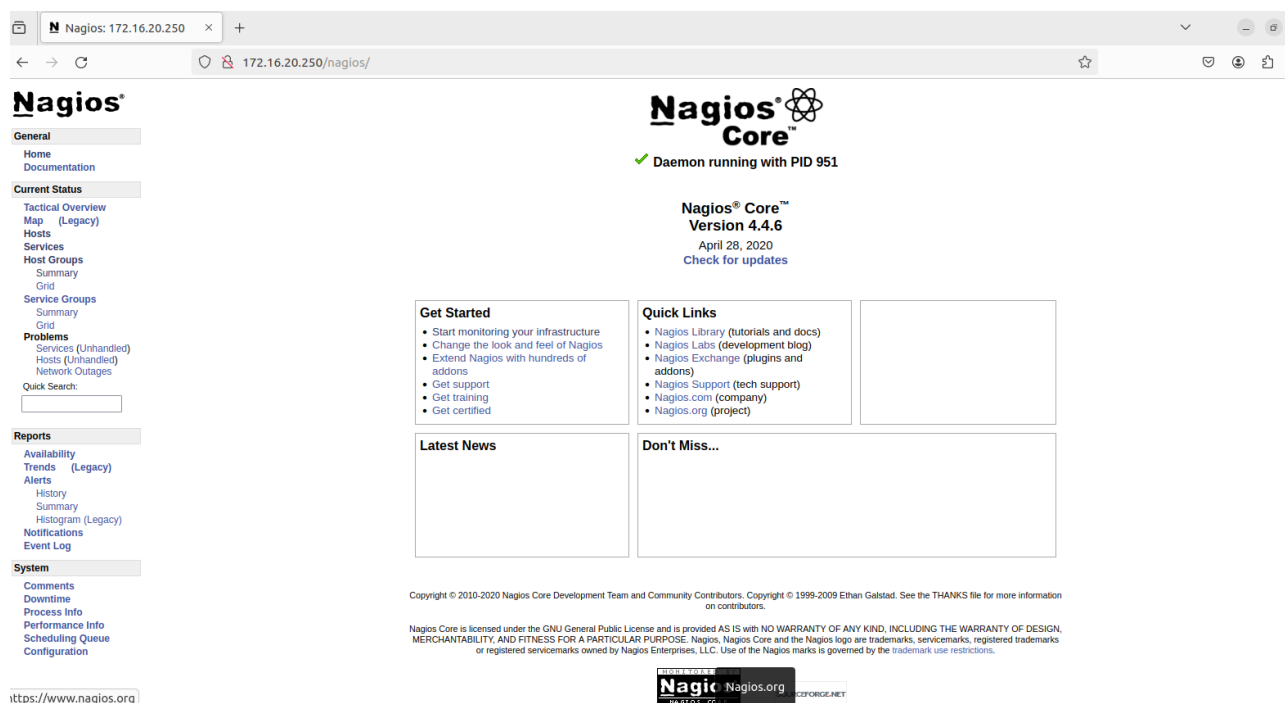


FIGURE 3.83 – Interface Web de Nagios Core

3.5 Test et Validation de la Solution Monitoring

Dans cette section, nous examinons les tests et la validation de la solution de monitoring mise en place. L'objectif principal est de s'assurer que la solution fonctionne comme prévu, qu'elle offre une surveillance efficace du réseau et qu'elle répond aux exigences de l'entreprise en termes de performance et de sécurité.


```
Fed1#ping 172.16.20.250

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.20.250, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/20/40 ms
```

