**REPUBLIQUE DU SENEGAL**

**Un Peuple – Un But – Une Foi**



\*\*\*\*\*\*\*\*\*\*

**MINISTERE DE L’ENSEIGNEMENT SUPERIEUR DE LA RECHERCHE ET DE L’INNOVATION**

**DIRECTION DE L’ENSEIGNEMENT SUPERIEUR**

\*\*\*\*\*\*\*\*\*\*

**INSTITUT SUPERIEUR DE TECHNOLOGIE INDUSTRIELLE**



**Sicap Sacré-Cœur II BP : 10155**

**Tél : 33 824 28 39 - Fax : 33 824 80 32**

**Email: information@ipg-isti.com Site web**: <http://www.ipg-isti>.com

**MEMOIRE DE FIN DE CYCLE POUR L’OBTENTION DU DIPLÔME D’INGENIEUR TECHNOLOGUE**

**Filière : Informatique de Gestion**

**OPTION : Administration Systèmes, Réseau et Maintenance**

**THEME :**

**ETUDE ET MISE EN PLACE D'UN RESEAU D'ENTREPRISE MULTIZONE SOUS OSPFV3**

Présenté par:

Allaoui MMADI

Encadré par :

M. Mohamadou NIASSE

Instructeur Cisco

***ANNEE ACADEMIQUE 2019-2020***

***ANNEE ACADEMIQUE : 2017-2018***

***ANNEE ACADEMIQUE : 2017-2018***

ETUDE ET MISE EN PLACE D'UN RESEAU D'ENTREPRISE MULTIZONE SOUS OSPFV3

# 

# Dédicaces

Moi Allaoui MMADI, je dédie ce travail estimable :

A ma très chère mers Fatima Ahamada, vous êtes l’exemple de dévouement qui n’a pas cessé de m’encourager et de prier pour moi. Puisse Dieu, le tout puissant, te préserver et t’accorder sante, longue vie et bonheur. A mon père Bacar MMADI, rien au monde ne vaut les efforts et conseils fournis jour et nuit pour la famille. Ce travail est le fruit de vos sacrifices que vous aviez consentis pour ma réussite.

A Madame DIOP, a le corps professoral du groupe IPG/ISTI, à mes frères et mes sœurs, mes oncles et tantes, en particulier a tout ma famille. En reconnaissance de tous les sacrifices consentis par tous et chacun pour me permettre d’atteindre cette étape de ma vie.

A mes oncle, tantes, cousins et cousines affectueuses reconnaissances. Et exceptionnellement à mon oncle Hassani Ahamada qui m’a toujours conseillé et m’encourageais. J’espère que vous trouverez dans ce travail toute ma reconnaissance et ma gratitude.

Je le dédie a tous mes amis et a tous ceux qui de près ou loin ont participé à cette réussite. Qu’ils trouvent à travers ce travail ma sincère reconnaissance.

Enfin je le dédie à tous ceux qui croyaient en moi et aussi à tout ce qui ont compté sur moi mais qui ne sont plus dans ce monde, ALLAH YA RHAM.

Que Dieu vous bénisse tous.

# Remerciements

Je remercie le bon Dieu qui m’a donné la vie et la sante pour pouvoir réaliser ce projet et qu’il me laissera récolte les fruits de ce magnifique travail.

Je tiens particulièrement à remercier notre encadreur Monsieur Mohamadou NIASSE de m’avoir encadré, soutenu et de me guider tout au long de l’étude pour la réalisation. Il a toujours été disponible, à l'écoute de mes nombreuses questions, et s'est toujours intéressé à l'avancée de mes travaux. Les nombreuses discussions que nous avons eues ainsi que ses conseils sont pour beaucoup dans le résultat final de ce travail. Ses capacités d'analyse et son enthousiasme m'ont montré que le monde de la recherche pouvait être un univers passionnant. Pour tout cela merci.

Je remercie également aussi à M. GUEYE, M. DIENG (surveillant) et a Mme DIALLO pour leur disponibilités et leur conseils.

Je remercie également tous les membres du jury pour leur présence, pour leur lecture attention portée à mon mémoire ainsi que pour les remarques qu'ils m'adresseront lors de cette soutenance pour améliorer mon travail.

J’exprime ma gratitude et ma reconnaissance à mes parents pour leur contribution, leurs soutiens et leurs patiences, encore une fois à mon oncle Hassani AHAMADA, à mes tantes Fahamwe ALI, Riyama AHAMADA, Mariama HASSANI. A mes frères et sœurs Eladine MMADI, Elhabib MMADI, Anyssa MMADI et Rayssa MMADI, et sans oublier mes cousins et cousines Fayssoil RADJAB, Hakim MHOUSSINE, Ali MHOUSSINE, Roukia HASSANE, Mouznati MHOUSSINE, et enfin à la famille MHOUDINE : Karima MHOUDINE et son mari Mohamed CHEIKH, Nassifa MHOUDINE, Zainou MHOUDINE, Assadillah MOHAMED, Charafoudine MOHAMED, Charfia MOHAMED et Anturia MOHAMED.

J’adresse mes plus sincères remerciement a tous mes proches et amis d’enfance, et a toutes les connaissances que je n’aurais pas pu citer.

Enfin, mes remerciements à mes collègues : Mohamdoul Amine DIOP, Ibrahim MOUSSA, Soulaimana ABDALLAH, Baye Fall, Serigne SY, Fania BOINA, Farahane SOULE, Miftahou MOHAMED ainsi à toutes les personnes qui auront contribué de près ou de loin à l’élaboration de ce travail ainsi qu’à ma réussite.

# Tableau de matières

[Dédicaces iii](#_Toc101376678)

[Remerciements iv](#_Toc101376679)

[Tableau de matières v](#_Toc101376680)

[Liste des Tableaux x](#_Toc101376681)

[Liste des Figures xi](#_Toc101376682)

[Liste des Abréviations xiii](#_Toc101376683)

[Avant-Propos xv](#_Toc101376684)

[Introduction générale 1](#_Toc101376685)

[PREMIERE PARTIE: CADRE THEORIQUE ET METHODOLOGIQUE 2](#_Toc101376686)

[I. CADRE THEORIQUE 3](#_Toc101376687)

[I.1 Problématique 3](#_Toc101376688)

[I.2 Objectifs 4](#_Toc101376689)

[I.3 Démarche à utiliser 4](#_Toc101376690)

[I.4 Hypothèses de recherche 5](#_Toc101376691)

[II. CADRE METHODOLOGIQUE 5](#_Toc101376692)

[II.1 Cadre de l’étude 5](#_Toc101376693)

[II.2 Délimiterons le champ de l’étude 6](#_Toc101376694)

[II.3 Méthodologies 6](#_Toc101376695)

[II.4 Solutions proposes 7](#_Toc101376696)

[II.5 Les difficultés rencontrés 7](#_Toc101376697)

[DEUXIEME PARTIE: CADRE OPERATIONNEL ET CONCEPTUEL 8](#_Toc101376698)

[III. CADRE OPERATIONNEL 9](#_Toc101376699)

[III.1 Analyse 9](#_Toc101376700)

[III.2 Notion de base 10](#_Toc101376701)

[III.2.1 Notion de base sur les réseaux 10](#_Toc101376702)

[III.2.2 Classification des réseaux informatiques 10](#_Toc101376703)

[III.2.2.1 Classification selon leur étendue géographique 10](#_Toc101376704)

[III.2.2.2 Classification selon les fonctions assumées par les ordinateurs 11](#_Toc101376705)

[III.2.2.3 Classification selon la topologie réseau : 14](#_Toc101376706)

[III.2.2.3.1 La topologie physique : 14](#_Toc101376707)

[III.2.2.3.2 Topologie Logique : 17](#_Toc101376708)

[III.2.3 Protocole IP : 18](#_Toc101376709)

[III.2.4 Le système d’interconnexion 18](#_Toc101376710)

[III.2.4.1 Le matériel d'interconnexion 19](#_Toc101376711)

[III.2.5 Les réseaux étendus 20](#_Toc101376712)

[III.2.5.1 Accès à distance 20](#_Toc101376713)

[III.2.5.2 Accès à internet par Fai 22](#_Toc101376714)

[III.2.5.3 Accès à internet par opérateur téléphonique 22](#_Toc101376715)

[III.2.5.4 Les ressources d’internet 22](#_Toc101376716)

[III.2.6 Les technologies des réseaux étendus 23](#_Toc101376717)

[III.2.7 Généalogie des technologies WAN 24](#_Toc101376718)

[III.2.7.1 Entreprise Internet Access 24](#_Toc101376719)

[III.2.7.2 Options de connectivité WAN privé 24](#_Toc101376720)

[III.3 Adresse IP 24](#_Toc101376721)

[III.3.1 IPv6 25](#_Toc101376722)

[III.3.2 Le principe de bout en bout 25](#_Toc101376723)

[III.3.3 Les autres avantages de l’IPv6 26](#_Toc101376724)

[III.3.4 Les types d’addresses IPv6 26](#_Toc101376725)

[III.4 Routage 27](#_Toc101376726)

[III.4.1 Les protocoles de routage 27](#_Toc101376727)

[III.4.2 Protocole de routage à état de lien 27](#_Toc101376728)

[III.4.3 Protocole à vecteur de distance 28](#_Toc101376729)

[III.4.4 Distances administratives (par défaut) 28](#_Toc101376730)

[III.4.5 Comparatif protocoles de routage 29](#_Toc101376731)

[III.4.6 Comparatif OSPF/RIP 30](#_Toc101376732)

[III.4.7 Les éléments clés d’OSPF 31](#_Toc101376733)

[III.4.8 La sécurité OSPF 31](#_Toc101376734)

[III.4.9 Support d’IPv6 : OSPFv3 33](#_Toc101376735)

[III.5 Zone OSPF 34](#_Toc101376736)

[III.5.1 Zone OSPF 34](#_Toc101376737)

[III.5.2 Opérations et rôles OSPF 34](#_Toc101376738)

[III.5.2.1 IR BR ABR ASBR OSPF 35](#_Toc101376739)

[III.5.2.1.1 OSPF Internal Router (IR) 35](#_Toc101376740)

[III.5.2.1.2 OSPF Backbone Router (BR) 35](#_Toc101376741)

[III.5.2.1.3 OSPF Area Border Router (ABR) 35](#_Toc101376742)

[III.5.2.1.4 OSPF Autonomous System Boundary Router (ASBR) 36](#_Toc101376743)

[III.5.3 Protocole OSPF a zones unique 36](#_Toc101376744)

[III.5.4 Protocole OSPF a zones multiples 37](#_Toc101376745)

[III.5.5 Hiérarchie a deux couches des zones OSPF 38](#_Toc101376746)

[III.5.5.1 Zone de backbone (de transit) 39](#_Toc101376747)

[III.5.5.2 Zone normale (hors backbone) 39](#_Toc101376748)

[III.5.6 Types de routeurs OSPF 39](#_Toc101376749)

[III.5.7 Types de LSA échangées entre les zones 40](#_Toc101376750)

[III.5.7.1 LSA OSPF de type 1 40](#_Toc101376751)

[III.5.7.2 LSA OSPF de type 2 40](#_Toc101376752)

[III.5.7.3 LSA OSPF de type 3 41](#_Toc101376753)

[III.5.7.4 LSA OSPF de type 4 42](#_Toc101376754)

[III.5.7.5 LSA OSPF de type 5 42](#_Toc101376755)

[III.5.8 Tableau de routage 44](#_Toc101376756)

[IV. CADRE CONCEPTUEL 45](#_Toc101376757)

[IV.1 Présentation des équipements utilisés 45](#_Toc101376758)

[IV.2 Nomination des équipements et désignations des interfaces 45](#_Toc101376759)

[IV.2.1 Nominations des équipements 45](#_Toc101376760)

[IV.2.2 Désignations des interfaces 46](#_Toc101376761)

[IV.3 Nomination des Vlans 47](#_Toc101376762)

[IV.4 Plan d’adressage 48](#_Toc101376763)

[IV.5 Nuage Frame Relay 50](#_Toc101376764)

[IV.6 Présentation générale du modèle type 51](#_Toc101376765)

[TROISIEME PARTIE: MISE EN ŒUVRE DE LA SOLUTION 54](#_Toc101376766)

[V. REALISATION 55](#_Toc101376767)

[V.1 Introduction 55](#_Toc101376768)

[V.2 Présentation de simulateur « Cisco Packet Tracer» 55](#_Toc101376769)

[V.3 Méthode configuration des équipements : 56](#_Toc101376770)

[V.4 Maquette de la mise en œuvre 57](#_Toc101376771)

[V.5 Configuration des équipements 57](#_Toc101376772)

[V.6 Configuration des commutateurs 57](#_Toc101376773)

[V.6.1 Configuration de Hostname 58](#_Toc101376774)

[V.6.2 Configuration des vlans 58](#_Toc101376775)

[V.7 Configurations des routeurs 59](#_Toc101376776)

[V.7.1 Configuration de Hostname 60](#_Toc101376777)

[V.7.2 Configuration d’accès à distance (SSH) 60](#_Toc101376778)

[V.7.3 Configuration des interfaces 61](#_Toc101376779)

[V.7.4 Configuration de routage 62](#_Toc101376780)

[V.7.5 Configuration de Frame Relay 63](#_Toc101376781)

[V.8 Configuration des PCs et serveurs 66](#_Toc101376782)

[V.9 Configuration des services 69](#_Toc101376783)

[V.9.1 DNS 69](#_Toc101376784)

[V.9.2 EMAIL 71](#_Toc101376785)

[V.9.3 WEB 73](#_Toc101376786)

[VI. TESTS ET VERIFICATION 75](#_Toc101376787)

[VI.1 Ping 75](#_Toc101376788)

[VI.2 SSH 79](#_Toc101376789)

[VI.3 Email 79](#_Toc101376790)

[VI.4 WEB 83](#_Toc101376791)

[VI.5 Routage 83](#_Toc101376792)

[CONCLUSION GENERALE 85](#_Toc101376793)

[REFERENCES 86](#_Toc101376794)

[BIBLIOGRAPHIE 86](#_Toc101376795)

[WEBGRAPHIE 87](#_Toc101376796)

# Liste des Tableaux

[Tableau 3. 1 18](#_Toc101376797)

[Tableau 3. 2 29](#_Toc101376798)

[Tableau 3. 3 29](#_Toc101376799)

[Tableau 3. 4 40](#_Toc101376800)

[Tableau 3. 5 44](#_Toc101376801)

[Tableau 4. 1 45](#_Toc101376802)

[Tableau 4. 2 45](#_Toc101376803)

[Tableau 4. 3 46](#_Toc101376804)

[Tableau 4. 4 46](#_Toc101376805)

[Tableau 4. 5 47](#_Toc101376806)

[Tableau 4. 6 48](#_Toc101376807)

[Tableau 4. 7 50](#_Toc101376808)

[Tableau 4. 8 50](#_Toc101376809)

# Liste des Figures

[Figure 3. 1 : Réseau Peer to Peer 11](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376810)

[Figure 3. 2 : Réseau Client/serveur 13](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376811)

[Figure 3. 3 : La topologie en bus 14](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376812)

[Figure 3. 4 : La topologie en étoile 15](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376813)

[Figure 3. 5 : La topologie en anneau 16](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376814)

[Figure 3. 6 : La topologie maillée 17](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376815)

[Figure 3. 7 : Concentrateur 19](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376816)

[Figure 3. 8 : commutateur 19](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376817)

[Figure 3. 9 : Routeur 20](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376818)

[Figure 3. 10 : Les types d’adresses IPv6 26](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376819)

[Figure 3. 11 : Opérations et rôles OSPF 35](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376820)

[Figure 3. 12 : zones multiples 38](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376821)

[Figure 3. 13 : Types de routeurs OSPF 39](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376822)

[Figure 3. 14 : LSA OSPF de type 1 40](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376823)

[Figure 3. 15 : LSA OSPF de type 2 41](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376824)

[Figure 3. 16 : LSA OSPF de type 3 41](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376825)

[Figure 3. 17 : LSA OSPF de type 4 42](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376826)

[Figure 3. 18 : LSA OSPF de type 5 43](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376827)

[Figure 4. 1 : Modèle type 52](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376828)

[Figure 5. 1 : Cisco Packet Tracer 55](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376829)

[Figure 5. 2 : CLI 56](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376830)

[Figure 5. 3 : Maquette de la mise en œuvre 57](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376831)

[Figure 5. 4 : Configuration de Hostname 58](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376832)

[Figure 5. 5 : Création vlans 58](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376833)

[Figure 5. 6 : Attribution de Vlans 59](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376834)

[Figure 5. 7 : Configuration de Hostname routeur 60](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376835)

[Figure 5. 8 : Configuration SSH 60](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376836)

[Figure 5. 9 : Configuration login ssh 61](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376837)

[Figure 5. 10 : Configuration des interfaces routeur 61](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376838)

