

REPUBLIQUE DU CAMEROUN

REPUBLIC OF CAMEROON

PAIX - TRAVAIL - PATRIE

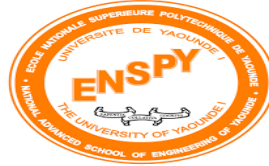
PEACE - WORK - FATHERLAND

UNIVERSITE DE YAOUNDE I

UNIVERSITY OF YAOUNDE I

ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE
YAOUNDE

NATIONAL ADVANCED SCHOOL OF ENGINEERING
YAOUNDE



Projet Réseaux IP 2025

Conception et Implémentation d'un Réseau IP Multi-Sites

Réalisé par:

NOMS ET PRENOMS	MATRICULE
AMOUGOU DANIEL WILLIAM ARSENE	24P801
DJOMGUEM DJOUYOU CHRISTOPHE JUNIOR	22P515
EFFO'O YVAN JUNIOR	21P357
KOUMTOUDJI DANIELLE DORCAS	24P803

Coordonnateur: Dr. MBOUS IKONG

Année Académique 2024-2025

TABLE DES MATIERES

TABLE DES MATIERES	I
LISTE DES FIGURES:	II
LISTE DES ABBREVIATIONS :	III
RESUME DU PROJET :	1
INTRODUCTION	2
I. PRESENTATION GENERALE DU PROJET.....	3
1. contexte.....	3
2. Problématique	3
II. ANALYSE ET CONCEPTION	4
1. choix des équipements	4
2. Plan d'Adressage IP global	5
3. plan d'adressage détaillé	6
4.Choix de la topologie.....	9
4.4.2. Topologie logique	14
5. Routage Inter-Site : OSPF	15
6. Sécurisation du réseau	16
III. RESULTATS ET DISCUSSIONS.....	17
1. Tests de connectivité	17
2. Interprétation	18
3. Limites du projet:.....	20
4. Difficultés rencontrées	20
CONCLUSION	21
PERSPECTIVES:.....	22
REFERENCES BIBLIOGRAPHIQUES.	23

LISTE DES FIGURES:

Figure 1: Router CISCO2911	4
Figure 2: Switch CISCO2960.....	4
Figure 3: Poste de travail (personal computer).....	5
Figure 4: table des VLANs du switch1	10
Figure 5: Table des VLANs du switch2	11
Figure 6: Interconnexion entre les différents équipements	13
Figure 7: table de routage ospf R1.....	15
Figure 8: table de routage ospf R2.....	16
Figure 9: table de routage ospf R3.....	16
Figure 10:Illustration du ping entre pc0 et pc1.....	17
Figure 11: Illustration du ping entre pc0 et pc5.....	18
Figure 12: Illustration du ping entre pc0 et pc10.....	18

LISTE DES ABBREVIATIONS :

- ACL : Access Control List
- AS : Autonomous System
- DHCP : Dynamic Host Configuration Protocol
- IGP : Interior Gateway Protocol
- IP : Internet Protocol
- LSA : Link-State Advertisement
- OSPF : Open Shortest Path First
- PC : Personal Computer
- RJ-45 : Registered Jack type 45
- SPF : Shortest Path First (algorithme de Dijkstra)
- SFP : Small Form-factor Pluggable
- VLAN : Virtual Local Area Network

RESUME DU PROJET :

Ce projet a pour objectif la conception et l'implémentation d'un réseau IP pour une école répartie sur trois sites géographiques au Cameroun, regroupant six départements : Ressources Humaines, Administration, Finance, Télécommunications, Informatique et Production. Afin de répondre aux besoins de segmentation, de sécurité et d'interconnexion, des VLANs ont été configurés pour isoler logiquement chaque département, tandis que le protocole OSPF a été utilisé pour assurer un routage dynamique efficace entre les différents sites. L'adressage IP a été structuré à partir de la plage 192.168.0.0/16, subdivisée en sous-réseaux de taille suffisante pour accueillir les 40 hôtes nécessaires par département, avec une marge pour une future extension. L'ensemble du réseau a été simulé à l'aide de Cisco Packet Tracer, et les résultats des tests de connectivité ont confirmé la fonctionnalité et la robustesse de l'architecture mise en place. Ce travail illustre une mise en pratique des concepts de segmentation réseau, de routage dynamique et de gestion d'adressage, répondant aux exigences fonctionnelles d'un réseau d'entreprise.