FIGURE 3.84 – Vérification de la connexion entre nagios et le federateur1

3.5.1 Surveillance des Périphériques avec Nagios Core

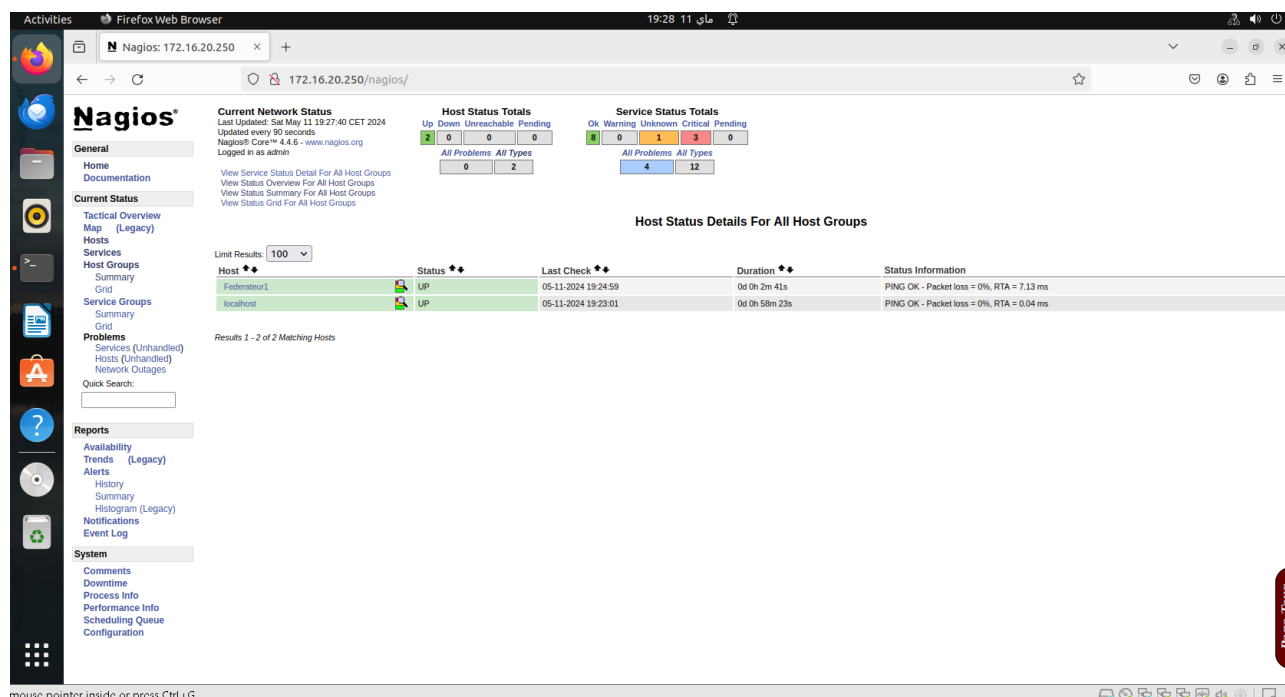


FIGURE 3.85 – Surveillance des Périphériques avec Nagios Core

3.6 Description de la Solution AAA

La solution AAA (Authentication, Authorization, and Accounting) est une approche intégrée pour contrôler et sécuriser l'accès aux ressources informatiques au sein d'un réseau. Voici une description de chaque composant de cette solution :

Authentication (Authentification) : Ce composant vérifie l'identité des utilisateurs ou des périphériques qui tentent d'accéder au réseau ou aux ressources. Il s'agit souvent du premier point de contact lorsqu'un utilisateur se connecte au système. Les méthodes d'authentification peuvent inclure des identifiants de connexion (nom d'utilisateur

et mot de passe), des certificats numériques, des jetons d'authentification, la biométrie, ou des méthodes d'authentification multifactorielle (MFA) pour renforcer la sécurité.

Authorization (Autorisation) : Une fois qu'un utilisateur est authentifié, ce composant détermine les actions qu'il est autorisé à effectuer et les ressources auxquelles il peut accéder. Cela implique de définir des politiques d'autorisation qui spécifient les permissions pour chaque utilisateur ou groupe d'utilisateurs. Les politiques d'autorisation peuvent être basées sur des rôles, des attributs d'utilisateur, des attributs de périphérique, ou d'autres critères spécifiques à l'organisation.