[Figure 5. 11 : Configuration de routage 62](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376839)

[Figure 5. 12 : Configuration de frame Relay 63](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376840)

[Figure 5. 13 : Configuration de serial0 Frame Relay 64](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376841)

[Figure 5. 14 : Configuration interface Frame Relay 64](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376842)

[Figure 5. 15 : Interface Frame Relay 65](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376843)

[Figure 5. 16 : Configuration de diffusion Frame Relay 65](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376844)

[Figure 5. 17 : Configuration des PCs (static) 66](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376845)

[Figure 5. 18 : Configuration des PCs (Auto-config) 67](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376846)

[Figure 5. 19 : Configuration des serveurs (auto-config) 68](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376847)

[Figure 5. 20 : Configuration de DNS 69](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376848)

[Figure 5. 21 : Configuration de nom DNS 70](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376849)

[Figure 5. 22 : Service DNS configuré 70](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376850)

[Figure 5. 23 : Configuration de serveur email 71](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376851)

[Figure 5. 24 : Configuration de serveur email (SMTP) 72](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376852)

[Figure 5. 25 : Configuration de serveur email (SMTP) 72](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376853)

[Figure 5. 26 : Configuration de serveur email (POP3) 73](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376854)

[Figure 5. 27 : Configuration de serveur web 74](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376855)

[Figure 5. 28 : Modification de fichier html 74](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376856)

[Figure 6. 1 : Teste ping routeur et routeur 75](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376857)

[Figure 6. 2 : Test ping PC et routeur 76](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376858)

[Figure 6. 3 : Teste ping PC et VLAN 77](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376859)

[Figure 6. 4 Teste ping Pcs/serveurs (statistique) 77](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376860)

[Figure 6. 5 : Teste ping Pcs/serveurs (auto-config) 78](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376861)

[Figure 6. 6 : Teste ping entre Vlans 78](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376862)

[Figure 6. 7 : Teste ssh 79](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376863)

[Figure 6. 8 : Configuration email PC6 79](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376864)

[Figure 6. 9 : Configuration email PC0 80](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376865)

[Figure 6. 10 : Teste envoi de mail 81](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376866)

[Figure 6. 11 : Envoi mail succès 81](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376867)

[Figure 6. 12 : Reçois mail succès 82](#_Toc101376868)

[Figure 6. 13 : Teste web 83](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376869)

[Figure 6. 14 : Information ospf 83](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376870)

[Figure 6. 15 : Table de routage 84](file:///D:\IG4-Memoire%20ALLAOUI%20MMADI-DIT-2019-2020\Mon%20projet.docx#_Toc101376871)

# Liste des Abréviations

* ATM: Asynchronous Transfer Mode
* ARP: Address Resolution Protocol
* AS: Autonomous System
* ABR: Area Border Router
* ASBR: Autonomous System Boundary Router
* BR: Backbone Router
* DCLI: Data link connection identifier
* DNS: Domain Name System
* EGP: Exterior gateway protocol
* EIGRP: Enhanced Interior Gateway Routing Protocol
* FAI : Fournisseur d'accès à Internet
* HTTP: Hypertext Transfer Protocol
* IPX: Internetwork Packet Exchange/
* IGMP: Internet Group Management Protocol
* ICMP: Internet Control Message Protocol
* IPSEC: Internet Protocol Security
* ISDN : Réseau numérique à intégration de services
* IETF: Internet Engineering Task Force
* IS-IS: Intermediate System - Intermediate System
* [IGRP](https://fr.wikipedia.org/wiki/IGRP) : Interior Gateway Routing Protocol
* IP: Internet Protocol
* ID: IDentifier
* LAN: Local Area Network
* LSA: Link State Advertisement
* MAN: Metropolitan Area Network
* MAC: Media Access Control
* NBMA: Non-broadcast multiple-access network
* OSPF: Open Shortest Path First
* OI: OSPF inter-zone
* OE1 : OSPF externe de type 1
* OE2 : OSPF externe de type 2
* PC:  Personal Computer
* PPP: Point-to-Point Protocol
* POP3: Post Office Protocol
* RARP: Reverse Address Resolution Protocol
* RNIS : Réseau numérique à intégration de services
* RIP: Routing Information Protocol
* RIPv2: Routing Information Protocol
* SMTP: Simple Mail Transfer Protocol
* TLS: Transport Layer Security
* TCP/IP: Transmission Control Protocol / Internet Protocol
* VLSM: Variable Length Subnetwork Mask
* VPN: Virtual Private Network
* VLAN: Virtual Local Area Network
* WAN: Wide Area Network

# Avant-Propos

L’Institut Supérieur de Technologie Industrielle (ISTI) comporte plusieurs départements. Parmi les quel celui de l’Informatique qui forme des étudiants tant sur le plan théorique que pratique. A l’issue de cette formation.

Ils obtiennent:

* Un Diplôme/Brevet de Technicien Supérieur (BAC+2)
* Une licence Professionnelle en Informatique (BAC+3)
* Un Diplôme D’ingénieur Technologue (BAC+4)
* Un master en Informatique (BAC+5)

Au terme d’une formation, l’étudiant(e) devra rédiger un mémoire qu’il devra soutenir en fin d’année pour l’obtention de son Diplôme. C’est dans ce cadre que le thème « *ETUDE ET MISE EN PLACE D'UN RESEAU D'ENTREPRISE MULTIZONE SOUS OSPFV3 »* a été choisi et traite dans ce présent mémoire.

# Introduction générale

L’usage des réseaux a largement progressé ces dernières années, il ne se limite pas au transfert et au traitement de l’information en toute sécurité mais actuellement il participe grandement à la rationalisation des utilisateurs et à l’amélioration des résultats applicatives. De ce fait on a besoin d’un ensemble des moyens et techniques permettant la diffusion d’un message auprès d’un groupe plus ou moins vaste et varie.

A ce niveau, nous allons implémenter un modèle de configuration typique pour un réseau d'entreprise. Ce dernier est un fournisseur de Cloud qui place des équipements chez ces clients. Il garantit l'authentification, l'approbation et le modèle des programmes au sein de l'entreprise. Ces programmes nécessitent un dossier technique abouti et un gain du temps nécessaire lors de la réalisation. Ce modèle considère le déploiement d'un réseau multizone dans un système autonome sous un protocole de routage dynamique en IPV6. La connexion au sein de l'entreprise vers l'extérieur est garantie par une technologie de réseau étendu.

Notre étude s’articule autour de trois extrêmes parties :

La première, repose sur les cadres théorique et méthodologique. Dans cette partie, nous énoncerons la problématique, les objectifs, démarche à suivre et hypothèses de recherches. Nous ferons également état du cadre de l’étude, délimiterons le champ de l’étude, citerons les méthodes utilisés et solutions adaptes.

La seconde partie portera sur le cadre opérationnel et conceptuel. Dans cette partie, nous montrerons l’utilité de certaine technologie, présenterons et développerons de manière élaborée les concepts relatifs au thème.

En dernier ressort nous finissons par la réalisation à travers le simulateur « Cisco Packet Tracer ».

# PREMIERE PARTIE: CADRE THEORIQUE ET METHODOLOGIQUE

Pour mener à bien notre étude, cette première partie sera consacrée aux deux chapitres à savoir le cadre théorique et le cadre méthodologique.

# CADRE THEORIQUE

Ce chapitre permet de développer une problématique et de répondre à nos questions de recherche.

## Problématique

Internet reste jusqu'aujourd'hui la technologie qui nous permet d'être en contact informatique avec une masse d'utilisateurs globale et hétérogène.

En tant qu’entreprise a la fine pointe de la technologie, elle juge bon d’innover et toujours offrir à ses clients de meilleures conditions pour réduire et optimiser le temps d’exécution de leurs taches.

La société développe régulièrement des infrastructures à usage interne ou celle réalisées pour des tiers extérieurs à la structure.

En même temps, elle éprouve un besoin pressant de :

* Partager différentes ressources entre les services et personnes autorisées
* De diminuer le temps de déploiement des serveurs
* De simplifier l’utilisation des technologies existantes.

Face à ce besoin et dans le souci de contribuer à l’amélioration des conditions de travail de ladite société, comment faudra-t-on procéder pour palier à ces problèmes ?

L'un des problèmes majeurs, d'IPv4 est la croissance incontrôlée des tables de routage. Ce phénomène est dû à une mauvaise agrégation des adresses dans les tables. Il faudrait pouvoir router des ensembles de réseaux identifiés par un descripteur unique. Le CIDR "Classless Inter-Domain Routing" apporte une amélioration, mais elle est insuffisante en pratique : les adresses IPv4 sont trop courtes pour permettre une bonne structuration, et surtout il faut assumer le coût du passé avec les adresses déjà allouées.

Pour mieux appréhender notre étude, notre problématique de recherche sera scindée de la manière suivante :

Lors de la mise en place d'un réseau multizone, quels sont les éléments à prendre en compte pour parvenir à une mise en œuvre fiable et à moindre coût ?

Quel intérêt trouve-t-il à mettre en place un réseau multi-zoning tout en cherchant à réaliser le déploiement d'une technologie FAI ?

Toutes ces questions posées sont à la base de notre recherche en nous proposant dans les parties qui suivent des pistes de solutions.

## Objectifs

L'objectif de notre travail est de permettre à notre entreprise d'interconnecter nos multizones sous ospfv3, et d'augmenter considérablement le nombre de routeurs. Avoir un système autonome (AS) au lieu de remodeler le réseau si des zones supplémentaires ou des configurations de câblage sont ajoutées en temps réel.

## Démarche à utiliser

Pour parvenir à la réalisation effective de ce projet, nous passerons par plusieurs étapes :

• Dans un premier temps, nous réaliserons une étude suivie d'une analyse pour connaître les besoins de l'infrastructure réseau ;

• Deuxièmement, nous examinerons des propositions de solutions, puis nous en retiendrons une ;

• Troisièmement, nous passerons à la simulation.

Au terme de cette étude, nous aurons comme résultat un réseau capable de répondre aux exigences en termes de besoins.

## Hypothèses de recherche

Nous essayons autant que possible d'envisager une politique de partage d'informations optimale afin que l'échange de ressources ne soit plus un problème au sein de l'entreprise.

Dans le cadre de notre travail, nous avons pensé qu'il serait judicieux d'intégrer un serveur DNS et des serveurs d’email au système de l'entreprise pour lui permettre :

* Une bonne conservation et recherche aisée des informations en interne et externe ;
* L'échange des données entre les différentes zones ;
* La récupération de l'information en temps réel.

En vue de remédier toujours aux inquiétudes soulevées au travers des questions posées dans les parties précédentes, nous allons mettre en place :

* Un moyen d'échange d'informations qui serait adapté à la gestion efficace et efficiente ;
* Une configuration de type client/serveur pour assurer l'accès sécurisé à l'information. Nous allons configurer un serveur web (http).

# CADRE METHODOLOGIQUE

Dans ce chapitre, nous nous intéresserons au cadre de l’étude, la délimitation du champ de l’étude et les difficultés rencontrées.

## Cadre de l’étude

Le multi-zonage est utilisé pour diviser en plusieurs zones un réseau OSPF de grande taille. Car un nombre excessif de routeurs dans une même zone augmenterait la charge sur le processeur et rendrait la base de données d'états de liens très volumineuse.

Le choix de notre cas pratique est porté sur une entreprise, fournisseur de Cloud qui place des équipements chez ces clients.

D’où le thème : « *ETUDE ET MISE EN PLACE D'UN RESEAU D'ENTREPRISE MULTIZONE SOUS OSPFV3* » afin de faire profiter aux entreprises cette étude et au monde scientifique nos connaissances acquises durant notre parcours des études professionnel.

## Délimiterons le champ de l’étude

Après avoir cadré l'étude, il est important de la délimiter. Dans le cadre de l'espace, notre étude s'effectue au sein de notre entreprise, plus précisément dans sa structure d'administration du réseau multizone. Nous n'allons pas aborder les questions liées à la conception d'un réseau VPN et à toutes les technologies déployées par les FAI, car cela semble être des sujets très complexes. Ainsi, nous avons pensé limiter notre étude par rapport au contenu, au temps et au domaine de recherche.

Dans le temps, notre étude se limite sur la situation du mode de fonctionnement des entreprises des années 2000 jusqu'à ces dernières années et nous ne traiterons que du système d'information existant.

Dans le cadre de la recherche, notre travail est orienté sur ; "réseaux informatique", "protocole de routage dynamique OSPF" et "multizone sous ospfv3".

## Méthodologies

Pour définir les contours de l'expression des besoins de ce système d'information, des méthodes et techniques ont été utilisées en l'occurrence : la méthode dynamique et la méthode ipv6 pour l'infrastructure.

La phase d'analyse permet de lister les résultats attendus, en termes de fonctionnalités, de performance, de maintenance, d'extensibilité, tandis que la phase de conception permet de décrire de manière non ambiguë, le plus souvent en utilisant un langage de modélisation, le fonctionnement du système, afin d'en faciliter la réalisation.

Les techniques suivantes ont été utilisées pour arriver à un résultat fiable : les techniques documentaires pour recueillir des informations relatives à notre sujet, de questionnement par laquelle nous avons eu des informations en échangeant avec certaines profs, la consultation des sites web afin de nous adapter à l'évolution technologique, la consultation des spécialistes pour des éventuels explications claires et précises, et nous, nous servirons aussi de notre expérience professionnelle dans ce domaine.

## Solutions proposes

L'objectif de notre projet est de mettre en place un modèle type de configuration réseau afin de faciliter la préparation et la mise en œuvre de notre projet. Ce modèle est basé sur un réseau étendu multizone, qui sera fourni par une technologie de réseau étendu avec un protocole de routage dynamique. La réalisation de notre projet est conforme. La partie sécurité de réseau ne sera pas traitée car elle ne fait pas partie du cahier des charges de notre projet. Notre modèle type doit être :

* Permettre le fonctionnement même en cas de problèmes matériels.
* Autoriser lors de l'installation de nouveaux équipements la pris en charge
* Transmettre les informations de route par défaut aux voisins.
* Rendre accessible à une communauté d'utilisateurs des programmes, et des données indépendamment de leur localisation.

## Les difficultés rencontrés

Durant le processus des recherches, de rédaction du mémoire ainsi que celui de la réalisation du modèle type, nous avons été confrontés à certaines difficultés, notamment l’émulateur « GNS3 », que je voulais utiliser pour la simulation des réponses du projet. Suit à des problèmes techniques, manque de ressources car l’ordinateur ne pouvez pas supporter.

# DEUXIEME PARTIE: CADRE OPERATIONNEL ET CONCEPTUEL

Dans cette partie, nous présenterons l’analyse, les notions sur le thème, le choix des technologies et des équipements

# CADRE OPERATIONNEL

## Analyse

Le réseau de notre entreprise est basé sur une liaison de type WAN. C'est un réseau basé sur la topologie en mode NBMA.

Cette infrastructure contient cinq zones : la zone 0 est l'endroit où toutes les autres zones sont reliées. Il y a des zones où il y a des serveurs, et les zones reliant les machines.

L’architecture du réseau est élaborée de manière à ce que l’entreprise envoi ces information en temps réel. Au niveau des zones, les équipements terminaux constituent des nœuds auxquels sont relies aux commutateurs.

Ces nœuds principaux sont à leur tour reliés au routeur, ce dernier rattaché à la zone 0, à son tour est connecté au routeur du fournisseur d’accès internet.

Nous avons également des serveurs dans lesquels nous pouvons déployer des services tels que DNS, Email, http…

Pour que le système ait accès aux ressources ou ait un lien avec l'extérieur, il aura besoin de la technologie ISP (FAI).

Nous avons un réseau d'infrastructure interne qui doit être routé.

## Notion de base

### Notion de base sur les réseaux

Le réseau informatique est un ensemble d'équipements informatiques ou systèmes digitaux interconnectés entre eux à travers des médias d’accès en vue de partager des données.

### Classification des réseaux informatiques

La classification se fait par rapport à un critère donné, ainsi nous pouvons classifier les réseaux informatiques de la manière suivante :

* Classification selon leur étendue géographique ;
* Classification selon les fonctions qu’occupent les ordinateurs ;
* Classification selon la topologie

#### Classification selon leur étendue géographique

Selon la taille géographique qu'occupe un réseau, on peut les classer en deux (2) grandes catégories suivantes :

• LAN (Local Area Network);

• MAN (Metropolitan Area Network); WAN (Wide Area Network).

1. **Le réseau LAN (Local Area Network) :**

Les réseaux locaux connectent plusieurs ordinateurs situés sur une zone géographique relativement restreinte, tels qu'un domicile, un bureau, un bâtiment, un campus universitaire. Ils permettent aussi aux entreprises de partager localement des fichiers et des imprimantes de manière efficace et rendent possibles les communications internes.