INTRODUCTION

Dans le cadre du module « Réseaux IP 1 » de l'année académique 2024-2025, nous avons été amenés à concevoir et implémenter l'infrastructure réseau d'une école répartie sur trois sites géographiques au Cameroun. Cette école regroupe six départements fonctionnels : Ressources Humaines, Administration, Finance, Télécommunications, Informatique et Production. Le principal objectif de ce projet était de mettre en place un réseau structuré, segmenté et interconnecté, permettant une communication fluide, sécurisée et évolutive entre tous les départements. Pour cela, nous avons utilisé des VLANs afin de séparer logiquement les domaines de diffusion, et le protocole OSPF pour assurer le routage dynamique entre les différents sites. L'adressage IP a été soigneusement planifié à partir de la plage 192.168.0.0/16, subdivisée en sous-réseaux adaptés aux besoins de chaque département. L'ensemble de la solution a été implémenté à l'aide de l'outil Cisco Packet Tracer, avec une attention particulière portée sur la cohérence de la topologie, la sécurité des flux et la facilité d'administration.

I. PRESENTATION GENERALE DU PROJET

1. contexte

L'école est divisée en six départements, chacun ayant des fonctions spécifiques : Ressources Humaines (RH), Télécommunications, Informatique, Administration, Production et Finance. Ces départements sont répartis sur trois sites distincts : le premier site regroupe RH, Administration et Finance ; le deuxième site est dédié à Télécommunications et Informatique ; et le troisième site est consacré à la Production. Cette structure nécessite une interconnexion efficace, permettant un échange d'informations fluide et rapide entre les différents départements. L'implémentation d'un réseau efficace est d'autant plus importante dans le contexte actuel, où les entreprises doivent s'adapter aux exigences croissantes en matière de communication et de collaboration. L'utilisation de protocoles de routage dynamique, comme OSPF, est essentielle pour garantir que chaque département puisse communiquer sans faille, tout en optimisant les performances du réseau.

Chaque site sera équipé d'un routeur pour assurer la connectivité inter-sites via le protocole OSPF. Chaque département disposera d'un réseau local indépendant grâce à la mise en place de VLANs spécifiques.

2. Problématique

La problématique centrale de notre projet repose sur la conception d'une architecture réseau qui soit à la fois fonctionnelle et scalable. Comment créer un réseau capable de répondre aux besoins variés des départements tout en assurant la sécurité, la fiabilité et la performance ? En d'autres termes, quels choix techniques et matériels devons-nous faire pour garantir que le réseau supporte efficacement les opérations de l'école, tout en respectant les contraintes budgétaires et techniques ? Cette question fondamentale guidera notre démarche tout au long du projet, en nous amenant à évaluer minutieusement les équipements, l'adressage IP et les configurations nécessaires à une mise en œuvre réussie.

II. ANALYSE ET CONCEPTION

1. choix des équipements

Pour répondre aux besoins de ce projet, les équipements suivants ont été sélectionnés :

- ❖ 3 routeurs Cisco (un par site)



Figure 1: Router CISCO2911

- ❖ 3 switches de niveau 2 (un par site)



Figure 2: Switch CISCO2960

- ❖ Environ 240 postes de travail (environ 40 par département)



Figure 3: Poste de travail (personal computer)

- ❖ Interfaces réseau, câbles Ethernet RJ-45, modules SFP au besoin

Tous les équipements ont été simulés à l'aide de Cisco Packet Tracer.

2. Plan d'Adressage IP global

L'adresse réseau utilisée est 192.168.0.0/16. Pour permettre à chaque département d'héberger au moins 40 hôtes, nous avons opté pour des sous-réseaux en /26, offrant jusqu'à 62 adresses utilisables par sous-réseau. Voici le plan d'adressage défini :

Départements	Vlan	Adresse IP	Masque de sous-réseau	passerelle
RH	Vlan 10	192.168.0.0	255.255.255.192	192.168.0.1
administration	Vlan 20	192.168.0.64	255.255.255.192	192.168.0.65
Finance	Vlan 30	192.168.0.128	255.255.255.192	192.168.0.129

Production	-	192.168.0.192	255.255.255.192	192.168.0.193
Télécommunications	Vlan 40	192.168.1.0	255.255.255.192	192.168.1.1
Informatique	Vlan 50	192.168.1.64	255.255.255.192	192.168.1.65

3. plan d'adressage détaillé

Chaque hôte est configuré avec une adresse IP statique appartenant à son sous-réseau, un masque 255.255.255.192 et une passerelle correspondante et chaque segment entre deux routeurs représente un sous-réseau. Chaque département a été isolé à l'aide de VLANs pour améliorer la sécurité et la gestion du trafic réseau. Les switchs ont été configurés pour permettre l'accès VLAN via les ports en mode access, et des trunks ont été établis entre les switchs et les routeurs pour assurer la communication inter-VLAN via une interface router-on-a-stick.