Accounting (Comptabilité) : Ce composant enregistre et stocke les informations sur l'utilisation des ressources par les utilisateurs authentifiés. Il permet de suivre les activités des utilisateurs, les tentatives de connexion, les opérations effectuées, les ressources accédées, et d'autres données pertinentes. Les informations de comptabilité sont essentielles pour l'audit de sécurité, la conformité réglementaire, la facturation des services, et la détection des activités suspectes ou non autorisées.

En combinant ces trois composants, la solution AAA offre un cadre complet pour contrôler l'accès aux systèmes informatiques, garantir l'intégrité des données et des ressources, et assurer la conformité aux politiques de sécurité. Elle joue un rôle crucial dans la protection des informations sensibles, la prévention des intrusions, et la gestion des risques liés à la sécurité informatique.

3.7 Mise en place de la Solution de sécurité AAA de Tekup

La mise en place d'une solution de sécurité AAA (Authentication, Autorisation et Accounting) est cruciale pour garantir la sécurité des systèmes informatiques. Voici un guide général pour la mise en place de cette solution :

- Analyse des besoins de sécurité :

Identifiez les besoins spécifiques en matière d'authentification, d'autorisation et de suivi des activités pour votre organisation Tekup. Évaluez les types d'utilisateurs et de ressources système qui nécessitent une protection.

- Sélection de la solution AAA :

Recherchez les solutions de sécurité AAA disponibles sur le marché qui répondent aux besoins de Tekup. Prenez en compte des facteurs tels que la compatibilité avec les systèmes existants, la facilité de gestion, la scalabilité et les fonctionnalités de sécurité offertes.

- Installation et configuration de la solution :

Installez la solution AAA choisie sur les serveurs appropriés de Tekup. Configurez les paramètres d'authentification pour définir les méthodes d'authentification acceptées (par exemple, nom d'utilisateur/mot de passe, authentification à deux facteurs, certificats, etc.). Configurez les règles d'autorisation pour déterminer les actions que les utilisateurs sont autorisés à effectuer une fois connectés. Mettez en place le mécanisme de suivi des activités (accounting) pour enregistrer les actions des utilisateurs et générer des journaux d'audit.

- Intégration avec les systèmes existants :

Assurez-vous que la solution AAA est correctement intégrée avec les systèmes et les applications déjà en place à Tekup. Testez l'intégration pour vous assurer que les utilisateurs peuvent accéder aux ressources appropriées de manière transparente .

- Formation du personnel et sensibilisation à la sécurité :

Fournissez une formation aux administrateurs système sur la gestion et la maintenance de la solution AAA. Sensibilisez les utilisateurs finaux aux bonnes pratiques en matière de sécurité, y compris l'importance de protéger leurs informations d'identification et de signaler les activités suspectes.

- Tests et évaluation continue :

Effectuez des tests de sécurité réguliers pour identifier les vulnérabilités et les lacunes potentielles dans la solution AAA. Révissez périodiquement la configuration de la solution en fonction des évolutions des besoins de sécurité et des nouvelles menaces.

- Gestion des incidents de sécurité :

Mettez en place un processus de gestion des incidents de sécurité pour répondre rapidement aux violations de sécurité potentielles ou avérées. Documentez les leçons apprises à partir des incidents de sécurité et utilisez-les pour améliorer la posture de sécurité globale de Tekup.

```
Siege2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Siege2(config)#aaa new-model
Siege2(config)#aaa authentication login default group radius local
Siege2(config)#aaa authorization exec default group radius local
Siege2(config)#radius-server host 172.16.20.200
Warning: The CLI will be deprecated soon
'radius-server host 172.16.20.200 '
Please move to 'radius server <name>' CLI.
Siege2(config)#radius-server key VPN_SSIR
Siege2(config)#aaa authentication login local_auth local
Siege2(config)#aaa authorization exec local_auth local
Siege2(config)#privilege exec level 1 configure terminal
Siege2(config)#privilege exec level 10 show running-config
Siege2(config)#privilege exec level 15 write memory
Siege2(config)#
Siege2(config)#radius-server host 172.16.20.200
Siege2(config)#exit
```