1. **Le réseau MAN (Metropolitan Area Network)** :

Un réseau métropolitain (MAN) est similaire à un réseau local (LAN) mais s'étend sur une ville entière ou un campus. Les MANs sont formées en connectant plusieurs LANs. Ainsi, les MANs sont plus grandes que les LANs mais plus petits que les réseaux étendus (WAN). Le réseau MAN a une portée de 5 à 50 Kilomètres.

1. **Le réseau WAN (Wide Area Network)**

Contrairement au réseau métropolitain (MAN), le réseau étendu (WAN) offre une couverture bien supérieure. Un WAN connecte des LANs et des MANs, avec un exemple de WAN étant Internet. C’est un réseau qui couvre une zone géographique importante (un pays, voir même un continent).

#### Classification selon les fonctions assumées par les ordinateurs

Du point de vue architecture réseau, nous avons deux grandes catégories de réseaux :

* Réseau POSTE-à-POSTE (Peer to Peer) ;
* Réseaux Clients/Serveurs.

1. **Réseau POSTE-à-POSTE (Peer to Peer) :**

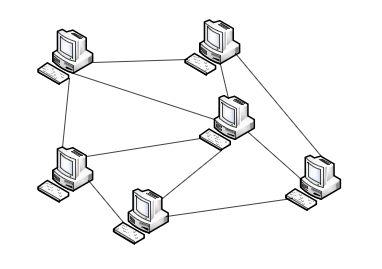
Le réseau peer to peer (P2P) définit un modèle de réseau informatique d'égal à égal entre ordinateurs, qui distribuent et reçoivent des données ou des fichiers. Dans ce type de réseau, chaque client devient lui-même un serveur. Le P2P facilite et accélère les échanges entre plusieurs ordinateurs au sein d'un réseau. En général, c'est un petit réseau de plus ou moins 10 postes, sans administrateur de réseau.

Figure 3. 1 : Réseau Peer to Peer

* Avantages :
* Implémentation moins coûteuse ;
* Ne requiert pas un système d'exploitation de réseau ; Ne requiert pas un administrateur de réseau dédié.
* Inconvénients :
* Moins sécurisé ;
* Chaque utilisateur doit être formé aux tâches d'administration ;
* ▪ Rend donc vite l'administration très complexe.

1. **Réseau Client/serveur :**

Un serveur informatique est un dispositif informatique matériel ou logiciel qui offre des services, a différents clients. Les services les plus courants sont :

* L’accès aux informations ;
* Le courrier électronique ;
* Le commerce électronique ;
* Le stockage en base de données ;
* La gestion de l’authentification et du contrôle d’accès ;
* Le jeu et la mise à disposition de logiciels applicatifs

Un serveur fonction en permanence, répondant automatiquement à des requetés provenant d’autre dispositif informatique (les clients), selon le principe dit client-serveur. Le format des requêtes et des résultats est normalisé, se conforme à des protocoles réseaux et chaque service peut être exploite par tout client qui met en œuvre le protocole propre a service.

Les serveurs sont utilisés par les entreprises, les institutions et les opérateurs de télécommunication, ils sont courants dans les centres de traitement de données et le réseau internet.

Dans une configuration client-serveur, les services de réseau sont placés sur un ordinateur dédié, appelé serveur, qui répond aux requêtes des clients. Ces clients individuels demandent des services et des ressources à un ou des serveurs centralisés.

En règle générale, les ordinateurs de bureau agissent comme des clients, alors qu'un ou plusieurs ordinateurs équipés d'un logiciel dédié, qui sont dotés d'une puissance de traitement et d’une mémoire plus importante assurent la fonction de serveurs. Les serveurs sont conçus pour gérer simultanément les requêtes de nombreux clients.

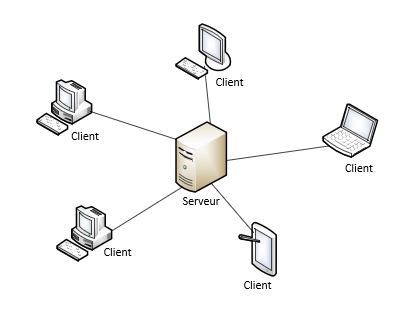


Figure 3. 2 : Réseau Client/serveur

* Avantages :
* Garantit une meilleure sécurité ;
* Plus facile à administrer lorsque le réseau est étendu car l'administration est centralisée ;
* Possibilité de sauvegarder toutes les données dans un emplacement central.
* Inconvénients
* Requiert l'utilisation d'un système d'exploitation de réseau, tel que NT, novelle Netware, Windows server 2003 etc. ...
* Le serveur nécessite du matériel plus puissant, mais coûteux ;
* Requiert un administrateur professionnel ;
* Présente un point unique de défaillance s'il n'y a qu'un seul serveur ; si le serveur est en panne, les données de l'utilisateur risquent de ne plus être disponibles.

#### Classification selon la topologie réseau :

Une topologie de réseau informatique correspond à l'architecture (physique ou logique) de celui-ci, définissant les liaisons entre les équipements du réseau et une hiérarchie éventuelle entre eux.

##### La topologie physique :

Elle définit la façon dont les équipements sont interconnectés et la représentation spatiale du réseau. Ainsi, nous avons :

###### La topologie en bus :

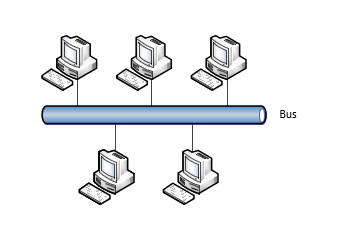


Figure 3. 3 : La topologie en bus

Une topologie de bus est une topologie pour un réseau local (LAN) dans lequel tous les nœuds sont connectés à un seul câble. Le câble auquel les nœuds se connectent, est appelé "épine dorsale" ou "Backbone ". L'extrémité du segment de câble principal doit comporter un terminateur qui absorbe le signal lorsque ce dernier atteint la fin de la ligne ou du câble.

En cas d'absence de terminateur, le signal électrique représentant les données est renvoyé à l'extrémité du câble, ce qui génère une erreur sur le réseau. Si le câble principal (backbone ou épine dorsale) est cassé, le segment entier échoue. Les topologies de bus sont relativement faciles à installer et ne nécessitent pas beaucoup de câblage par rapport aux alternatives.

###### La topologie en étoile :

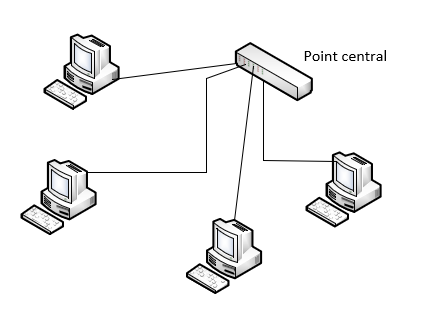
Une topologie en étoile est une topologie pour un réseau local (LAN) dans lequel tous les nœuds sont connectés individuellement à un point de connexion central, comme un concentrateur ou un commutateur. Cette topologie prend plus de câble que celle en bus par exemple. L'avantage est que si un câble tombe en panne, seulement un nœud sera défectueux.

Figure 3. 4 : La topologie en étoile

Tout le trafic émane du centre de l'étoile. Il contrôle tous les nœuds qui lui sont rattachés et est responsable de l'acheminement de tout le trafic vers d'autres nœuds. Le principal avantage d'un réseau en étoile est qu'un nœud défectueux n'affecte pas le reste du réseau. Cependant, ce type de réseau est couteux et dépend du nœud central.

###### La topologie en anneau :

Une topologie en anneau est une topologie pour un réseau local (LAN) dans lequel chaque périphérique a exactement deux voisins à des fins de communication. Comme son nom l'indique, la forme de connexion des hôtes est celle d'un cercle ou d'un anneau. Contrairement à la topologie en bus, aucune de ses extrémités ne nécessite de terminaison. Le mode de transmission des données est différent de celui d’une topologie en étoile ou en bus.

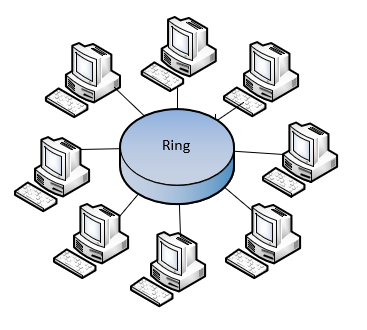
Une trame, appelée jeton, circule autour de l'anneau et s'arrête à chaque nœud. Si un nœud souhaite transmettre des données, il ajoute les données et les informations sur les adresses à la trame. La trame continue de circuler autour de l'anneau jusqu'à ce qu'elle trouve le nœud de destination. Ce dernier récupère alors les données dans la trame.

Figure 3. 5 : La topologie en anneau

L’avantage de cette topologie est qu'il n'y a pas de risque de collisions de paquets de données. Par contre, Une défaillance d'un câble ou d'un appareil rompt la boucle et entraîne la suppression de tout le segment. Un autre inconvénient de cette topologie est que si un appareil est ajouté ou retiré de l'anneau, l'anneau est défectueux et le segment échoue.

###### La topologie maillée :

Dans la topologie maillée, chaque appareil est connecté à tous les autres appareils du réseau via une liaison point à point dédiée. Lorsque nous disons dédié, cela signifie que le lien ne transporte uniquement que des données pour les deux appareils en communication.

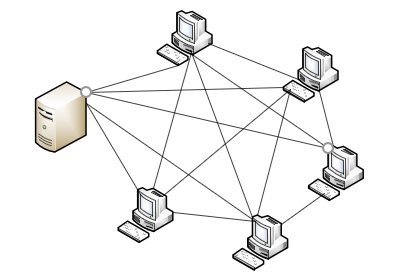


Figure 3. 6 : La topologie maillée

Elle est utilisée sur les réseaux étendus (WAN) pour interconnecter les réseaux locaux, mais également pour les réseaux vitaux comme ceux utilisés par les gouvernements. La topologie maillée est fiable et robuste car la défaillance d'une liaison n'affecte pas les autres liaisons et la communication entre les autres périphériques du réseau. Elle est sécurisée car il existe un lien point à point, donc un accès non autorisé n'est pas possible. La détection des pannes est facile.

Par contre, La quantité de fils nécessaires pour connecter chaque système est fastidieux. Étant donné que chaque périphérique doit être connecté à d'autres périphériques, le nombre de ports d'entrée et sortie (E/S) requis doit être énorme.

##### Topologie Logique :

La topologie logique représente des voies par lesquelles sont transmis les signaux sur le réseau (mode d'accès des données aux supports et de transmission des paquets de données). La topologie logique aide à concevoir l'architecture du réseau. Il comprend des informations sur les nœuds et les commutateurs qui sont placés dans le réseau. Elle permet d'identifier le problème initial dans le réseau afin que ce dernier puisse être mis en œuvre et que les paquets de données puissent être transmis facilement.

### Protocole IP :

IP, signifie « Internet Protocol », « protocole internet » en français. Il représente le protocole réseau le plus répandu. Il permet de découper l’information à transmettre en paquets, de les adresser, de les transporter indépendamment les uns des autres et de recomposer le message initial à l’arrivée. Ce protocole utilise ainsi une technique dite de commutation de paquets. Il apporte, en comparaison à Ipx/Spx et Netbeui, l’adressage en couche 3 qui permet, par exemple, la fonction principale de routage.

Il est souvent associé à un protocole de contrôle de la transmission des données appelé TCP, on parle ainsi du protocole TCP/IP. Cependant, TCP/IP est un ensemble de protocoles dont les plus connus :

Tableau 3. 1

|  |  |  |  |
| --- | --- | --- | --- |
| Protocole | Signification | Couche | Description |
| IP | Internet Protocol | Couche 3 | IP natif |
| ARP | Address Resolution Protocol | Couche 3 | Résolution d’adresse IP en adresse MAC |
| RARP | Reverse Address Resolution Protocol | Couche 3 | Résolution d’adresse MAC en adresse IP |
| ICMP | Internet Control Message Protocol | Couche 3 | Gestion des messages du protocole IP |
| IGMP | Internet Group Management Protocol | Couche 3 | Protocole de gestion de groupe |
| TCP | Transmission Control Protocol | Couche 4 | Transport en mode connecté |
| UDP | User Datagram Protocol | Couche 4 | Transport en mode non connecté |

### Le système d’interconnexion

Vu le nombre important des équipements à gérer et surtout pour faciliter la gestion de l'information. Nous disposons d'un réseau informatique composé d'un réseau câblé et d'un réseau centré. Ce réseau informatique encore embryonnaire utilise un certain nombre d’infrastructures informatiques pour la gestion quotidienne des clients.

#### Le matériel d'interconnexion

Les équipements d'interconnexion représentent le cœur du réseau dans une architecture. S'ils sont mal dimensionnés, ils pourront avoir des effets négatifs sur le trafic du réseau, pouvant entrainer la détérioration de celui-ci.

Les principaux équipements matériels mis en place dans les réseaux locaux sont :

* Les  [concentrateurs](http://www.commentcamarche.net/contents/concentrateurs.php3) (hubs), ce n'est pratiquement qu'un répétiteur. Il amplifie le signal réseau pour pouvoir le renvoyer vers tous PC connectés.



**FOCC. [s. d.]. Un regard plus attentif sur le hub, le switch et le routeur. [illustration].** http://fr.fibresplitter.com/news/a-closer-look-at-hub-switch-and-router-24301083.html

Figure 3. 7 : Concentrateur

* Les  [commutateurs](http://www.commentcamarche.net/contents/commutateurs.php3) (switches) permettent de réduire les [collisions](http://www.ybet.be/hardware/definition_hard2.htm) sur le câblage réseau ;



**SOSPC 24/244. [s. d.]. Commutateur réseau. [illustration].** https://www.sospc2424.ch/site/fr/lexique/-135-commutateur-reseau/

Figure 3. 8 : commutateur

* Les  [routeurs](http://www.commentcamarche.net/contents/routeurs.php3), permettant de relier de nombreux réseaux locaux de telles façons à permettre la circulation de données d'un réseau à un autre de la façon optimale ;



**CISCO. [s. d.]. Routeur Cisco 7201. [illustration].** https://www.cisco.com/c/fr\_ca/support/routers/7201-router/model.html

Figure 3. 9 : Routeur

### Les réseaux étendus

#### Accès à distance

L'accès à distance est une fonction importante des réseaux parce qu'il permet d'accéder aux ressources d'un réseau loin du lieu physique où il se trouve. L'accès à distance caractérise les réseaux étendus.

L'accès à distance peut s'effectuer de deux façons différentes :

* Le contrôle à distance qui consiste à prendre le contrôle d'un ordinateur distant à partir d'un terminal ou d'un autre ordinateur. Bien avant l'essor d'Internet, c'était pratiquement le seul moyen pour accéder à des ressources à distance. Les ordinateurs portables de l'époque n'étaient pas assez puissants pour être en mesure de charger les applications d'un serveur distant, et leur capacité de stockage ne leur permettait pas de stocker des données sur leur station itinérante dont le rôle consistait seulement à afficher l'interface de l'ordinateur distant et à envoyer des commandes. Cette technique nécessite l'installation d'un logiciel sur l'hôte et sur l'invité. De plus, il faut rester connecté pour travailler. Enfin, il faut placer l'ordinateur hôte en situation d'attente pour qu'il puisse recevoir l'appel de l'utilisateur distant. Aujourd'hui, les logiciels de prise de contrôle à distance sont surtout utilisés pour les applications qui exigent beaucoup de ressources, comme les bases de données, et pour les dépannages et les reconfigurations à distance. Il existe plusieurs logiciels permettant la prise de contrôle d'un autre ordinateur à distance :
  + PCANYWARE de Symantec
  + ReachOut de Stac
  + Laplink de Traveling Software
* Le nœud à distance est une technique plus récente qui a vu le jour avec l'essor de l'Internet et des capacités des ordinateurs. Le nœud à distance se connecte au réseau comme tout autre client du réseau, comme s'il était connecté sur place. L'ordinateur distant utilise un protocole de communication comme PPP de la pile TCP/IP pour établir une connexion jusqu'au réseau. Le nœud à distance est un ordinateur comme tous les autres du réseau, il peut accéder à toutes les ressources qui sont partagées sur les réseaux (à condition d'en avoir la permission) et peut effectuer toutes les opérations systèmes sur le réseau (à condition d'en avoir les droits et les privilèges). De plus, le nœud à distance peut télécharger les fichiers dont il a besoin, travailler hors connexion avec les applications installées sur le portable (ou sur un ordinateur de bureau), et enregistrer les fichiers en local. Le nœud à distance s'est largement répandu avec Internet, et beaucoup d'internautes emploient cette technique sans le savoir ; d'autre part de nombreuses entreprises profite de cette technique, avec des liaisons spécialisées, pour rapprocher leurs collaborateurs dans le monde entier, pour améliorer la gestion des différentes versions des documents sur lesquels ils travaillent en même temps, et pour accroître la productivité des groupes de travail (c'est la mondialisation). La connexion à un réseau à distance peut s'effectuer de différentes manières :
  + Par l'intermédiaire d'un Fournisseur d'Accès à Internet (FAI ou Provider en anglais).
  + Par l'intermédiaire de liaisons spécialisées fournies par les opérateurs téléphoniques. Le Provider peut s'occuper des formalités de réservation d'une ligne dédiée (une liaison de type T1 ou 56 K)

#### Accès à internet par Fai

L'accès à Internet s'effectue en général par l'intermédiaire d'un Fournisseur d'Accès à Internet (FAI) aussi appelé un Provider (ISP pour Internet Service Provider en anglais), dans le cadre d'un abonnement forfaitaire à une ligne analogique via un modem par exemple. Le plus souvent la connexion au Fournisseur d'accès à Internet s'effectue avec le protocole PPP et une adresse IP dynamique est allouée par le Provider. Les adresses IP dynamiques ne permettent pas de router soi-même le courrier électronique, ni d'avoir son propre serveur WEB, sauf utilisation de services spéciaux de DNS. Les messages électroniques sont récupérés et envoyés au serveur de messagerie du Provider en utilisant le protocole POP3 ou IMAP 4, et ils sont routés sur le réseau Internet avec le protocole SMTP.