❖ Exemple de configuration d'un VLAN sur un switch

La syntaxe est la suivante :

- ✧ Enable
- ✧ configure terminal
- ✧ *vlan 10*
- ✧ *name RH*
- ✧ *interface f0/1*
- ✧ *switchport mode access*
- ✧ *switchport access vlan 10*

Cette syntaxe permet de créer un vlan d'ID 10 nommé RH et de configurer l'interface f0/1 du switch en mode accès.

❖ Création des interfaces virtuelles sur un routeur (router-on-a-stick)

CONCEPTION ET IMPLEMENTATION D'UN RESEAU D'ENTREPRISE

La syntaxe est la suivante :

- ✧ Enable
- ✧ configure terminal
- ✧ *interface g0/0*
- ✧ *switchport trunk encapsulation dot1q*
- ✧ *switchport mode trunk*
- ✧ *interface g0/0.10*
- ✧ *encapsulation dot1Q 10*
- ✧ *ip address 192.168.0.1 255.255.255.192*

Cette commande permet de configurer l'interface g0/0 du switch en mode trunk et d'y créer une sous-interface g0/0.10.

Voici un tableau récapitulatif pour chaque équipement :

Équipements	interfaces	passerelle	Adresse IP	Adresse MAC	Masque
PC0	Fa0	192.168.0.1	192.168.0.2	00E0.A3CA.8BED	255.255.255.192
PC1	Fa0	192.168.0.1	192.168.0.3	000A.F3B0.2AB3	255.255.255.192
PC2	Fa0	192.168.0.65	192.168.0.66	0001.9736.4178	255.255.255.192
PC3	Fa0	192.168.0.65	192.168.0.67	0001.C9B1.92CA	255.255.255.192
PC4	Fa0	192.168.0.129	192.168.0.130	0005.5EDB.1632	255.255.255.192
PC5	Fa0	192.168.0.129	192.168.0.131	00D0.9710.1456	255.255.255.192
PC6	Fa0	192.168.0.193	192.168.0.195	0030.F222.C92D	255.255.255.192
PC7	Fa0	192.168.0.193	192.168.0.194	00D0.977D.64A1	255.255.255.192

CONCEPTION ET IMPLEMENTATION D'UN RESEAU D'ENTREPRISE

PC8	Fa0	192.168.1.65	192.168.1.67	0060.2F86.286C	255.255.255.192
PC9	Fa0	192.168.1.65	192.168.1.66	00D0.FF77.960D	255.255.255.192
PC10	Fa0	192.168.1.1	192.168.1.3	0001.9714.3521	255.255.255.192
PC11	Fa0	192.168.1.1	192.168.1.2	00D0.97C9.DBD0	255.255.255.192
R1	G0/0		192.168.1.134	0060.5CA5.1401	255.255.255.252
	G0/1		192.168.1.130	0060.5CA5.1402	255.255.255.252
	G0/2.10		192.168.0.1	0060.5CA5.1403	255.255.255.192
	G0/2.20		192.168.0.65	0060.5CA5.1403	255.255.255.192
	G0/2.30		192.168.0.129	0060.5CA5.1403	255.255.255.192
R2	G0/0		192.168.1.137	000A.4161.A301	255.255.255.252
	G0/1		192.168.1.129	000A.4161.A302	255.255.255.252
	G0/2.40		192.168.1.1	000A.4161.A303	255.255.255.192
	G0/2.50		192.168.1.65	000A.4161.A303	255.255.255.192
R3	G0/0		192.168.1.133	0060.5C77.4D01	255.255.255.252
	G0/1		192.168.1.138	0060.5C77.4D02	255.255.255.252
	G0/2		192.168.0.193	0060.5C77.4D03	255.255.255.192
Switch 1	Fa0/1			0002.4AD8.C101	
	Fa0/2			0002.4AD8.C102	
	Fa0/3			0002.4AD8.C103	
	Fa0/4			0002.4AD8.C104	

CONCEPTION ET IMPLEMENTATION D'UN RESEAU D'ENTREPRISE

	Fa0/5			0002.4AD8.C105	
	Fa0/6			0002.4AD8.C106	
	Fa0/7			0002.4AD8.C107	
Switch 2	Fa0/1			0001.C70E.8501	
	Fa0/2			0001.C70E.8502	
	Fa0/3			0001.C70E.8503	
	Fa0/4			0001.C70E.8504	
	Fa0/5			0001.C70E.8505	
Switch 3	Fa0/1			00E0.F966.7E01	
	Fa0/2			00E0.F966.7E02	
	Fa0/3			00E0.F966.7E03	

4.Choix de la topologie

4.1. Généralités sur les VLANs

Un VLAN (Virtual Local Area Network) est une technologie de segmentation réseau permettant de diviser un réseau physique en plusieurs sous-réseaux logiques indépendants, appelés domaines de diffusion. Cette segmentation logique se fait au niveau des switches (commutateurs), sans modifier l'infrastructure physique. Ainsi, des équipements connectés à un même switch peuvent appartenir à des VLANs différents et ne pourront pas communiquer directement sans passer par un équipement de niveau 3 (comme un routeur ou un switch de couche 3).