FIGURE 3.86 – mise en place server AAA en siege2

```
SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#aaa new-model
SW2(config)#aaa authentication login default group radius local
SW2(config)#aaa authorization exec default group radius local
SW2(config)#radius-server host 172.16.20.200
SW2(config)#radius-server key VPN_SSIR
SW2(config)#aaa authentication login local_auth local
SW2(config)#aaa authorization exec local_auth local
SW2(config)#privilege exec level 1 configure terminal
SW2(config)#privilege exec level 10 show running-config
SW2(config)#privilege exec level 15 write memory
SW2(config)#exit
SW2#wr
Building configuration...

*Mar 1 00:20:33.379: %SYS-5-CONFIG_I: Configured from console by belkis on console[OK]
SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#ip access-list extended TO-Sw2
SW2(config-ext-nacl)#host 172.16.20.100 host 172.16.20.102 range 22 23
SW2(config-ext-nacl)#host 172.16.20.150 host 172.16.20.102 range 22 23
SW2(config-ext-nacl)#deny ip any any log
SW2(config-ext-nacl)#exit
SW2(config)#line vty 0 15
SW2(config-line)#access-class TO-Sw2 in
SW2(config-line)#exit
```

FIGURE 3.87 – mise en place server AAA en SW2

```
Federateur2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Federateur2(config)#aaa new-model
Federateur2(config)#aaa authentication login default group radius local
Federateur2(config)#aaa authorization exec default group radius local
Federateur2(config)#radius-server host 172.16.20.200
Federateur2(config)#radius-server key VPN_SSIR
Federateur2(config)#aaa authentication login local_auth local
Federateur2(config)#aaa authorization exec local_auth local
Federateur2(config)#privilege exec level 1 configure terminal
Federateur2(config)#privilege exec level 10 show running-config
Federateur2(config)#privilege exec level 15 write memory
Federateur2(config)#exit
Federateur2#wr
```

FIGURE 3.88 – mise en place server AAA en Federateur 2

```
[OK]
Siegel#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Siegel(config)#aaa new-model
Siegel(config)#aaa authentication login default group radius local
Siegel(config)#aaa authorization exec default group radius local
Siegel(config)#radius-server host 172.16.20.200
Warning: The CLI will be deprecated soon
'radius-server host 172.16.20.200 '
Please move to 'radius server <name>' CLI.
Siegel(config)#radius-server key VPN_SSIR
Siegel(config)#aaa authentication login local_auth local
Siegel(config)#aaa authorization exec local_auth local
Siegel(config)#privilege exec level 1 configure terminal
Siegel(config)#privilege exec level 10 show running-config
Siegel(config)#privilege exec level 15 write memory
Siegel(config)#
Siegel#
*May  4 20:58:05.787: %SYS-5-CONFIG_I: Configured from console by belkis on console
Siegel#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Siegel(config)#radius-server host 172.16.20.200
Siegel(config)#exit
```