Il est possible de recevoir une adresse IP fixe de la part du Provider, cela coûte plus cher qu'une adresse IP dynamique, mais moins cher qu'une liaison numérique dédiée.

#### Accès à internet par opérateur téléphonique

L'accès à Internet peut également s'effectuer par l'intermédiaire d'un opérateur téléphonique, dans le cadre d'un abonnement permanent à une ligne numérique dédiée via un routeur et un dispositif de connectivité spécialisé par exemple.

Les paquets du réseau interne destinés à Internet sont filtrés et routés par le routeur (en utilisant le protocole EGP par exemple), puis les paquets sont transmis à Internet par le dispositif de connectivité spécialisé. C'est le dispositif de connectivité spécialisé qui assure la liaison avec le réseau Internet. Le plus souvent la connexion à une ligne numérique dédiée permet d'avoir une adresse IP fixe. Une adresse IP fixe permet d'avoir son propre serveur WEB et son propre serveur de messagerie pour router les messages électroniques directement avec SMTP.

#### Les ressources d’internet

L'accès à Internet permet de se connecter aux ressources du réseau :

* Consulter ou créer un site WEB
* Communiqué par e-mail
* Télécharger des fichiers par FTP
* Dialoguer dans les salons CHAT avec IRC
* Échanger des Informations avec USENET (les newsgroups, les listes, les forums de discussion)
* Rechercher des informations avec GOPHER et ARCHIE
* Contrôler un hôte distant avec TELNET

### Les technologies des réseaux étendus

Les technologies WAN sont considérées comme des technologies d’accès au réseau (L2) positionnées physiquement (HDLC, Ethernet) et/ou logiquement (PPP, IP/MPLS, IPSEC, TLS, HTTPS).

Elles sont utilisées pour un accès :

1. Soit, à un WAN privé qui interconnecte des sites distants ;
2. Soit, à l’Internet (WAN public)

Afin d’accéder à des ressources publiques ou afin d’accéder à des ressources privées éventuellement via des tunnels VPN et de manière optionnelle avec des services de sécurité qui assurent des niveaux de confidentialité, d’authentification et d’intégrité.

Les technologies WAN sont diverses dans le monde pour des accès et dans les infrastructures des opérateurs. Les acronyms suivant désignent certaines de ces technologies.

* Metro ethernet
* VSAT
* Cellulaire 3g/4g
* IP MPLS
* T1/E1
* ISDN / RNIS
* xDSL, PPPoE
* Frame-Relay
* Cable DOCSIS
* VPN: IPSEC, DMVPN, VPN TLS

### Généalogie des technologies WAN

Les technologies évoluent depuis bien plus longtemps que les technologies TCP/IP.

Généalogie des technologies WAN depuis le milieu du XXe siècle

#### Entreprise Internet Access

* Broadband PPPoE
* Internet DSL Link
* DOCSIS Cablo-opérateurs
* Wireless ISP

#### Options de connectivité WAN privé

* Metro Ethernet
* IP MPLS
* Les technologies VPN

Ces technologies sont facturées par quantité de données échangées.

## Adresse IP

Avant toute chose, il est important de **comprendre le système qui régit le transfert de paquets de données sur Internet**. Une adresse fixe est attribuée à chaque ordinateur relié au réseau Internet. Pour comparer avec une lettre envoyée à la poste, chaque ordinateur est donc l’équivalent d’une maison, pourvue d’une adresse fixe avec une certaine logique de segmentation (pays, ville, quartier rue…). **Sur Internet, cette adresse fixe est l’IP ou Internet Protocol et elle se présente sous cette forme : X**.X.X.X. Ce standard est alors appelé IPv4, et il existe depuis 1974.

### IPv6

IPv6 qui signifie **« Internet Protocol version 6 »** a été introduit par l’IETF (Internet Engineering Task Force) et il est basé sur la couche réseau (Layer 3) du modèle OSI. Pour un aperçu rapide de la différence entre l’IPv4 et l’IPv6, il suffit de comparer ces deux adresses IP :

* IPv4: 192.168.0.0
* IPv6: 2001:0db8:0000:0000:0210:24ff:ac1f:8001

La différence la plus évidente es**t l’utilisation d’une chaîne de caractères bien plus longue (deux fois plus longue)**. Puis, nous remarquons aussi l’**apparition des lettres résultent de l’introduction de la base hexadécimale**. Plus concrètement, l’IPv4 est codé sur 32 bits tandis que l’IPv6 permet des adresses de 128 bits basées sur une écriture hexadécimale. À titre de comparaison,**l’adressage IPv4 permet de créer environ 4,3 milliards d‘adresses tandis que l’IPv6 peut atteindre jusqu’à plus de 340 sextillions d’adresses** (1 sextillion comporte 36 zéros). Ce nouveau système répond ainsi parfaitement à une demande croissante d’adresse IP dans le monde entier. En effet, le nombre d’appareils connectés à Internet augmentera de manière significative dans les prochaines années.

Une adresse IPv6 comporte exactement 39 caractères, **dont 8 blocs de 4 caractères séparés par des points-virgules**. Il est cependant possible de réduire cette longueur par la suppression de 0 avant les autres chiffres pour chaque bloc et par la concaténation des valeurs nulles qui se suivent.

Ainsi, l’adresse IPv6 suivant :

2001:0db8:0000:0000:0210:24ff:ac1f:8001

Devient :

 2001:db8::210:24ff:ac1f:8001

### Le principe de bout en bout

L’agrandissement de la plage d’adressage d’IP a aussi **permis un grand changement dans la communication sur Internet** : celui de permettre à chaque appareil donné connecté à un réseau d’avoir sa propre adresse IP. Elle est générée manuellement ou sur la base de l’adresse MAC de la carte réseau de l’appareil. **Chaque appareil utilisé sur Internet possède en effet une adresse MAC pour Media Access Protocol et elle est unique**. Constituée d’une séquence de 6 blocs de deux chiffres hexadécimaux, séparés par des deux points, l’adresse MAC est définie, soit par le constructeur de l’appareil, soit par l’administrateur réseau (assez rare et non recommandé).

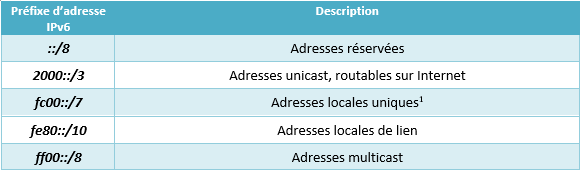
Le principe de bout en bout consiste à profiter de l’intelligence et de la force de calcul des appareils connectés au réseau, plutôt que de**rendre le réseau intelligent et encombrer ainsi son moteur avec des opérations complexes**. À titre d’exemple, dans un cas de chiffrement de bout en bout, les données seront cryptées par l’ordinateur qui envoi et déchiffre directement par l’ordinateur qui reçoit. **Il en résulte une augmentation considérable de la sécurité des données**, si de nos jours ces opérations sont encore réalisées par des serveurs centraux de part et d’autre. Le réseau ne servirait dans ce cas que de relais de transfert.

### Les autres avantages de l’IPv6

Outre le volet sécurité, l’IPv6 offre d’autres avantages. **Nous pouvons par exemple citer la simplification des différentes topologies de réseau et des en-têtes de paquet**, ainsi que le transfert des informations optionnelles pour un routage plus rapide.

Toutefois, l’adressage IPv6 pourrait être utilisé pour **dresser un profil de comportement d’un internaute**, ce qui serait contraire aux éthiques de confidentialité. Ce dernier point devrait faire l’objet de grandes réflexions de la part des autres organismes concernés.

### Les types d’addresses IPv6

Une adresse IPv6 non spécifiée est alors abrégée en ::0.0.0.0 ou de façon canonisée en ::. Tout comme en IPv4, il existe plusieurs catégories d’adresses, chacune jouant des rôles particuliers, décrits au sein des RFC5156, RFC4291 et RFC3587.

**IT-Connect. [s. d.]. IPV6 : Norme et définition. [illustration].** https://www.it-connect.fr/chapitres/ipv6-normes-et-definitions/

Figure 3. 10 : Les types d’adresses IPv6

## Routage

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires.

### Les protocoles de routage

En fonction du nombre de destinataires et de la manière de délivrer le message, on distingue :

* [Unicast](https://fr.wikipedia.org/wiki/Unicast), qui consiste à acheminer les données vers une seule destination déterminée,
* [Broadcast](https://fr.wikipedia.org/wiki/Broadcast_(informatique)) qui consiste à diffuser les données à toutes les machines,
* [Multicast](https://fr.wikipedia.org/wiki/Multicast) qui consiste à délivrer le message à l'ensemble des machines manifestant un intérêt pour un groupe,
* [Anycast](https://fr.wikipedia.org/wiki/Anycast) qui consiste à délivrer les données à n'importe quel membre d'un groupe, mais généralement le plus proche, au sein du réseau.

Pendant un certain temps, plusieurs protocoles ont coexisté pour le routage à l’intérieur d’une organisation. RIP et IGRP/EIGRP ont eu leurs partisans. RIPv2 supprime cet inconvénient mais il n’a pas atteint la même ubiquité, IGRP/EIGRP est un protocole spécifique à Cisco et ne doit donc pas être utilise.

OSPF est désormais mis en œuvre sur toutes les plateformes.

### Protocole de routage à état de lien

Un protocole de routage à état de lien utilise un algorithme (plus) efficace (autre que RIP, comme “Dijkstra” ou “Shortest Path First”). Les routeurs collectent l’ensemble des coûts des liens et construisent de leur point de vue l’arbre de tous les chemins possibles. Les meilleures routes sont alors intégrées à la table de routage.

On parlera de routage hiérarchique (à deux niveaux). On citera OSPF et IS-IS. Ils convergent très rapidement. Les routeurs entretiennent des relations de voisinage maintenues.

Le protocole OSPF a été développé par l’IETF pour répondre au besoin d’un protocole de routage intérieur (IGP, “Internal Gateway Protocol”) dans la pile des protocoles TCP/IP, non-propriétaire et hautement fonctionnel.

### Protocole à vecteur de distance

Un protocole de routage à vecteur de distance est celui qui utilise un algorithme de routage qui additionne les distances pour trouver les meilleures routes (Bellman-Ford). Les routeurs envoient l’entièreté de leur table de routage aux voisins. Ils sont sensibles aux boucles de routage.

Dans ce type de protocole, aucun routeur ne remplit de fonction particulière. On parlera de connaissance “plate” de l’inter-réseau ou de routage non-hiérarchique. Ils convergent lentement.

On citera RIP et IGRP (propriétaire obsolète) comme étant représentatifs. EIGRP est aussi un protocole à vecteur de distance avancé entièrement optimisé par Cisco Systems qui ne présente pas ces désavantages.

### Distances administratives (par défaut)

La distance administrative est le poids administratif d’une route apprise par un protocole de routage. Une distance administrative faible donne la préférence pour une route apprise quelle que soit la méthode de routage. Les distances administratives ont une valeur par défaut. Une route EIGRP sera préférée à une route RIP. Par défaut, une route statique sera préférée à toute autre route dynamique.

Tableau 3. 2

|  |  |
| --- | --- |
| Méthode de routage | Distance administrative |
| Réseau connecté | 0 |
| Route statique | 1 |
| Ext-BGP | 20 |
| Int-EIGRP | 90 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| Int-BGP | 200 |
| Inconnu | 255 |

### Comparatif protocoles de routage

Tableau 3. 3

|  |  |
| --- | --- |
| Vecteur de distance | Etat de lien |
| Algorithme Bellman-Ford (RIP) | Algorithme Dijkstra (OSPF) |
| Facile à configurer | Compétences requises |
| Partage des tables de routage | Partage des liaisons |
| Réseaux plats | Réseaux conçus (design) organisés en areas |
| Convergence plus lente | Convergence rapide, répartition de charge |
| Topologies limitées | Topologies complexes et larges |
| Gourmand en bande passante | Relativement discret |
| Peu consommateur en RAM et CPU | Gourmand en RAM et CPU |
| Mises à jour régulière en Broadcast/Multicast | Mises à jour immédiate |
| Pas de signalisation | Signalisation fiable et en mode connecté |
| RIPv1/RIPv2 et EIGRP | OSPFv2/v3 et IS-IS |

### Comparatif OSPF/RIP

En OSPF, il n’y a pas de limite du nombre de sauts comme en RIP. OSPF étant un protocole de routage à état de lien, chaque routeur possède une connaissance complète des réseaux au sein d’une zone. Aussi, le danger des boucles de routage n’étant a priori plus présent, la limite du nombre de sauts n’est plus nécessaire.

L’utilisation intelligente du “VLSM” (masques à longueur variable) améliore les plans d’adressage. OSPF supporte aussi l’agrégation et la “summarization” de routes.

Il utilise le Multicast pour envoyer ses mises à jour d’état de lien. Aussi, ces mises à jour sont envoyées uniquement lors d’un changement de topologie. On économise la bande passante. Les mises à jour sont seulement incrémentielles et opportunes.

OSPF offre une meilleure convergence que RIP parce que les changements de routage sont propagés instantanément et (non périodiquement) de manière incrémentielle grâce aux relations de voisinage entretenues.

OSPF est meilleur pour la répartition de charge (load balancing). Le choix du meilleur chemin est basé sur le coût (la bande passante inversée). Cette métrique peut être définie manuellement sur les interfaces.

OSPF permet une définition logique des réseaux où les routeurs peuvent être répartis en zones. Cette fonctionnalité empêche une explosion de mises à jour d’états de lien sur l’ensemble du réseau. C’est aussi au niveau des zones que l’on peut agréger les routes et stopper la propagation inutile des informations de sous-réseaux existants.

OSPF autorise l’authentification des informations de routage par l’utilisation de différentes méthodes d’identification avec mots de passe.

Il permet le transfert et l’étiquetage des routes extérieures injectées dans un Système Autonome (AS) pour permettre de les maintenir par des “EGPs” comme BGP.

### Les éléments clés d’OSPF

Les routeurs OSPF entretiennent une relation orientée connexion avec les routeurs d’un même segment physique. Dans la terminologie OSPF, on parlera d’adjacency, en français, d’adjacence ou de contiguïté.

Au lieu d’envoyer des mises à jour entières lors d’un changement topologique, OSPF envoie des mises à jour incrémentielles.

OSPF n’est pas limité par une segmentation dépendante de l’adressage IP ou des sous-réseaux, il utilise la notion d’area (zone) pour désigner un groupe de routeurs.

OSPF supporte entièrement les possibilités du “VLSM” et de la “summarization” manuelle des routes.

Grâce à la possibilité de donner des rôles particuliers aux routeurs, la communication “inter-area/inter-routeurs” est efficace.

Bien qu’OSPF permette une communication “inter-area”, il reste un protocole de routage intérieur (IGP).

### La sécurité OSPF

Quand on parle de sécurité OSPF on parle d'authentification OSPF. Il est important de comprendre comment le mettre en place pour une utilisation future.

L’OSPF est un protocole de routage utilisé par les routeurs qui gèrent le trafic des adresses IP. L'acheminement du trafic via un routeur est un moyen de déplacement le trafic réseau d'un réseau à un autre. OSPF utilise différentes méthodes d'authentification pour rendre le trafic sécurisé. Ces méthodes offrent des garanties, mais le gestionnaire de réseau doit décider qui est le mieux pour leur entreprise. L’authentification OSPF est configurable par lien, ou par aire. Il existe trois types d’authentification OSPF :

* **Authentification Null**

Null est la méthode d'authentification OSPF par défaut. Aussi appelé type zéro, est la condition d'authentification par défaut pour OSPF. Lorsque le trafic ne contient pas d'information particulière, il est l’idéal. Il n'y a pas d'authentification, de sorte que le trafic est grande ouverte. Cela signifie que les paquets de trafic, qui constituent le flux de données OSPF, n'ont aucun élément de cryptage. Signifie trafic ouverte que l'information n'est pas assurée d'être non modifié. Alors que le message est en transit, il est possible pour un pirate d'intervenir et de modifier le trafic. C'est pourquoi il est important pour un gestionnaire de réseau afin de contrôler le trafic et déterminer si elle mérite un autre type d'authentification pour le sécuriser.