L'un des principaux avantages des VLANs est la réduction du domaine de broadcast, ce qui améliore les performances globales du réseau. De plus, les VLANs renforcent la sécurité en isolant les flux de trafic : un poste dans le VLAN « Administration » ne peut

CONCEPTION ET IMPLEMENTATION D'UN RESEAU D'ENTREPRISE

pas, par défaut, communiquer avec un poste du VLAN « Production ». Ils permettent également une meilleure organisation du réseau selon des critères fonctionnels (par département, service, zone géographique, etc.).

Chaque VLAN est identifié par un ID numérique (généralement entre 1 et 4094), et les ports d'un switch peuvent être configurés soit en mode access (pour accueillir un seul VLAN), soit en mode trunk (pour transporter plusieurs VLANs simultanément, en utilisant un tag VLAN selon la norme IEEE 802.1Q).

En résumé, les VLANs sont essentiels dans les réseaux modernes pour assurer la segmentation, la sécurité, l'efficacité et la flexibilité du réseau, tout en simplifiant la gestion et la maintenance des infrastructures complexes.

```
switch1#SHOW VLAN
```

VLAN Name	Status	Ports
-----	-----	-----
1 default	active	Fa0/8, Fa0/9,
Fa0/10, Fa0/11		Fa0/12,
Fa0/13, Fa0/14, Fa0/15		Fa0/16,
Fa0/17, Fa0/18, Fa0/19		Fa0/20,
Fa0/21, Fa0/22, Fa0/23		Fa0/24,
Gig0/1, Gig0/2		
10 vlan10	active	Fa0/2, Fa0/3
20 vlan20	active	Fa0/4, Fa0/5
30 vlan30	active	Fa0/6, Fa0/7
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Figure 4: table des VLANs du switch1

```
switch2#SHOW VLAN
```

VLAN Name	Status	Ports
1 default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
40 vlan40	active	Fa0/2, Fa0/3
50 vlan50	active	Fa0/4, Fa0/5
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Figure 5: Table des VLANs du switch2

4.2. Modes de configuration d'un switch

Dans une infrastructure réseau utilisant des VLANs, les ports d'un switch peuvent fonctionner en différents modes selon leur rôle dans la topologie. Les deux modes les plus courants sont le mode access et le mode trunk.

Le mode access est utilisé pour connecter des équipements finaux tels que des ordinateurs, des imprimantes ou des caméras IP. Dans ce mode, le port du switch est associé à un seul VLAN, et toute trame qui entre ou sort par ce port appartient uniquement à ce VLAN. Ce mode ne nécessite pas de marquage (tag) des trames avec une étiquette VLAN, car l'appareil connecté n'a pas besoin d'être conscient de la segmentation réseau. Par exemple, pour affecter un port au VLAN 10, on utilise la commande `switchport mode access` suivie de `switchport access vlan 10`.

Le mode trunk, quant à lui, est utilisé pour le transport de plusieurs VLANs sur un seul lien physique. Ce mode est essentiel lorsqu'on souhaite faire transiter des trames appartenant à différents VLANs entre deux équipements réseau tels que deux switches ou un switch et un routeur (cas du router-on-a-stick). Pour cela, les trames sont taguées selon la norme IEEE 802.1Q, permettant au périphérique de destination d'identifier le VLAN auquel chaque trame appartient. Un port configuré en mode trunk doit spécifier l'encapsulation utilisée

CONCEPTION ET IMPLEMENTATION D'UN RESEAU D'ENTREPRISE

(souvent dot1q) avec la commande switchport trunk encapsulation dot1q, puis être mis en mode trunk avec switchport mode trunk.

Il existe également des modes dynamiques comme dynamic auto et dynamic desirable, qui permettent une négociation automatique du mode trunk entre deux ports. Toutefois, ces modes peuvent engendrer des comportements imprévus et sont généralement évités dans des environnements professionnels où la configuration manuelle et explicite des trunks est privilégiée.

La configuration correcte des modes de ports est essentielle pour assurer la segmentation logique, la sécurité et la bonne circulation des données dans un réseau à VLANs. Un mauvais paramétrage peut entraîner des problèmes d'accessibilité, de sécurité ou d'instabilité du réseau.