FIGURE 3.89 – mise en place server AAA en siegel


```

Branch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Branch1(config)#aaa new-model
Branch1(config)#aaa authentication login default group radius local
Branch1(config)#aaa authorization exec default group radius local
Branch1(config)#radius-server host 172.16.20.200
Warning: The CLI will be deprecated soon
'radius-server host 172.16.20.200 '
Please move to 'radius server <name>' CLI.
Branch1(config)#radius-server key VPN_SSIR
Branch1(config)#aaa authentication login local_auth local
Branch1(config)#aaa authorization exec local_auth local
Branch1(config)#privilege exec level 1 configure terminal
Branch1(config)#privilege exec level 10 show running-config
Branch1(config)#privilege exec level 15 write memory
Branch1(config)#radius-server host 172.16.20.200
Branch1(config)#exit
Branch1#wr
Building configuration...

*May  4 21:04:22.027: %SYS-5-CONFIG_I: Configured from console by belkis on console[OK]
Branch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Branch1(config)#ip access-list extended TO-Branch1
Branch1(config-ext-nacl)#host 172.16.20.100 host 172.16.12.12 range 22 23
Branch1(config-ext-nacl)#host 172.16.20.150 host 172.16.12.12 range 22 23
Branch1(config-ext-nacl)#deny ip any any log
Branch1(config-ext-nacl)#exit
Branch1(config)#line vty 0 15
Branch1(config-line)#access-class TO-Branch1 in
Branch1(config-line)#exit
Branch1(config)#
Branch1(config)#exit

```

FIGURE 3.90 – mise en place server AAA en Branch1

```

Branch2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Branch2(config)#aaa new-model
Branch2(config)#aaa authentication login default group radius local
Branch2(config)#aaa authorization exec default group radius local
Branch2(config)#radius-server host 172.16.20.200
Warning: The CLI will be deprecated soon
'radius-server host 172.16.20.200 '
Please move to 'radius server <name>' CLI.
Branch2(config)#radius-server key VPN_SSIR
Branch2(config)#aaa authentication login local_auth local
Branch2(config)#aaa authorization exec local_auth local
Branch2(config)#privilege exec level 1 configure terminal
Branch2(config)#privilege exec level 10 show running-config
Branch2(config)#privilege exec level 15 write memory
Branch2(config)#radius-server host 172.16.20.200
Branch2(config)#exit
Branch2#wr
*May  4 21:04:04.111: %SYS-5-CONFIG_I: Configured from console by belkis on console
Branch2#wr
Building configuration...
[OK]
Branch2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Branch2(config)#ip access-list extended TO-Branch2
Branch2(config-ext-nacl)#host 172.16.20.100 host 172.16.22.22 range 22 23
Branch2(config-ext-nacl)#host 172.16.20.150 host 172.16.22.22 range 22 23
Branch2(config-ext-nacl)#deny ip any any log
Branch2(config-ext-nacl)#exit
Branch2(config)#line vty 0 15
Branch2(config-line)#access-class TO-Branch2 in
Branch2(config-line)#exit
Branch2(config)#exit

```

FIGURE 3.91 – mise en place server AAA en Branche2

```

SW4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW4(config)#aaa new-model
SW4(config)#aaa authentication login default group radius local
SW4(config)#aaa authorization exec default group radius local
SW4(config)#radius-server host 172.16.20.200
SW4(config)#radius-server key VPN_SSIR
SW4(config)#aaa authentication login local_auth local
SW4(config)#aaa authorization exec local_auth local
SW4(config)#privilege exec level 1 configure terminal
SW4(config)#privilege exec level 10 show running-config
SW4(config)#privilege exec level 15 write memory
SW4(config)#exit
SW4#wr
Building configuration...

*Mar 1 00:20:08.027: %SYS-5-CONFIG_I: Configured from console by belkis on console[OK]
SW4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW4(config)#ip access-list extended T0-Sw4
SW4(config-ext-nacl)#host 172.16.20.100 host 172.16.103.100 range 22 23
SW4(config-ext-nacl)#host 172.16.20.150 host 172.16.103.100 range 22 23
SW4(config-ext-nacl)#deny ip any any log
SW4(config-ext-nacl)#exit
SW4(config)#line vty 0 15
SW4(config-line)#access-class T0-Sw4 in
SW4(config-line)#exit
SW4(config)#privilege exec level 15 write memory
SW4(config)#exit