* **Authentification clear text**

Authentification en texte clair implique la transmission de données à l'état brut, sans cryptage.

Clear Text (une authentification de type 1) implique la transmission du trafic en utilisant le texte lisible. Le texte créé dans un programme comme bloc-notes est du texte brut. Le texte ne contient pas de caractères spéciaux ou des fonctions. Les caractères gras ou italiques ne font pas partie du texte.

Le niveau de sécurité offert ici est minime. Tout un expéditeur et le besoin de récepteur est un mot de passe commun. Si les deux de trafic est lisible, alors que les pirates peuvent accéder au message, ils doivent passer par les étapes de l'apprentissage de la passe. Ceci, cependant, n'est pas un problème difficile à surmonter.

* **Authentification MD5**

Un peu valeur de hachage 128 est comme une clé et protège les messages.

MD5 (algorithme de hachage un message) est un niveau d'authentification de type deux OSPF. Les gestionnaires de réseaux peuvent créer un niveau élevé de sécurité pour le trafic OSPF à l'aide MD5. C'est la méthode d'authentification OSPF le plus sécurisé disponible aujourd’hui. Il fonctionne en ayant le contenu d'un message calculé pour donner une valeur de hachage (un numéro unique à 128 bits). Cette valeur de hachage est une partie du paquet de transmission. Il y a un mot de passe, mais il ne va pas sur la ligne de réseau.

Le récepteur qui connaît le même mot de passe peut faire passer le message. Avant que le récepteur puisse le lire, un calcul de la valeur de hachage du message reçu se produit. Si les deux valeurs de hachage correspondant, le message reçu est le même que message envoyé. À ce moment, le parti peut lire le message transmis.

La sécurité vient du fait que les deux valeurs de hachage sont 128 bits et doivent correspondre exactement. Si le message reçu n'est pas comme l’original, il a changé pendant la transmission, la partie qui reçoit ne peut pas lire le message, même si la partie destinataire dispose d’un mot de passe. Le mot de passe sera d'aucune utilité.

### Support d’IPv6 : OSPFv3

OSPFv2 et OSPFv3 ont des messages, un algorithme et un fonctionnement très proches.

Parmi d’autres, on notera au moins deux différences entre OSPFv2 et OSPFv3. En OSPFv3 :

* Des messages renommés et nouveaux
* Deux approches de configuration OSPFv3 sous Cisco IOS :
  + Une configuration traditionnelle (uniquement IPv6)
  + L’approche par address-family (supportant le transport en IPv6 des routes IPv4 et des routes IPv6)

## Zone OSPF

### Zone OSPF

Une caractéristique principale d’OSPF est de supporter des inters réseaux très larges grâce au regroupement des routeurs dans des entités logiques appelées areas ou zones.

La communication inter-areas ne laisse passer que les échanges d’information minimale de routage dans le seul objectif de connecter les zones entre elles.

Il en résulte que les efforts de calcul de routes ne s’opèrent qu’au sein d’une même zone.

Les routeurs d’une zone ne sont pas affectés (en calcul) par les changements intervenus dans une autre zone.

Dans un contexte où OSPF demande beaucoup de ressources en CPU et en mémoire, cette notion de conception est très importante.

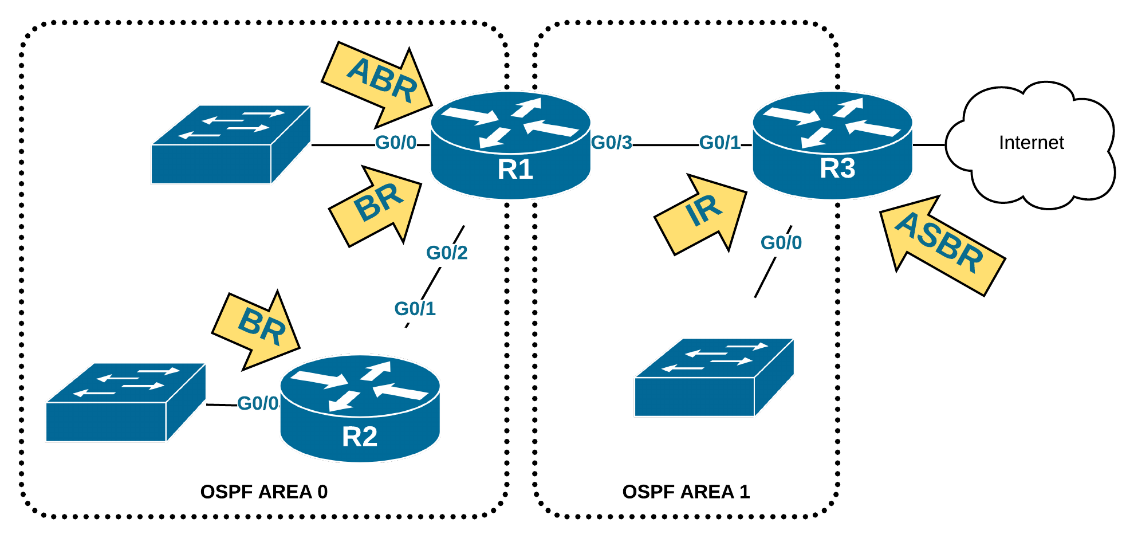
### Opérations et rôles OSPF

Un routeur OSPF peut prendre en charge trois types d’opérations :

* Opérations dans une zone,
* Connexions inter-zones
* Connexions avec d’autres systèmes autonomes (AS).

Un routeur OSPF remplit un rôle et une responsabilité particulière qui dépend de la hiérarchie OSPF établie :

1. Internal Router (IR)
2. Backbone Router (BR)
3. Area Border Router (ABR)
4. Autonomous System Boundary Router (ASBR)



François Goffinet. [10 aout 2020]. Définition au protocole de routage dynamique osfp. [Illustration]. *https://cisco.goffinet.org/ccna/ospf/introduction-au-protocole-routage-dynamique-ospf/*

Figure 3. 11 : Opérations et rôles OSPF

#### IR BR ABR ASBR OSPF

##### **OSPF Internal Router (IR)**

Un IR remplit des fonctions au sein d’une zone (area) uniquement, autre que la zone Backbone.

Sa fonction primordiale est d’entretenir à jour avec tous les réseaux de sa zone (area) sa base de données d’états de lien (link-state database) qui est identique sur chaque IR.

Il renvoie toute information aux autres routeurs de sa zone (area), le routage ou l’inondation (flooding) des autres zones requiert l’intervention d’un Area Border Router (ABR).

##### **OSPF Backbone Router (BR)**

Une des règles de conception OSPF est que chaque zone (area) dans l’inter réseau doit être connectée à une seule zone, la zone 0 ou la backbone area.

Les BR ont une interface connectée à la backbone area.

##### **OSPF Area Border Router (ABR)**

Un ABR connecte au moins deux zones (area) dont l’area 0.

Un ABR possède autant de bases de données d’états de lien qu’il y a d’interfaces connectées à des zones différentes.

Chacune de ces bases de données contient la topologie entière de la zone connectée et peut donc être “summarizée”, c’est-à-dire agrégée en une seule route IP.

Ces informations peuvent être transmises à la zone de backbone pour la distribution.

Un élément clé est qu’un ABR est l’endroit où l’agrégation doit être configurée pour réduire la taille des mises à jour de routage qui doivent être envoyées ailleurs.

Donc quand on parle des capacités d’OSPF de minimiser les mises à jour de routage, on peut directement penser au rôle rempli par les ABR.

##### **OSPF Autonomous System Boundary Router (ASBR)**

OSPF est un IGP (Interior Gateway Protocol), autrement dit il devra être connecté au reste de l’Internet par d’autres AS.

Ce type de routeur fera en quelque sorte office de passerelle vers un ou plusieurs AS. L’échange d’information entre un AS OSPF et d’autres AS est le rôle d’un ASBR.

Les informations qu’il reçoit de l’extérieur seront redistribuées au sein de l’AS OSPF.

### Protocole OSPF a zones unique

Le protocole OSPF à zone unique est utile sur les réseaux de petite taille où la structure des liaisons du routeur n'est pas complexe et où les chemins d'accès aux différentes destinations peuvent être déterminés facilement.

Lorsqu'une zone devient trop grande, il peut y avoir plusieurs types de problèmes, par exemple une :

* Taille excessive de la table de routage : Selon, la taille du réseau, la table de routage peut devenir très importante et provoquer de forte latence sur le routeur.
* on peut aussi avoir une Taille excessive de la base de données d'états de liens : la LSDB couvre l’ensemble de la topologie du réseau, chaque routeur doit conserver une entrée pour chaque réseau de la zone, même si elle ne figure pas dans la table de routage.
* et on peut avoir une Fréquence élevée des calculs de l'algorithme SPF : car dans un réseau de grande taille, les changements sont inévitables ; les routeurs relancent régulièrement l'algorithme SPF pour mettre à jour leurs tables de routage.

Pour une meilleure efficacité et afin d’éviter ces types de problèmes, le protocole OSPF prend en charge le routage hiérarchique à l'aide de zones. Une zone (ou area en anglais) correspond à un groupe de routeurs qui partagent les mêmes informations dans leur base de données d’états de liens.

### Protocole OSPF a zones multiples

Le protocole OSPF à zones multiples est utilisé pour diviser en plusieurs zones un réseau OSPF de grande taille. Car un nombre excessif de routeurs dans une même zone augmenterait la charge sur le processeur et rendrait la base de données d'états de liens très volumineuse. C’est pourquoi il est recommandé de partitionner de manière efficace une zone de grande taille en plusieurs zones plus petites. La zone 0, qui est utilisée avec le protocole OSPF à zone unique, est appelée « zone fédératrice ».

Pour une meilleure efficacité et afin d’éviter ces types de problèmes, le protocole OSPF prend en charge le routage hiérarchique à l'aide de zones. Une zone (ou area en anglais) correspond à un groupe de routeurs qui partagent les mêmes informations dans leur base de données d’états de liens.

Lorsqu'une zone OSPF de grande taille est divisée en zones plus petites, on parle de zones multiples, très utiles sur de grands réseaux afin de réduire la charge de traitement et de stockage.

Par exemple, chaque fois qu'un routeur reçoit de nouvelles informations relatives à une modification topologique dans la zone, notamment l'ajout, la suppression ou la modification d'un lien, le routeur doit relancer l'algorithme SPF, créer une nouvelle arborescence et mettre à jour sa table de routage. L'algorithme SPF est très exigeant en ressource processeur et le temps de calcul dépendra de la taille de la zone. Un nombre excessif de routeurs dans une zone rendrait les bases de données d’état de lien, les LSDB, très volumineuses et augmenterait la charge sur le processeur. Organiser les routeurs en zones, partitionne efficacement une grosse base de données en bases de données plus petites et plus faciles à gérer.

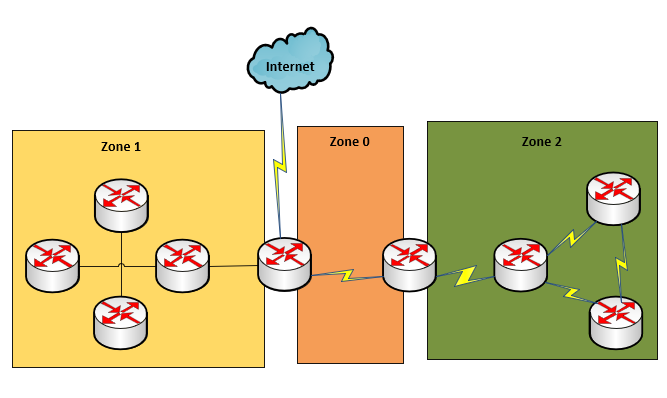


Figure 3. 12 : zones multiples

Comme le montre l’image, le multizone présente plusieurs avantages. :

* la taille des tables de routage est réduite, car les adresses réseau sont abrégées entre les zones. Par exemple, sur l’image, le routeur R1 abrège les routes de la zone 1 vers la zone 0 et le routeur R2 s’occupe des routes de la zone 51 vers la zone 0.
* les mises à jour d’état de liens sont moins surchargées: car il y’a beaucoup moins de routeurs qui s’échange des messages LSA (Link-State Advertissement).
* la Réduction de calculs d’algorithmes SPF : car les changements de topologie ou incident réseau se propagent uniquement à la zone.

### Hiérarchie a deux couches des zones OSPF

Le routage OSPF à zone multiple est mis en œuvre selon une hiérarchie de zones a deux couches :

#### Zone de backbone (de transit)

* Zone dont la fonction principale est de traiter le mouvement rapide et efficace des paquets IP.
* Est connectée à d’autre type de zone OSPF
* Appelée zone 0 toutes les autres zones s’y connectent directement

#### Zone normale (hors backbone)

* Connecte les utilisateurs et les ressources
* Une zone normale n’autorise pas le trafic issu d’une autre zone à utiliser ses liens pour atteindre d’autres zones

### Types de routeurs OSPF

* Routeurs internes
* Toutes les interfaces situées dans la même zone
* LSDB identique
* Routeurs backbone
* Au moins 1 interface dans la zone 0
* Routeurs ABR
* Interfaces situées dans plusieurs zones
* Routeurs ASBR

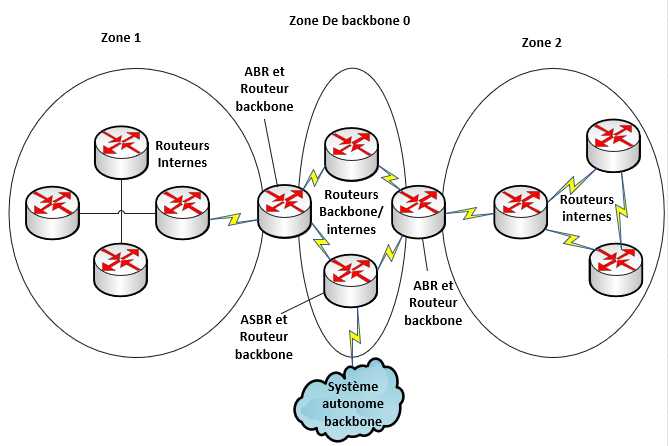


Figure 3. 13 : Types de routeurs OSPF

### Types de LSA échangées entre les zones

**Type courants de LSA OSPF**

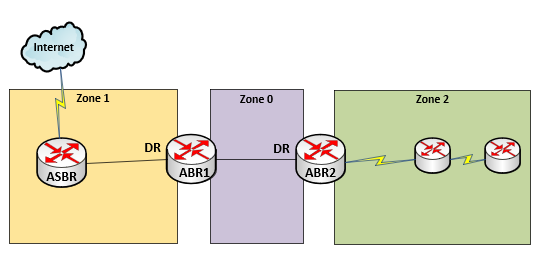
Tableau 3. 4

|  |  |
| --- | --- |
| Type de LSA | Description |
| 1 | LSA de routeur |
| 2 | LSA de routeur |
| 3 & 4 | LSA récapitulatives |
| 5 | LSA externes du système autonome |

#### LSA OSPF de type 1

* Une seule LSA de routeur (type 1) pour chaque routeur d’une zone
* Comprend une liste de liens directement connectes
* Chaque lien est identifié par le préfixe IP attribue au lien et par son type
* Identifiée par l’ID de routeur du routeur émetteur
* Diffusée uniquement dans sa zone sans traverser l’ABR

Figure 3. 14 : LSA OSPF de type 1



**Type 1**

**Type 1**

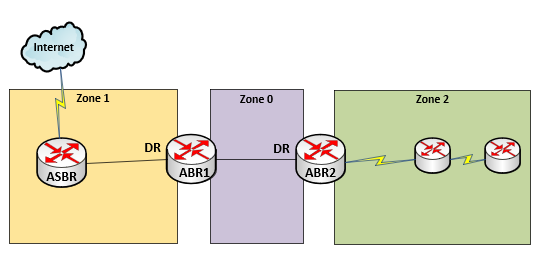
**Type 1**

**Type 1**

#### LSA OSPF de type 2

* Une seule LSA de routeur (type 2) pour chaque diffusion de transit ou de réseau NBMA par zone
* Comprend une liste des routeurs connectes au lien de transit
* Comporte de masque de sous-réseau du lien
* Annoncée par le DR du réseau de diffusion
* Diffusée uniquement dans sa zone sans traverser l’ABR

Figure 3. 15 : LSA OSPF de type 2



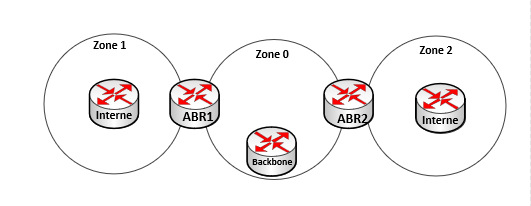
Type 2

Type 2

#### LSA OSPF de type 3

Annonce servant à diffuser des informations de réseau aux zones situées en dehors de la zone émettrice (inter-zone). Décrit le numéro de réseau et le masque du lien.