4.3. Comparaison entre une architecture sans VLANs et une architecture avec VLANs

Critère	Sans VLAN	Avec VLAN
Segmentation du réseau	Aucune segmentation logique	Segmentation logique par fonction ou service
Domaine de broadcast	Un seul domaine pour tout le réseau	Un domaine de broadcast par VLAN
Performance réseau	Dégradée en cas de nombreux hôtes (trafic inutile)	Optimisée grâce à la réduction du trafic broadcast
Sécurité	Faible (tous les hôtes peuvent se voir)	Élevée (isolation entre VLANs, contrôle du trafic inter-VLAN)
Évolutivité	Limitée, risque de saturation rapide	Élevée, gestion plus souple de l'ajout de nouveaux services ou sites
Complexité de configuration	Simple à configurer	Configuration plus technique (VLANs, trunks, routage inter-VLAN)

CONCEPTION ET IMPLEMENTATION D'UN RESEAU D'ENTREPRISE

Critère	Sans VLAN	Avec VLAN
Souplesse administrative	Faible (le déplacement physique impacte la connectivité logique)	Élevée (indépendance entre la topologie physique et logique)
Routage inter-départements	Non nécessaire, mais tout est mélangé	Requiert un routeur ou switch L3 pour gérer la communication inter-VLAN

4.4. Topologie

4.4.1. Topologie physique

Il s'agit d'une topologie en étoile étendue avec routage multi-sites, illustrant une segmentation logique par départements. Voici les éléments clés :

Topologie hybride combinant :

- ❖ Topologie en étoile (au niveau local) : chaque site (ou bâtiment) a ses hôtes connectés à un switch central.
- ❖ Topologie en maille au niveau du backbone : les 3 routeurs sont connectés en triangle pour la redondance (possibilité d'utiliser un protocole de routage comme OSPF).

Voici un schéma topologique illustrant ces connexions :

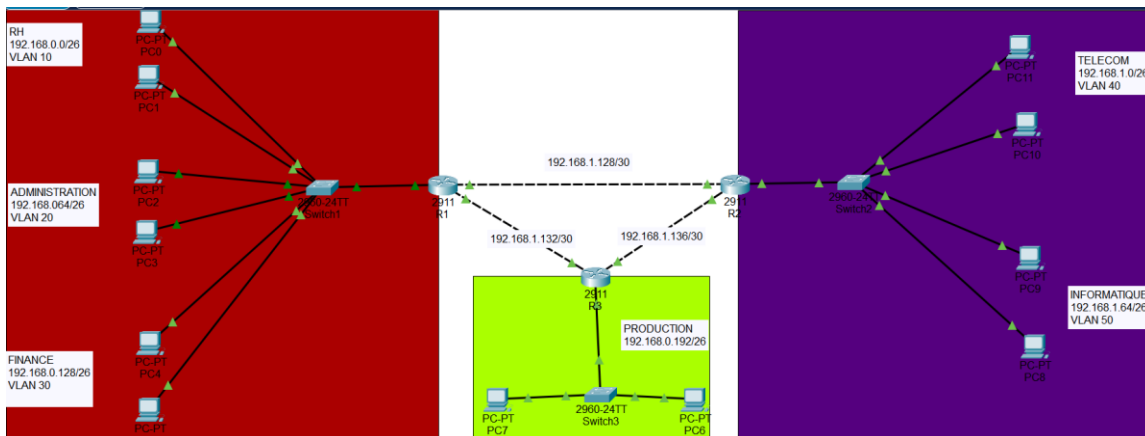


Figure 6: Interconnexion entre les différents équipements

4.4.2. Topologie logique

La topologie logique du réseau présenté repose sur une architecture hiérarchique segmentée en plusieurs VLANs correspondant aux différents départements d'une entreprise répartie sur trois sites distincts. Chaque site est équipé d'un switch central auquel sont connectés les ordinateurs des utilisateurs selon leur service. La segmentation du réseau est réalisée au moyen de VLANs, ce qui permet une séparation logique du trafic pour des raisons de sécurité, de performance et de gestion. Le premier site regroupe les départements RH (VLAN 10, réseau 192.168.0.0/26), Administration (VLAN 20, 192.168.0.64/26) et Finance (VLAN 30, 192.168.0.128/26). Le second site héberge le département Production (réseau 192.168.0.192/26), et le troisième site comprend les départements Télécom (VLAN 40, 192.168.1.0/26) et Informatique (VLAN 50, 192.168.1.64/26). Les VLANs sont configurés sur les switches, avec des liens en mode trunk reliant ces derniers aux routeurs Cisco 2911 afin de permettre le routage inter-VLAN. Trois routeurs (R1, R2, R3) assurent l'interconnexion entre les différents sites et permettent la communication entre tous les VLANs. Les routeurs sont reliés entre eux via des liens point-à-point configurés avec des sous-réseaux en /30 (192.168.1.128/30, 192.168.1.132/30, 192.168.1.136/30) pour optimiser l'adressage IP. Le routage entre les VLANs et les sites est assuré soit de manière statique soit à travers un protocole de routage dynamique tel qu'OSPF. Cette topologie logique permet une isolation efficace du trafic, une meilleure sécurité réseau et une évolutivité facilitée tout en assurant la communication entre tous les services de l'entreprise.