```

FIGURE 3.92 – mise en place server AAA en SW4

```

SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#aaa new-model
SW1(config)#aaa authentication login default group radius local
SW1(config)#aaa authorization exec default group radius local
SW1(config)#radius-server host 172.16.20.200
SW1(config)#radius-server key VPN_SSIR
SW1(config)#aaa authentication login local_auth local
SW1(config)#aaa authorization exec local_auth local
SW1(config)#privilege exec level 1 configure terminal
SW1(config)#privilege exec level 10 show running-config
SW1(config)#privilege exec level 15 write memory
SW1(config)#exit
SW1#wr
Building configuration...

*Mar 1 00:20:21.743: %SYS-5-CONFIG_I: Configured from console by belkis on console[OK]
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#ip access-list extended T0-Sw1
SW1(config-ext-nacl)#host 172.16.20.100 host 172.16.20.101 range 22 23
SW1(config-ext-nacl)#host 172.16.20.150 host 172.16.20.101 range 22 23
SW1(config-ext-nacl)#deny ip any any log
SW1(config-ext-nacl)#exit
SW1(config)#line vty 0 15
SW1(config-line)#access-class T0-Sw1 in
SW1(config-line)#exit
SW1(config)#exit
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#ip access-list extended T0-Sw1
SW1(config-ext-nacl)#host 172.16.20.100 host 172.16.20.101 range 22 23
SW1(config-ext-nacl)#host 172.16.20.150 host 172.16.20.101 range 22 23
SW1(config-ext-nacl)#
*Mar 1 00:23:26.467: %SYS-5-CONFIG_I: Configured from console by belkis on console[OK]
SW1(config-ext-nacl)#exit
SW1(config)#line vty 0 15
SW1(config-line)#access-class T0-Sw1 in
SW1(config-line)#exit
SW1(config)#exit

```

FIGURE 3.93 – mise en place server AAA en SW1

```

Federateur1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Federateur1(config)#aaa new-model
Federateur1(config)#aaa authentication login default group radius local
Federateur1(config)#aaa authorization exec default group radius local
Federateur1(config)#radius-server host 172.16.20.200
Federateur1(config)#radius-server key VPN_SSIR
Federateur1(config)#aaa authentication login local_auth local
Federateur1(config)#aaa authorization exec local_auth local
Federateur1(config)#privilege exec level 1 configure terminal
Federateur1(config)#privilege exec level 10 show running-config
Federateur1(config)#privilege exec level 15 write memory
Federateur1(config)#exit
Federateur1#wr
Building configuration...

*Mar 1 00:41:15.155: %SYS-5-CONFIG_I: Configured from console by belkis on console[OK]
Federateur1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Federateur1(config)#ip access-list extended T0-Federateur1
Federateur1(config-ext-nacl)#host 172.16.20.100 host 172.16.20.2 range 22 23
Federateur1(config-ext-nacl)#host 172.16.20.150 host 172.16.20.2 range 22 23
Federateur1(config-ext-nacl)#deny ip any any log
Federateur1(config-ext-nacl)#exit
Federateur1(config)#line vty 0 15
Federateur1(config-line)#access-class T0-Federateur1 in
Federateur1(config-line)#exit
Federateur1(config)#exit
Federateur1#wr
Building configuration...