* Emise par l’ABR de la zone émettrice
* Réémise par les ABR suivants en vue d’une inondation à travers le système autonome
* Par défaut, les routes ne sont pas récapitulées. Des LSA de type 3 sont diffusées par chaque sous-réseau.



**Type 1**

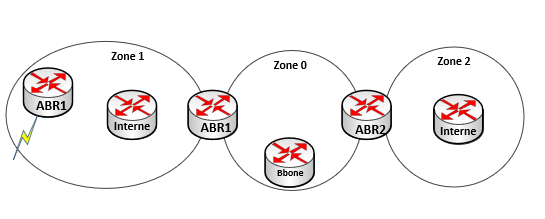
**Type 3**

**Type 3**

Figure 3. 16 : LSA OSPF de type 3

#### LSA OSPF de type 4

* Permet d’annonces un ASBR toutes les autres zones du système autonome
* Emise par l’ABR de la zone émettrice
* Réémise par les ABR suivants en vue d’une inondation a travers le système autonome
* Contient l’ID de routeur de l’ASBR



**Type 4**

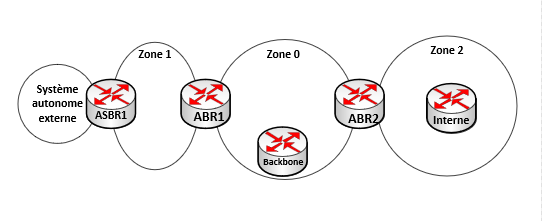
**Type 4**

**Type 1**

Figure 3. 17 : LSA OSPF de type 4

#### LSA OSPF de type 5

* Sert à annoncer les réseaux issus d’autres systèmes autonomes
* Annoncée et détenue par l’ASBR émetteur
* Diffusée à travers tout le système autonome
* Routeur annonceur (ASBR) non modifie à travers tout le système autonome
* LSA de type 4 nécessaire pour localiser l’ASBR
* Par défaut les routeurs ne sont pas récapitulés



**Type 5**

**Type 5**

**Type 1**

Figure 3. 18 : LSA OSPF de type 5

### Tableau de routage

Tableau 3. 5

|  |  |  |
| --- | --- | --- |
|  | **Descripteur de routage** | **Description** |
| O | LSA OSPF interne a une zone (LSA de routeur) et LSA de réseau | * Réseaux situes à l’intérieur de la zone du routeur * Annonces par les LSA de routeur et de réseau |
| OI | OSPF inter-zone (LSA récapitulative) | * Réseaux situes à l’extérieur de la zone du routeur, mais dans le périmètre du système autonome OSPF * Annonces par des LSA récapitulatives |
| OE1 | Routes externes de type 1 | * Réseaux situes à l’extérieur du système autonome du routeur * Annonces par des LSA externes |
| OE2 | Routes externes de type 2 | * Réseaux situes à l’extérieur du système autonome du routeur * Annonces par des LSA externes |

# CADRE CONCEPTUEL

La conception d’architecture du modèle type est l'une des étapes essentielles permettant d'assurer la rapidité et la stabilité d'un réseau. Si un réseau n'est pas conçu adéquatement, de nombreux problèmes imprévus peuvent survenir, ce qui peut entraver son fonctionnement. La conception est véritablement un processus en profondeur. Ce chapitre présente un aperçu du processus la conception du modèle type.

## Présentation des équipements utilisés

Choix des équipements retenu :

Tableau 4. 1

|  |  |
| --- | --- |
| Equipements de modèle type | Type et marque de Switch |
| Switch | Cisco Catalyst 2960 |
| Routeur | Cisco 1941 series |

## Nomination des équipements et désignations des interfaces

### Nominations des équipements

On nomine les équipements par des noms significatifs pour faciliter la conception d’architecture. Les tableaux ci-dessous indiquent les noms des équipements :

Tableau 4. 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A l’entreprise | | | | | |
| Zones | Routeurs | Switch | Serveurs | PCs | Autres |
| Zone 0 | Zone0-R1  Zone0-R2  Zone0-R3 |  |  |  |  |
| Zone 1 | R1 | SW1 | Srv DNS  Srv email SMTP  Srv email POP3  Srv1 |  |  |
| Zone 2 | R2 | SW2 | Srv2  Srv3  Srv4 | PC0 |  |
| Zone 3 | R3 | SW3 |  | PC1  PC2  PC3  PC4 |  |
| Zone 4 | R4 | SW4 |  | PC5  PC6  Laptop de service | Impriment  WIFI |

Tableau 4. 3

|  |
| --- |
| Hors de l’entreprise |
| Rtr-Fr  R-Exterieur  Srv WEB  Cloud Frame Relay |

### Désignations des interfaces

Les interfaces sur les équipements seront comme indique :

Tableau 4. 4

|  |  |  |  |
| --- | --- | --- | --- |
| Equipements | | interfaces | |
| Zone0-R1 | Zone0-R2 | Se0/0/1 | Se0/0/1 |
| Zone0-R1 | Zone0-R3 | Se0/1/1 | Se0/1/1 |
| Zone0-R1 | Rtr-Fr | Se0/0/0 | Se0/0/0 |
| Zone0-R2 | Zone0-R3 | Se0/1/0 | Se0/1/0 |
| Zone0-R2 | R3 | Se0/0/0 | Se0/0/0 |
| Zone0-R2 | R4 | Se0/1/1 | Se0/1/1 |
| Zone0-R3 | R1 | Se0/0/1 | Se0/0/1 |
| Zone0-R3 | R2 | Se0/0/0 | Se0/0/0 |
| R1 | SW1 | GigabitEthernet0/1 | GigabitEthernet0/1 |
| R2 | SW2 | GigabitEthernet0/1 | GigabitEthernet0/1 |
| R3 | SW3 | GigabitEthernet0/1 | GigabitEthernet0/1 |
| R4 | SW4 | GigabitEthernet0/1 | GigabitEthernet0/1 |
| Rtr-Fr | Cloud | Se0/0/1 | Se0 |
| R-Exterieur | Cloud | Se0/0/0 | Se1 |
| R-Exterieur | Srv-WEB | GigabitEthernet0/1 | GigabitEthernet0/1 |
| SW1 | Srv DNS | FastEthernet0/1 | FastEthernet0 |
| SW1 | Srv email SMTP | FastEthernet0/2 | FastEthernet0 |
| SW1 | Srv email POP3 | FastEthernet0/3 | FastEthernet0 |
| SW1 | Srv1 | FastEthernet0/4 | FastEthernet0 |
| SW2 | Srv2 | FastEthernet0/1 | FastEthernet0 |
| SW2 | Srv3 | FastEthernet0/2 | FastEthernet0 |
| SW2 | Srv4 | FastEthernet0/3 | FastEthernet0 |
| SW2 | PC0 | FastEthernet0/4 | FastEthernet0 |
| SW3 | PC1 | FastEthernet0/1 | FastEthernet0 |
| SW3 | PC2 | FastEthernet0/2 | FastEthernet0 |
| SW3 | PC3 | FastEthernet0/10 | FastEthernet0 |
| SW3 | PC4 | FastEthernet0/20 | FastEthernet0 |
| SW4 | PC6 | FastEthernet0/1 | FastEthernet0 |
| SW4 | Impriment | FastEthernet0/2 | FastEthernet0 |
| SW4 | WIFI | FastEthernet0/3 | FastEthernet0 |

## Nomination des Vlans

Les Vlans seront nommées dans la configuration comme suit :

Tableau 4. 5

|  |  |  |
| --- | --- | --- |
| Nom de Vlan | ID Vlan | Adresse |
| Vlan\_service | 10 | 2011:10:10:10::/64 |
| Vlan\_management | 20 | 2011:20:20:20::/64 |

## Plan d’adressage

L’adressage est considéré comme points clés pour la réussite la réalisation.

On utilise dans ce modèle le protocole ipv6, les adresses ont une longueur de 128 bits. Une telle taille d’espace d’adressage permet de subdiviser les adresses disponibles en une hiérarchie de domaines de routage qui reflète la topologie d’Internet. Elle permet également de mapper les adresses des interfaces qui connectent les appareils au réseau. IPv6 contient une fonctionnalité inhérente permettant de résoudre les adresses au niveau le plus bas, c’est-à-dire au niveau de l’interface réseau, et contient également des fonctionnalités de configuration automatique.

Tableau 4. 6

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Périphériques | Interfaces | Adresse ipv6 | Longueur du préfixe | Passerelle par défaut |
| Zone0-R1 | Se0/0/0 | 2001:DB8:CAFE:200::1 | 64 | N/A |
| Se0/0/1 | 2001:DB8:CAFE:4::2 | 64 | N/A |
| Se0/1/1 | 2001:DB8:CAFE:3::1 | 64 | N/A |
| Zone0-R2 | Se0/0/0 | 2001:DB8:CAFE:7::2 | 64 | N/A |
| Se0/0/1 | 2001:DB8:CAFE:4::1 | 64 | N/A |
| Se0/1/0 | 2001:DB8:CAFE:5::1 | 64 | N/A |
| Se0/1/1 | 2001:DB8:CAFE:8::2 | 64 | N/A |
| Zone0-R3 | Se0/0/0 | 2001:DB8:CAFE:6::2 | 64 | N/A |
| Se0/0/1 | 2001:DB8:CAFE:2::2 | 64 | N/A |
| Se0/1/0 | 2001:DB8:CAFE:5::2 | 64 | N/A |
| Se0/1/1 | 2001:DB8:CAFE:3::2 | 64 | N/A |
| R1 | Se0/0/1 | 2001:DB8:CAFE:2::1 | 64 | N/A |
| Gig0/1 | 2001:DB8:CAFE:1::1 | 64 | N/A |
| R2 | Se0/0/0 | 2001:DB8:CAFE:6::1 | 64 | N/A |
| Gig0/1 | 2001:DB8:CAFE:9::1 | 64 | N/A |
| R3 | Se0/0/0 | 2001:DB8:CAFE:7::1 | 64 | N/A |
| Gig0/1.10 | 2011:10:10:10::1 | 64 | N/A |
| Gig0/1.20 | 2011:20:20:20::1 | 64 | N/A |
| R4 | Se0/1/1 | 2001:DB8:CAFE:20::1 | 64 | N/A |
| Gig0/1 | 2001:DB8:CAFE:8::1 | 64 | N/A |
| Rtr-Fr | Se0/0/0 | 2001:DB8:CAFE:200::2 | 64 | N/A |
| Se0/0/1 | 2001:DB8:CAFE:100::2 | 64 | N/A |
| R-Exterieur | Se0/0/0 | 2001:DB8:CAFE:100::1 | 64 | N/A |
| Gig0/1 | 2001:DB8:99:1::1 | 64 | N/A |
| Srv-WEB | Carte réseau | 2001:DB8:99:1::10 | 64 | 2001:DB8:99:1::1 |
| Srv DNS | Carte réseau | 2001:DB8:CAFE:1::2 | 64 | 2001:DB8:CAFE:1::1 |
| Srv email SMTP | Carte réseau | 2001:DB8:CAFE:1::3 | 64 | 2001:DB8:CAFE:1::1 |
| Srv email POP3 | Carte réseau | 2001:DB8:CAFE:1::4 | 64 | 2001:DB8:CAFE:1::1 |
| Srv1 | Carte réseau | 2001:DB8:CAFE:1::5 | 64 | 2001:DB8:CAFE:1::1 |
| Srv2 | Carte réseau | Auto-config | 64 |  |
| Srv3 | Carte réseau | Auto-config | 64 |  |
| Srv4 | Carte réseau | Auto-config | 64 |  |
| PC0 | Carte réseau | 2001:DB8:CAFE:9::5 | 64 | 2001:DB8:CAFE:9::1 |
| PC1 | VLAN 10 | 2011:10:10:10::2 | 64 | 2011:10:10:10::1 |
| PC2 | VLAN 20 | 2011:20:20:20::2 | 64 | 2011:20:20:20::1 |
| PC3 | VLAN 10 | 2011:10:10:10::3 | 64 | 2011:10:10:10::1 |
| PC4 | VLAN 20 | 2011:20:20:20::3 | 64 | 2011:20:20:20::1 |
| PC5 | Carte réseau | Auto-config | 64 |  |
| PC6 | Carte réseau | 2001:DB8:CAFE:20::2 | 64 | 2001:DB8:CAFE:20::2 |
| Impriment | Carte réseau | Auto-config |  |  |

## Nuage Frame Relay

Afin de créer un PVC (circuit virtuel permanent) entre le routeur FR et le routeur extérieur, on définit deux DLCI qui seront répartis sur les interfaces des deux routeurs.

Tableau 4. 7

|  |  |  |
| --- | --- | --- |
| Routeur | Interface | DLCI |
| Rte-Fr | se0/0/1 | 102 |
| R-Exterieur | e0/0/0 | 202 |

L’adresse 2001:DB8:CAFE:100::/64 est utilisée pour l’administration de Frame Relay .

Tableau 4. 8

|  |  |  |  |
| --- | --- | --- | --- |
| Routeur | Interface | Adresse IP | DLCI |
| Rtr-FR | Frame Relay serial 0/0/1 | 2001:DB8:CAFE:100::2 | 102 |
| R-Exterieur | Frame Relay serial 0/0/0 | 2001:DB8:CAFE:100::1 | 202 |

## Présentation générale du modèle type

Le modèle type doit fournir un design physique compose de différentes zones :

* La zone 0 qui est aussi appelle zone fédératrice. Toutes les autres zones doivent se connecter sur cette zone.
* Des routeurs qui relient les zones qu’on appelle les routeurs ABR (Area Border Router).

Certains périphériques sont configurés en auto-config et d'autres en statique. Cette architecture complètement modulaire offre une approche évolutive avec une simplicité d’exploitation, de gestion et de maintenance au système. Cette architecture respecte la division en quatre zones plus la zone 0 et offre une séparation aussi bien logique que physique.

Le schéma ci-dessous est un schéma synoptique du modèle type.

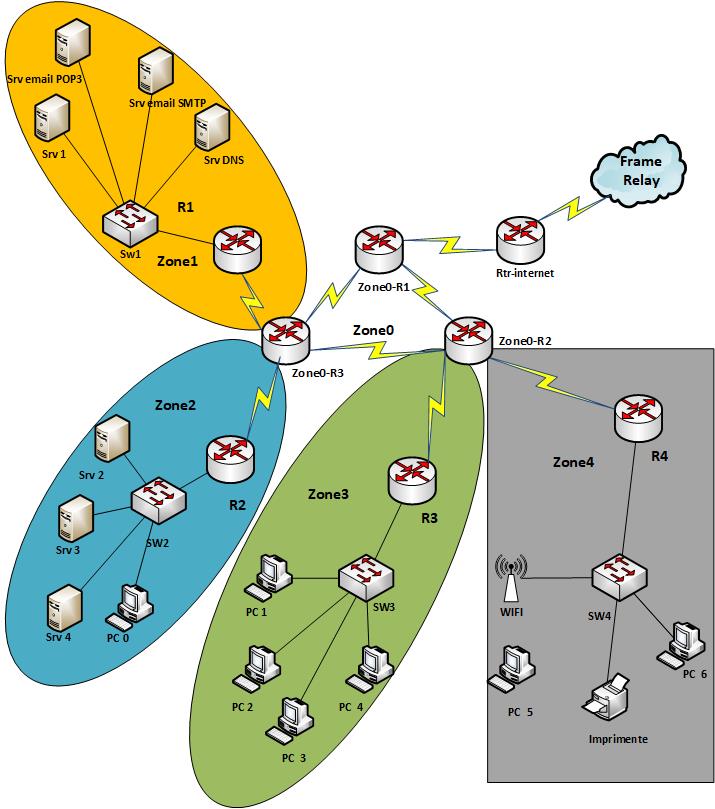


Figure 2. 1 : Modèle type

Figure 4. 1 : Modèle type

Le modèle type est composé par les zones suivant :

* Zone 0 (backbone): composé de trois routeur lie l'un et l'autre. Qui sont reliés aux routeurs des différentes zones ainsi qu'au routeur Rtr-Fr connecté au switch périphérique au cloud.
* Zone 1, Zone 2, Zone 3 et Zone 4 : composé de quatre routeurs (R1, R2, R3 et R4) reliés à quatre commutateurs (SW1, SW2, SW3 et SW4) et de périphériques reliés aux différents commutateurs.
* Module réseau étendu (WAN) : nous avons la technologie de Frame Relay (FR)

# TROISIEME PARTIE: MISE EN ŒUVRE DE LA SOLUTION

Dans cette partie nous mettrons en place le modèle type et vérifierons nos hypothèses.