Technologies impliquées :

- ❖ VLANs (802.1Q)
- ❖ Routage inter-VLAN
- ❖ OSPF pour le routage dynamique
- ❖ Subnetting bien appliqué pour l'adressage IP

5. Routage Inter-Site : OSPF

OSPF (Open Shortest Path First) est un protocole de routage dynamique utilisé dans les réseaux IP pour permettre aux routeurs de partager des informations sur les chemins vers les différentes destinations réseau. Il fait partie de la famille des protocoles IGP (Interior Gateway Protocol), utilisés à l'intérieur d'un système autonome (AS). IL a été mis en place dans une zone unique (area 0) pour assurer l'interconnexion des trois sites. Chaque routeur a été configuré pour annoncer ses réseaux VLAN respectifs. Exemple de configuration sur un routeur :

- ✧ *router ospf 1*
- ✧ *router-ID 1*
- ✧ *network 192.168.0.0 0.0.0.63 area 0*

```
R1#show ip route ospf
      192.168.0.0/24 is variably subnetted, 7 subnets, 2 masks
O       192.168.0.192 [110/2] via 192.168.1.133, 00:03:21,
GigabitEthernet0/0
      192.168.1.0/24 is variably subnetted, 7 subnets, 3 masks
O       192.168.1.0 [110/2] via 192.168.1.129, 00:03:21,
GigabitEthernet0/1
O       192.168.1.64 [110/2] via 192.168.1.129, 00:03:21,
GigabitEthernet0/1
O       192.168.1.136 [110/2] via 192.168.1.129, 00:03:21,
GigabitEthernet0/1
                                [110/2] via 192.168.1.133, 00:03:21,
GigabitEthernet0/0
```

Figure 7: table de routage ospf R1

```
R2#show ip route ospf
      192.168.0.0/26 is subnetted, 4 subnets
O       192.168.0.0 [110/2] via 192.168.1.130,
00:4294967242:4294967245, GigabitEthernet0/1
O       192.168.0.64 [110/2] via 192.168.1.130,
00:4294967242:4294967245, GigabitEthernet0/1
O       192.168.0.128 [110/2] via 192.168.1.130,
00:4294967242:4294967245, GigabitEthernet0/1
O       192.168.0.192 [110/2] via 192.168.1.138,
00:4294967242:4294967245, GigabitEthernet0/0
      192.168.1.0/24 is variably subnetted, 9 subnets, 3 masks
O       192.168.1.132 [110/2] via 192.168.1.130, 00:05:16,
GigabitEthernet0/1
                                [110/2] via 192.168.1.138, 00:05:16,
GigabitEthernet0/0
```

Figure 8: table de routage ospf R2

```
R3#show ip route ospf
      192.168.0.0/24 is variably subnetted, 5 subnets, 2 masks
O       192.168.0.0 [110/2] via 192.168.1.134, 00:06:09,
GigabitEthernet0/0
O       192.168.0.64 [110/2] via 192.168.1.134, 00:06:09,
GigabitEthernet0/0
O       192.168.0.128 [110/2] via 192.168.1.134, 00:06:09,
GigabitEthernet0/0
      192.168.1.0/24 is variably subnetted, 7 subnets, 3 masks
O       192.168.1.0 [110/2] via 192.168.1.137,
4294967288:4294967240:4294967272, GigabitEthernet0/1
O       192.168.1.64 [110/2] via 192.168.1.137,
4294967288:4294967240:4294967272, GigabitEthernet0/1
O       192.168.1.128 [110/2] via 192.168.1.134, 00:06:09,
GigabitEthernet0/0
                                [110/2] via 192.168.1.137, 00:06:09,
GigabitEthernet0/1
```

Figure 9: table de routage ospf R3

Cette configuration permet une convergence rapide et une évolutivité facile du réseau.

6. Sécurisation du réseau

La sécurité du réseau consiste à protéger les données, les équipements et les communications contre les accès non autorisés. Dans ce projet, plusieurs mesures de base ont été mises en œuvre. La segmentation via VLANs permet d'isoler les départements, limitant ainsi les risques de propagation d'attaques ou de fuites de données. Les ports inutilisés des switches ont été désactivés ou placés dans un VLAN isolé, et des mots de passe d'accès ont été configurés sur les routeurs et switches pour restreindre la configuration.