```

FIGURE 3.94 – mise en place server AAA en Federateur1

```

SW3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#aaa new-model
SW3(config)#aaa authentication login default group radius local
SW3(config)#aaa authorization exec default group radius local
SW3(config)#radius-server host 172.16.20.200
SW3(config)#radius-server key VPN_SSIR
SW3(config)#aaa authentication login local_auth local
SW3(config)#aaa authorization exec local_auth local
SW3(config)#privilege exec level 1 configure terminal
SW3(config)#privilege exec level 10 show running-config
SW3(config)#privilege exec level 15 write memory
SW3(config)#exit
SW3#wr
Building configuration...

*Mar 1 00:18:59.695: %SYS-5-CONFIG_I: Configured from console by belkis on console[OK]
SW3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#ip access-list extended T0-SW3
SW3(config-ext-nacl)#host 172.16.20.100 host 172.16.101.100 range 22 23
SW3(config-ext-nacl)#host 172.16.20.150 host 172.16.101.100 range 22 23
SW3(config-ext-nacl)#deny ip any any log
SW3(config-ext-nacl)#exit
SW3(config)#line vty 0 15
SW3(config-line)#access-class T0-SW3 in
SW3(config-line)#exit
SW3(config)#exit
SW3#
*Mar 1 00:21:33.355: %SYS-5-CONFIG_I: Configured from console by belkis on console
SW3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#ip access-list extended T0-SW3
SW3(config-ext-nacl)#host 172.16.20.100 host 172.16.101.100 range 22 23
SW3(config-ext-nacl)#host 172.16.20.150 host 172.16.101.100 range 22 23
SW3(config-ext-nacl)#deny ip any any log
SW3(config-ext-nacl)#exit
SW3(config)#line vty 0 15
SW3(config-line)#access-class T0-SW3 in
SW3(config-line)#exit
SW3(config)#exit

```

FIGURE 3.95 – mise en place server AAA en SW3

3.8 Test et Validation des Services de la solution de sécurité AAA

Avant de procéder aux tests, nous avons configuré le serveur RADIUS pour qu'il puisse se connecter et surveiller les équipements du projet. Cela implique la mise en place des autorisations et des paramètres nécessaires pour établir une communication fiable avec les appareils du réseau. L'image ci-dessous présente le test effectué entre le serveur nagios et le federateur2.

```
Federateur2#ping 172.16.20.200  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.16.20.200, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/24/60 ms  
Federateur2#
```

FIGURE 3.96 – Vérification de la connexion entre radius et le federateur2

On teste la connectivité entre l'admin 1 et le switch 1

```
SW1#ping 172.16.20.100  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.16.20.100, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/230/1040 ms  
SW1#
```

FIGURE 3.97 – Vérification de la connexion entre radius et le federateur2

On teste la connectivité entre l'admin2 et le switch 2

```
SW2#ping 172.16.20.150  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.16.20.150, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/260/1056 ms  
SW2#
```

FIGURE 3.98 – Vérification de la connexion entre radius et le federateur2

3.9 conclusion

Dans ce chapitre, nous avons examiné de manière exhaustive la configuration des services réseau, en répondant aux exigences spécifiques énoncées dans le cahier des charges.

Nous avons traité divers aspects, allant de l'administration des accès à la gestion AAA, en passant par la mise en place d'un serveur de supervision, SNMP, le logging, NTP et IP SLA. Chaque élément a été configuré minutieusement pour garantir la sécurité, la disponibilité et les performances optimales de l'infrastructure réseau. En suivant ces étapes méthodiques, nous avons établi une base solide pour la mise en œuvre et la gestion continue des services réseau de Tekup.

3.10 Conclusion general

En conclusion, la mise en place d'un VPN-MPLS au sein de la maquette du modèle Backbone IP/MPLS représente une étape essentielle dans la conception et la gestion d'une infrastructure réseau moderne et performante. Tout au long de ce processus, nous avons exploré les principaux aspects liés à la technologie VPN-MPLS, ainsi que l'architecture de la solution, en mettant en évidence l'environnement de travail avec des outils tels que GNS3 et VMware.

La technologie VPN-MPLS offre une solution robuste pour répondre aux besoins croissants de connectivité sécurisée, de qualité de service (QoS) et de gestion de trafic dans un environnement réseau complexe. En utilisant GNS3 et VMware, les professionnels des réseaux peuvent simuler, concevoir et tester divers scénarios, assurant ainsi une mise en œuvre efficace de la maquette du modèle Backbone IP/MPLS.