# REALISATION

## Introduction

Dans cette partie, qui est considère comme la plus important on essaye de configurer notre modèle type en utilisant le simulateur « Cisco Packet Tracer ».

## Présentation de simulateur « Cisco Packet Tracer»

Packet Tracer est un simulateur de matériel réseau Cisco ([routeurs](https://fr.wikipedia.org/wiki/Routeurs), [commutateurs](https://fr.wikipedia.org/wiki/Commutateur_r%C3%A9seau)..). Cet outil est créé par [Cisco Systems](https://fr.wikipedia.org/wiki/Cisco_Systems) qui le fournit gratuitement aux centres de formation, étudiants et diplômés participant, ou ayant participé, aux programmes de formation Cisco. Le but de Packet Tracer est d'offrir aux élèves et aux professeurs un outil permettant d'apprendre les principes du réseau, tout en acquérant des compétences aux technologies spécifiques de Cisco. Il peut être utilisé pour s’entraîner, se former, préparer les examens de certification Cisco, mais également pour de la [simulation réseau](https://fr.wikipedia.org/wiki/Simulation_r%C3%A9seau).

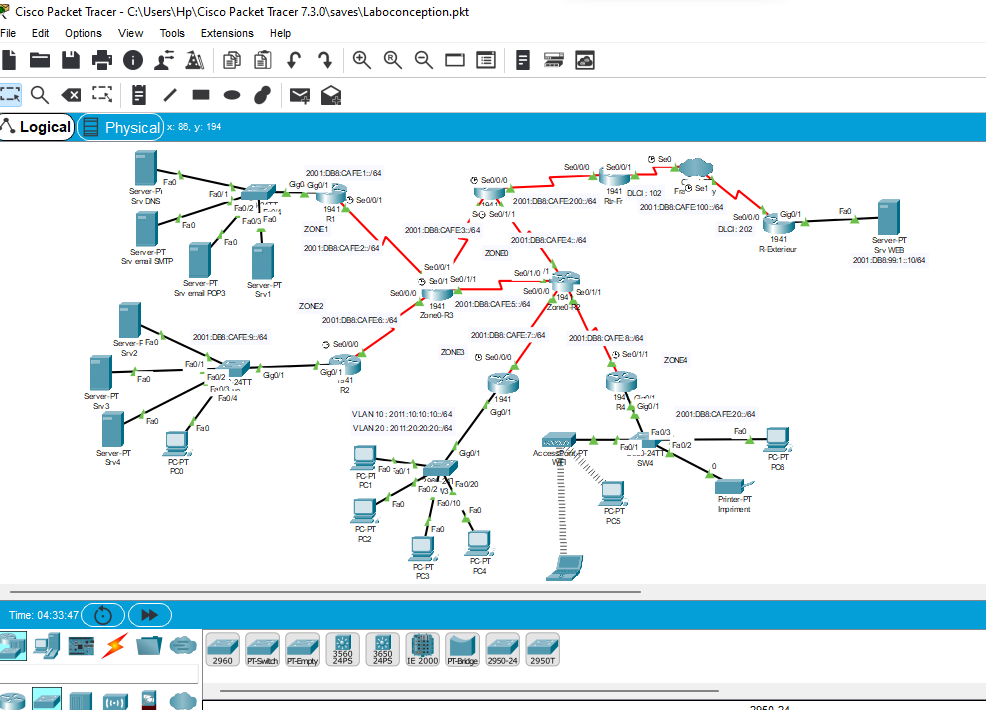


Figure 5. 1 : Cisco Packet Tracer

## Méthode configuration des équipements :

Pour configurer les équipements du modèle on utilise le CLI (Command Language Interface).

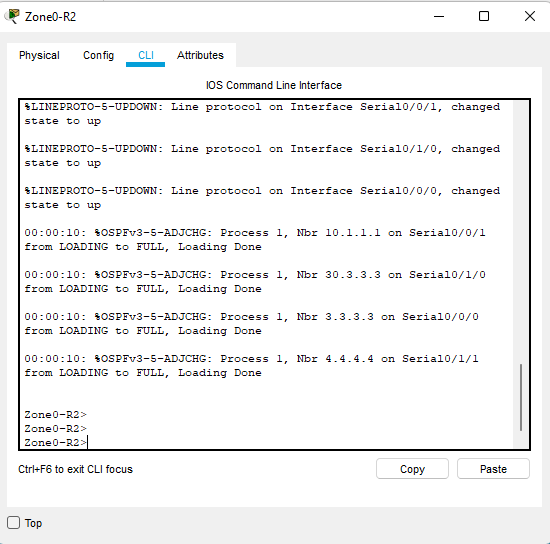


Figure 5. 2 : CLI

La plupart des périphériques d'interconnexion peuvent être configurés à l'aide de l'interface graphique ou de l'interface de ligne de commande. L'utilisation de l'interface de ligne de commande (CLI) peut fournir à l'administrateur réseau un contrôle et une flexibilité plus précis que l'utilisation de l'interface graphique.

## Maquette de la mise en œuvre

Dans le cadre de cette mise en œuvre, nous avons utilisé septe (7) PCs et huit (8) serveurs pour les équipements finaux. Neuf (9) routeurs Cisco 1941 series et quatre (4) switchs Cisco Catalyst 2960 pour l’interconnexion du système. Un (1) Access point pour crée un réseau sans fil. Un (1) Cloud pour mettre en place une technologie de FAI (Frame Relay). Une (1) machine (Laptop) pour se connecter à distance via SSh.

La figure 5.3 illustre les dispositions des équipements dans le réseau :

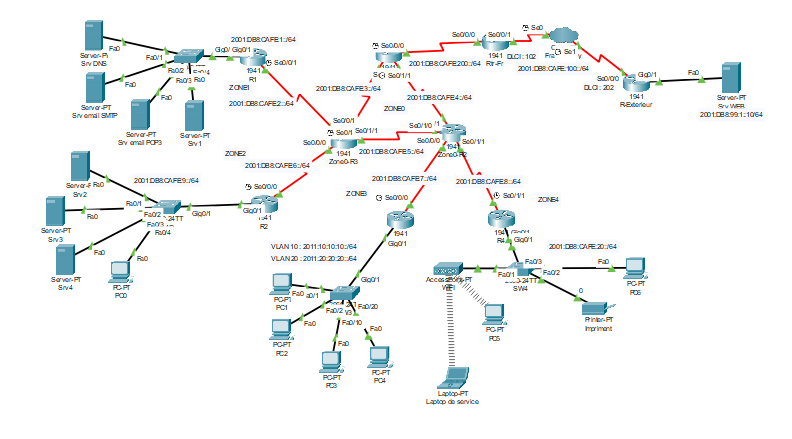


Figure 5. 3 : Maquette de la mise en œuvre

## Configuration des équipements

On va lancer des séries des configurations sur tous les équipements du réseau. Dans ce qui suit on va présenter la configuration en générale de tous les équipements avec un exemple configurée.

## Configuration des commutateurs

On suit les étapes de configuration illustrées ci-dessous pour configurer les commutateurs :

1. Configuration de Hostname : (Nomination des équipements sur « Cisco Packet Tracer »)
2. Configuration de vlans

On rappelle que les switches travaillent sur la couche 2 de modèle OSI.

Exemple : de configuration : le switch zone 1 (SW1) :

### Configuration de Hostname

****

Figure 5. 4 : Configuration de Hostname

On passe en mode configuration en saisissant les commandes « enable » ou « en » puis « configuration terminal » ou « conf t ».

### Configuration des vlans

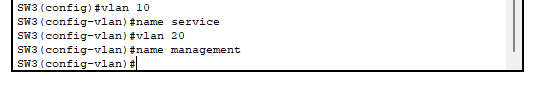
Exemple de configuration : le switch zone 3 (SW3)

Figure 5. 5 : Création vlans

Nous avons créé deux vlans pour le réseau LAN qui se trouve sur la zone 3.

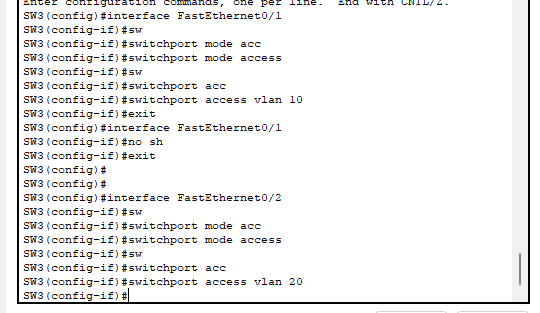


Figure 5. 6 : Attribution de Vlans

Ensuite, nous attribuons les vlans aux interfaces. Dans la figure 5.6, nous avons attribué vlan10 à l'interface « FastEthernet0/10 » et vlan20 à l'interface « FastEthernet0/20 ».

Nous avons configuré les vlans uniquement sur le switch 3 (SW3). C'est le seul réseau qui a des vlans.

## Configurations des routeurs

De même on va suivre les étapes de configurations suivantes :

1. Configuration de Hostname
2. Configuration d’accès à distance (ssh)
3. Configuration des interfaces
4. Configuration de routage
5. Configuration de frame relay

### Configuration de Hostname

Exemple de configuration : le routeur zone 1 (R1)



Figure 5. 7 : Configuration de Hostname routeur

### Configuration d’accès à distance (SSH)

Exemple de configuration : le routeur 1 zone 1 (R1)

SSH est le protocole le plus sécurisé pour établir une communication avec un équipement distant. Les communications sont chiffrées entre les 2 équipements concernés sur le port 22. Malheureusement ce protocole n’est pas pris en compte sur tous les équipements.

Voici maintenant la configuration SSH en détail

* Référençons un nom de domaine avec la commande : ip domain-name monlabo.com
* Activons le cryptage avec les paires de clé RSA en saisissant la commande : crypto key generate rsa

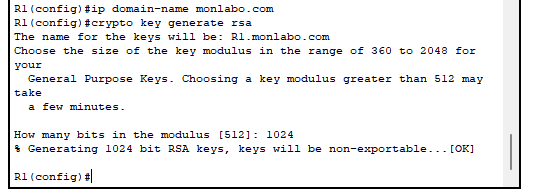


Figure 5. 8 : Configuration SSH

Par défaut, une longueur de 512 bits est proposée. Pour plus de sécurité il faut augmenter le nombre de bits. Pour une sécurité minimum Cisco préconise une valeur de 1024. Mais on peut aller jusqu’à 2048 bits.

Ensuite configurons un login « monlabo » et un mot de passe qui sera « Az001122 » avec la commande : username monlabo password Az001122.

Configuration des lines pour déclarer que seul le protocole SSH sera disponible avec l’utilisateur que nous venons de créer.

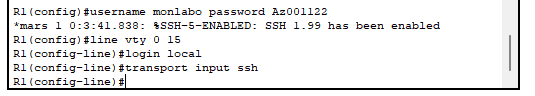


Figure 5. 9 : Configuration login ssh

### Configuration des interfaces

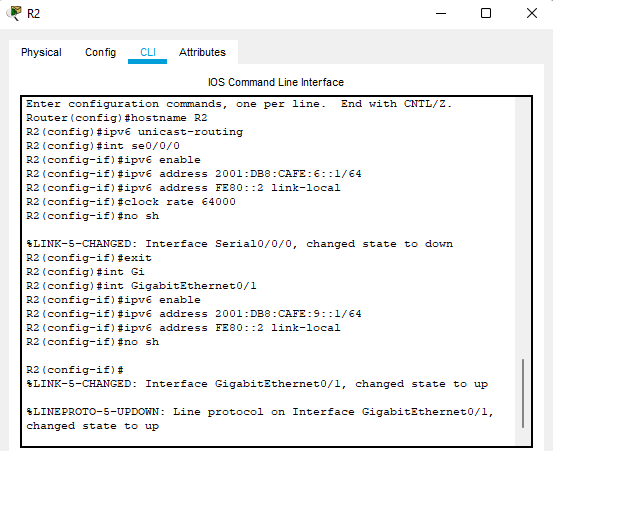
****Exemple de configuration : le routeur 2 (R2)

Figure 5. 10 : Configuration des interfaces routeur

Contrairement à l'adressage IPv4, les interfaces IPv6 ont généralement plusieurs adresses IPv6. Au minimum, un appareil IPv6 doit avoir une adresse lien-local IPv6, mais très probablement aussi une adresse de monodiffusion globale IPv6. IPv6 permet également à une interface d'avoir plusieurs adresses de monodiffusion globales IPv6 à partir du même sous-réseau.

### Configuration de routage

Exemple de configuration : le routeur 3 zone 0 (Zone0-R3)

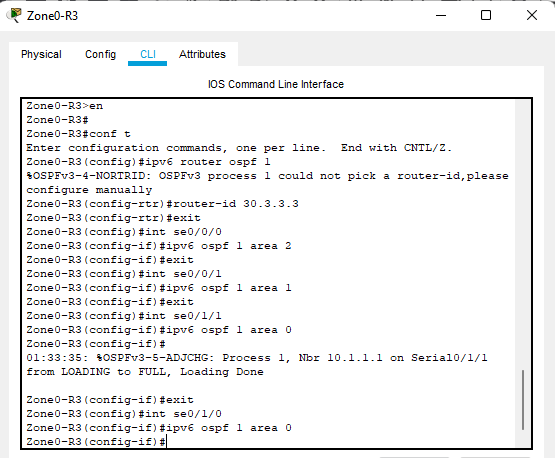
****

Figure 5. 11 : Configuration de routage

Une des raisons qui nous a poussés à choisir ipv6 est la configuration de certaines technologies et protocoles que certains ignorent.

Nous voulons montrer que la configuration du protocole OSPFv3 n'est pas seulement différente de OSPF (ipv4) mais aussi facile.

Comme nous le savons, IPV6 a été créé pour éviter ou résoudre certains problèmes dus à la configuration d'IPV4. Nous verrons que c'est le cas pour le protocole OSPFv3.

Pour configurer OSPFv3, dans la figure 5.11, nous avons entré sur le routeur (Zone0-R3), puis activé le protocole OSPF avec la commande « ipv6 route ospf 1 ». Ensuit on a mis l'id du routeur en question « 30.3.3.3 » qui celui de ce routeur, et enfin on est rentré dans les interfaces « se0/0/0, se0/0/1 et se0/1/1 » pour déclarer le protocole et la zone avec la commande « ipv6 ospf 1 area 0 », puisque l'on est dans une multizone.

### Configuration de Frame Relay

Exemple de configuration : le routeur de Frame Relay (Rtr-Fr)

Nous allons d’abord configure les deux routeurs qui son relier avec le cloud. En configurant l’adressage et aussi la diffusion de la technologie frame relaye.

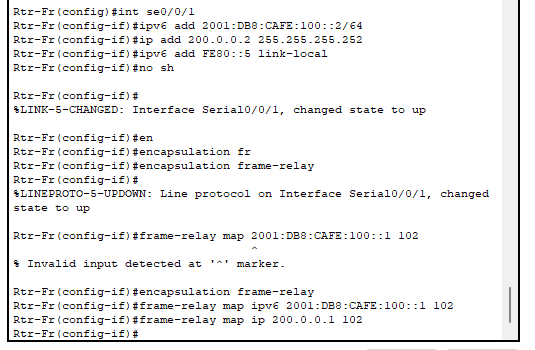
****

Figure 5. 12 : Configuration de frame Relay

Après avoir configuré les deux routeurs (Rtr-Fe et R-Exterieur) pour se connecter au cloud à relais de trames, nous entrerons dans le cloud. Cliquez sur l'interface et sélectionnez l'interface "serial0/serial1". Pour définir le DLCI et le nom comme suit :

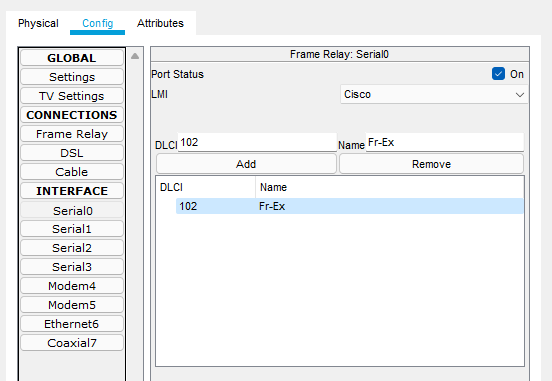


Figure 5. 13 : Configuration de serial0 Frame Relay

Ensuite, nous allons dans Frame Relay pour sélectionner le port et le sous-lien. Ici, nous avons sélectionné serial0 avec le sous-lien Fr-Ex (nom) et serial1 avec le « Ex-Fr ».