CONCEPTION ET IMPLEMENTATION D'UN RESEAU D'ENTREPRISE

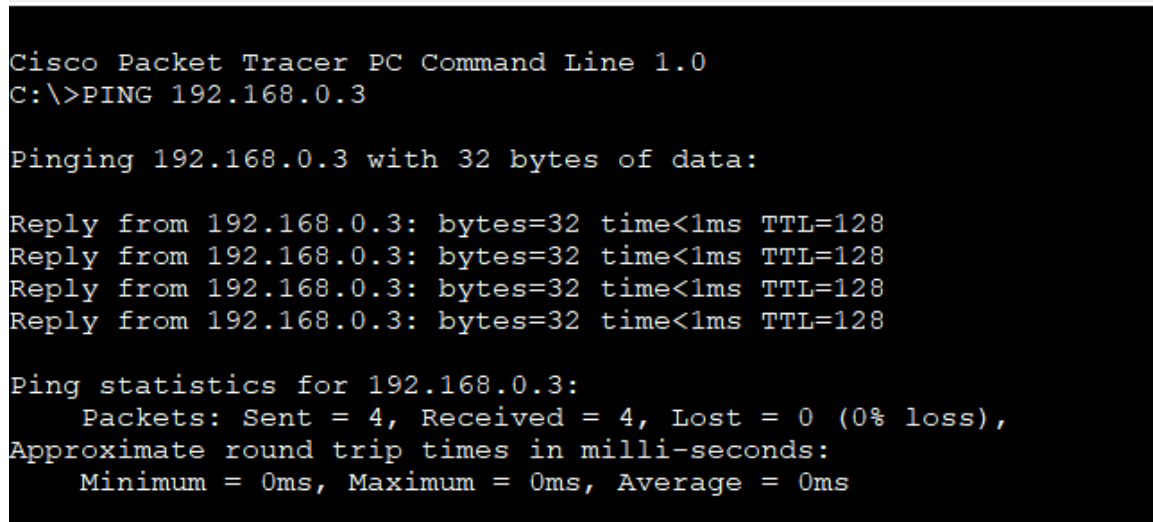
Le protocole OSPF, utilisé pour le routage inter-sites, peut aussi être sécurisé par authentification, bien que cela n'ait pas été activé ici. Pour un déploiement réel, l'ajout de listes de contrôle d'accès (ACL), d'authentification OSPF et de surveillance du trafic serait recommandé.

III. RESULTATS ET DISCUSSIONS

1. Tests de connectivité

Des tests de connectivité ont été réalisés pour vérifier :

- La communication entre deux hôtes du même VLAN: PC0 et PC1



```
Cisco Packet Tracer PC Command Line 1.0
C:\>PING 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 10: Illustration du ping entre pc0 et pc1

- La communication entre deux VLANs différents (inter-VLAN): PC0 et PC5

```
Pinging 192.168.0.130 with 32 bytes of data:

Reply from 192.168.0.130: bytes=32 time<1ms TTL=127
Reply from 192.168.0.130: bytes=32 time<1ms TTL=127
Reply from 192.168.0.130: bytes=32 time<1ms TTL=127
Reply from 192.168.0.130: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 11: Illustration du ping entre pc0 et pc5

- La communication entre deux hôtes sur des sites différents (via OSPF): PC0 et PC10

```
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 12: Illustration du ping entre pc0 et pc10

2. Interprétation

À l'issue de l'implémentation du réseau, plusieurs tests ont été menés afin de vérifier la conformité du système avec les objectifs initiaux. Tout d'abord, la configuration des VLANs a permis d'assurer une séparation logique efficace entre les six départements de l'école. Chaque département disposait de son propre domaine de diffusion, ce qui a considérablement réduit le trafic inutile et amélioré la sécurité intra-réseau.

CONCEPTION ET IMPLEMENTATION D'UN RESEAU D'ENTREPRISE

Le plan d'adressage IP basé sur le subnetting de 192.168.0.0/16 avec des sous-réseaux en /26 s'est révélé suffisant pour couvrir les besoins des 40 hôtes par département, tout en conservant une bonne marge pour l'évolutivité. L'attribution claire des plages IP à chaque département a permis une configuration simple, une gestion aisée et une bonne lisibilité de l'architecture.

L'implémentation du protocole OSPF avec une zone unique (Area 0) entre les trois routeurs a permis d'établir une communication fluide entre les différents sites. Les routeurs ont échangé leurs routes de manière dynamique, assurant ainsi la résilience et l'adaptabilité du réseau. Les tests de connectivité ont montré que les paquets circulaient correctement entre les VLANs (via le router-on-a-stick) et entre les sites (grâce à OSPF), avec un temps de réponse stable.

Les tests de ping entre hôtes du même VLAN, entre différents VLANs, ainsi qu'entre hôtes de sites distants ont tous abouti avec succès, confirmant que le routage inter-VLAN et le routage inter-sites fonctionnaient comme prévu. Cela prouve que l'infrastructure réseau est fonctionnelle, bien segmentée et interconnectée.

Enfin, le projet a mis en évidence l'importance de la configuration rigoureuse des ports (modes access et trunk), du marquage VLAN et du bon paramétrage des interfaces. Quelques difficultés initiales liées aux trunks oubliés ou aux erreurs de masque ont été corrigées grâce à une vérification méthodique et à des commandes de diagnostic (show vlan, show ip route, show ip ospf neighbor, etc.).

En résumé, les résultats obtenus confirment que le réseau conçu est fiable, sécurisé, scalable et répond aux exigences fonctionnelles du cahier des charges. Il constitue une base solide pour une éventuelle extension future ou l'ajout de services réseau supplémentaires.

3. Limites du projet:

- ❖ Simulation uniquement virtuelle : le réseau a été conçu et testé dans Cisco Packet Tracer, sans déploiement réel.
- ❖ Sécurité de base : pas d'authentification OSPF, ni de listes de contrôle d'accès (ACL) avancées.
- ❖ Services limités : aucun service réseau comme DHCP, DNS ou VPN n'a été intégré.
- ❖ Redondance absente : l'architecture ne prévoit pas de liens de secours ni de haute disponibilité.
- ❖ Zone OSPF unique : pas de hiérarchisation en plusieurs zones, ce qui limite l'optimisation.

4. Difficultés rencontrées

- ❖ Configuration des VLANs : Comprendre et appliquer le mode trunk et router-on-a-stick a nécessité plusieurs essais.
- ❖ Plan d'adressage : Éviter les chevauchements d'adresses et adapter le subnetting pour 40 hôtes par département a demandé une grande rigueur.
- ❖ Protocole OSPF : Configurer et vérifier les mises à jour de routage entre les sites a pris du temps.
- ❖ Logiciel de simulation : Certaines limitations de Cisco Packet Tracer, comme l'absence de fonctionnalités avancées, ont impacté la simulation.
- ❖

CONCLUSION

En conclusion, ce projet de conception et d'implémentation d'un réseau pour l'école basée au Cameroun nous a permis d'explorer les défis et les opportunités liés à la création d'une infrastructure réseau moderne. À travers l'allocation stratégique des départements sur trois sites distincts et l'implémentation du routage dynamique OSPF, nous avons pu établir un cadre qui favorise la communication et la collaboration entre les différentes entités.

La réalisation de ce projet a mis en lumière l'importance d'un design réfléchi et adapté aux besoins spécifiques de chaque département. En tenant compte des contraintes techniques et budgétaires, nous avons appris à sélectionner les équipements appropriés et à configurer un réseau robuste et performant.

L'expérience acquise tout au long de ce projet sera précieuse pour notre avenir professionnel, en nous préparant à relever des défis similaires dans le monde réel. Nous sommes confiants que notre solution répondra aux exigences de l'école et contribuera à son efficacité opérationnelle.

PERSPECTIVES:

- ❖ Ajout de services réseau : Intégration future de serveurs DHCP, DNS, ou web internes.
- ❖ Supervision du réseau : Déploiement d'outils de monitoring (ex. : SNMP, NetFlow) pour surveiller la performance en temps réel.
- ❖ Évolutivité : Préparation de l'infrastructure pour accueillir de nouveaux départements ou utilisateurs sans refonte majeure.
- ❖ Migration vers le cloud : Possibilité d'héberger certains services dans un environnement cloud sécurisé.

REFERENCES BIBLIOGRAPHIQUES.

1. Ouvrages:

- ❖ Cisco Networking Academy. Introduction to Networks v7 (ITN). Cisco Press, 2021.
- ❖ RFC 2328. OSPF Version 2. Internet Engineering Task Force (IETF), 1998.
- ❖ Notes de cours "Réseaux IP 1", Année académique 2024–2025.

2. Sites et pages:

- ❖ Cisco Networking Academy — <https://www.netacad.com>
- ❖ Packet Tracer Tutorials — <https://www.packettracernetwork.com>
- ❖ Comment Ça Marche (réseaux informatiques) <https://www.commentcamarche.net>
- ❖ OpenAI (réponses assistées et générées) — <https://chat.openai.com>