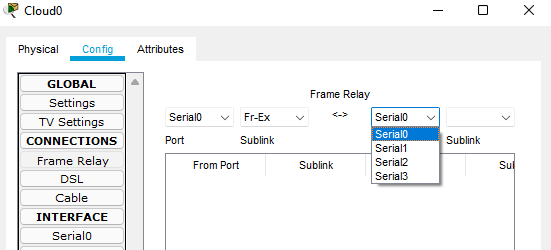


Figure 5. 14 : Configuration interface Frame Relay

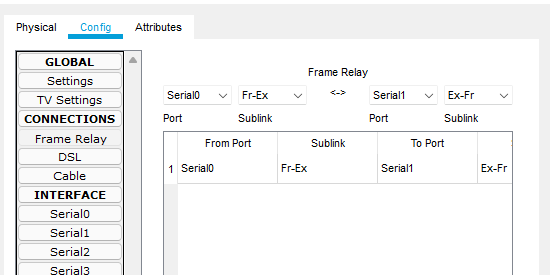


Figure 5. 15 : Interface Frame Relay

Sur la figure suivante, on mappe l'adresse IP de destination sur DLCI 102. Et le protocole OSPF utilisera DLCI 102 pour diffuser les mises à jour.

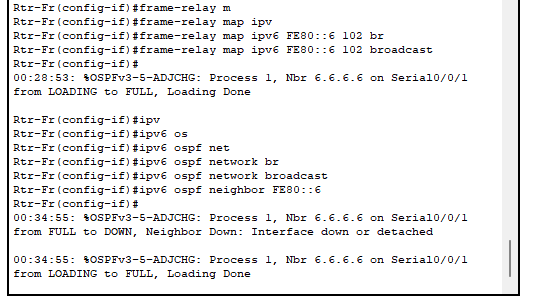


Figure 5. 16 : Configuration de diffusion Frame Relay

## Configuration des PCs et serveurs

Nous avons dans ce modèle PC7 qui nous allons configurées son adresse IP et sa passerelle.

Sur ce PC, dans la figure 5.17, nous avons configuré l'adresse de manière statique tandis que dans la figure 5.18, nous l'avons configurée en auto-config.

Exemple de configuration : PC0

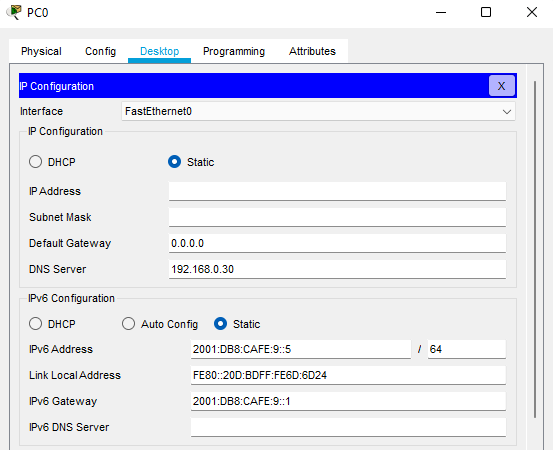


Figure 5. 17 : Configuration des PCs (static)

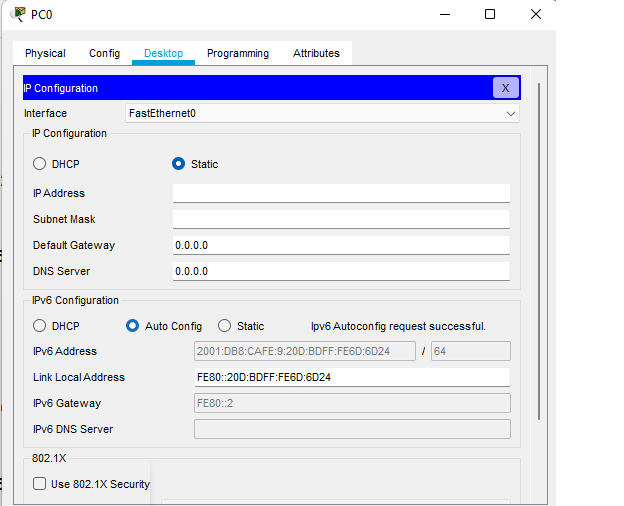


Figure 5. 18 : Configuration des PCs (Auto-config)

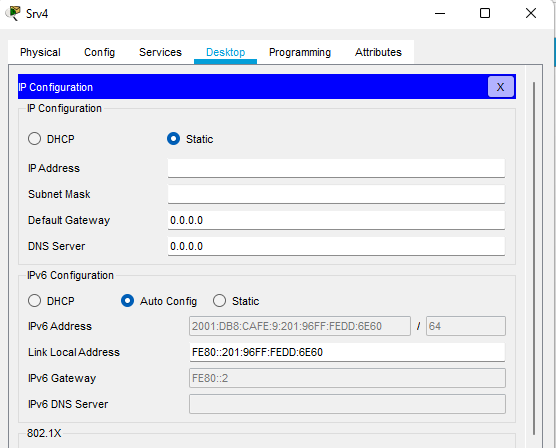
Exemple de configuration Serveur 4 (Srv4)

Figure 5. 19 : Configuration des serveurs (auto-config)

## Configuration des services

### DNS

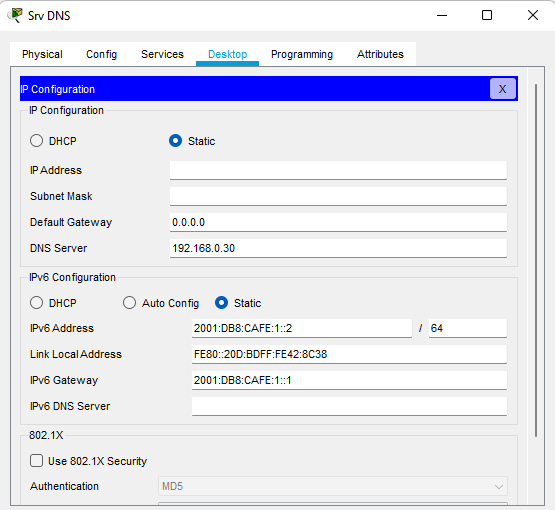
****Nous allons configure le serveur DNS « Domain Name System », qui est un des services qu’on a déployé sur le système.

Figure 5. 20 : Configuration de DNS

Dans la figure nous avons l'adresse du serveur qui est "2001:DB8:CAFE:1::2". Qui a été configuré avec sa passerelle de manière statique.

Nous avons configuré le DNS sur ce serveur avec l'adresse "192.168.0.30", que nous mettrons ensuite dans tous les PC et serveurs (de manière statique).

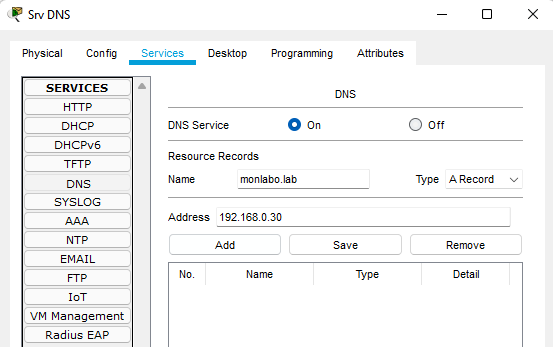
****Ensuite dans la figure 5.21, on va dans l'onglet services pour configurer le service DNS en saisissant le nom de domaine qui sera "monlabo.com" et en ajoutant l'adresse DNS.

Figure 5. 21 : Configuration de nom DNS

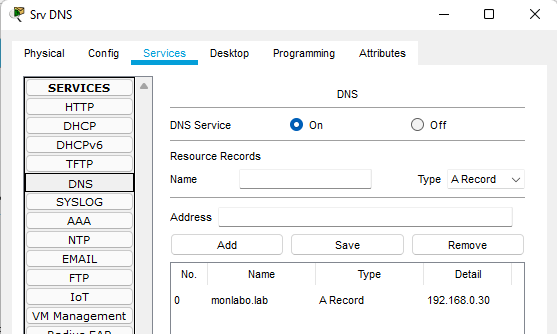
****

Figure 5. 22 : Service DNS configuré

### EMAIL

Nous allons un service de messagerie. Dans ce cas, nous avons besoin de deux serveurs. Le premier pour l'envoi et le second pour le recevoir.

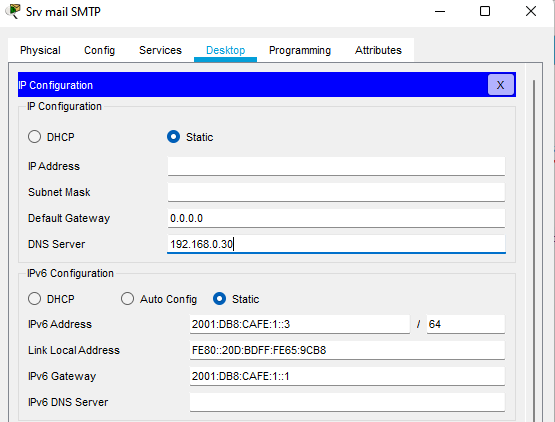


Figure 5. 23 : Configuration de serveur email

Ici nous avons le serveur d'envoi, dans lequel nous lui donnerons une adresse et aussi l'adresse DNS.

Puis on vient au service pour ajouter le nom de domaine « service.lab ». Ajoutant également des utilisateurs comme le montre la figure 6. On coche aussi "on" à "SMTP Service" qui est le protocole responsable de l'envoi.

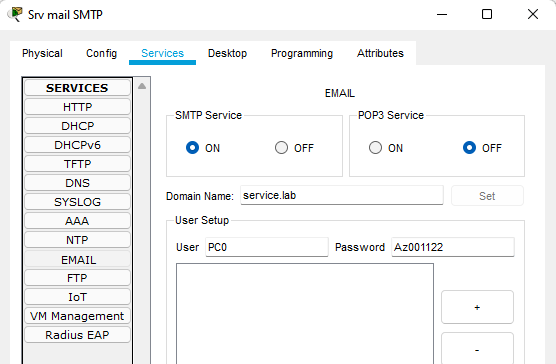
****

Figure 5. 24 : Configuration de serveur email (SMTP)

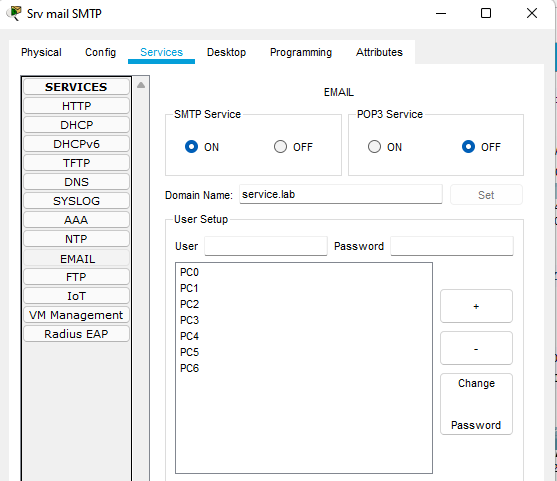
****

Figure 5. 25 : Configuration de serveur email (SMTP)

Nous configurons ensuite le deuxième serveur qui sera chargé à la réception. En lui donnant l'adresse et en cochant « on » au protocole « POP3 Service » responsable de la réception. Avec le nom de Domain « manage.lab ».

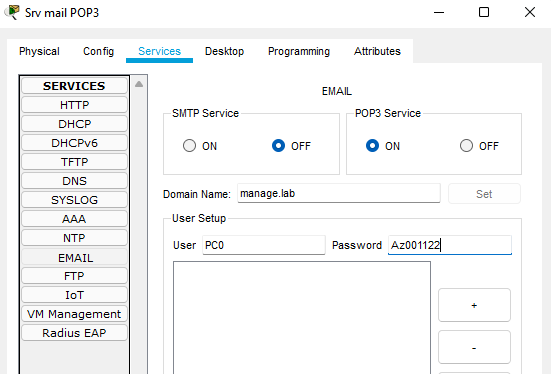
****

Figure 5. 26 : Configuration de serveur email (POP3)

### WEB

Le serveur web appelle également le serveur http « Hypertext Transfer Protocol » qui signifie protocole d'échange hypertexte. Il permet de stocker et de diffuser des pages Web qui sont généralement rendues en html.

Nous allons le configurer en lui donnant une adresse statique, l'adresse de la passerelle et l'adresse DNS. Ensuite, nous entrons dans le service http pour modifier le code html.

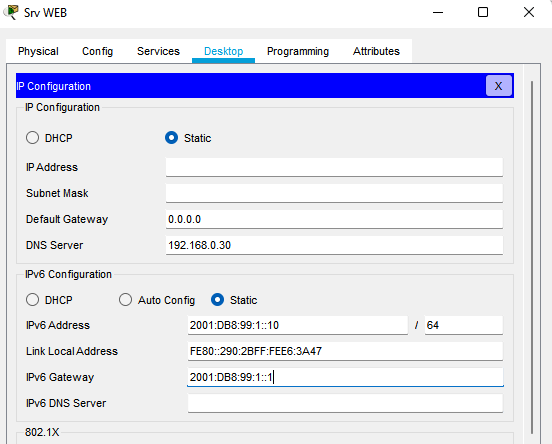


Figure 5. 27 : Configuration de serveur web

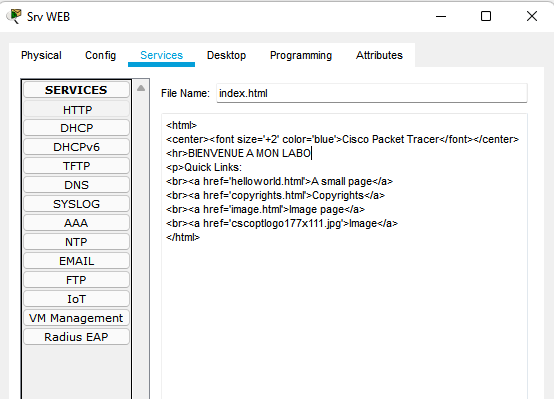
****

Figure 5. 28 : Modification de fichier html

# TESTS ET VERIFICATION

On test les communications entre tous les équipements en utilisant la commande Ping. Ces tests sont faits entre équipements, entre Vlans et entre les réseaux. Il est à noter que la commande Ping est très utile pour tester la réponse d'un ordinateur sur un réseau. Cette commande envoie des paquets avec le protocole ICMP.

Nous allons aussi teste le routage, les services et les technologies déployer.

## Ping

Pour les ping nous les faisons entre équipements.

* Entre routeurs

Exemple teste : R4 et R1.

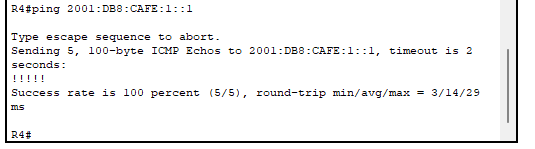


Figure 6. 1 : Teste ping routeur et routeur

* Entre PCs et routeurs

Exemple teste PC6 et R1.

Nous allons faire un ping sur le PC6 avec l’adresse de passerelle du réseau « 2001:DB8:CAFE:1::/64 ».

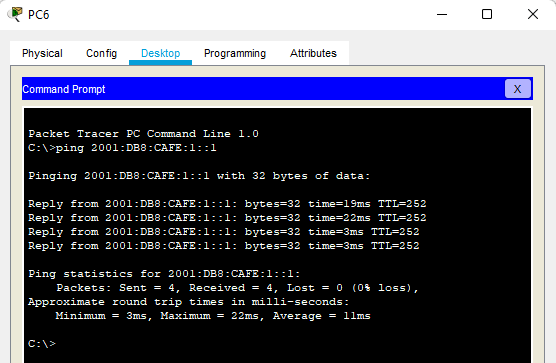


Figure 6. 2 : Test ping PC et routeur

* Entre PCs et Vlans

Exemple teste PC0 et PC3 (Vlan10).

Ce ping va se faire entre un réseau et vlan, d’où nous allons pinger le PC0 avec l’adresse vlan10 du PC3 « 2011:10:10:10::3».

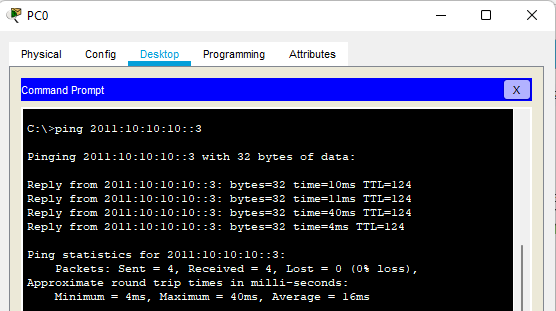


Figure 6. 3 : Teste ping PC et VLAN

* Entre PCs/Serveurs

Nous allons d'abord tester entre les points de terminaison qui sont configurés de manière statique, puis le faire sur ceux qui sont configurés en auto-config.

Exemple de tests PC/serveurs configurés statiquement : entre PC0 et PC6.

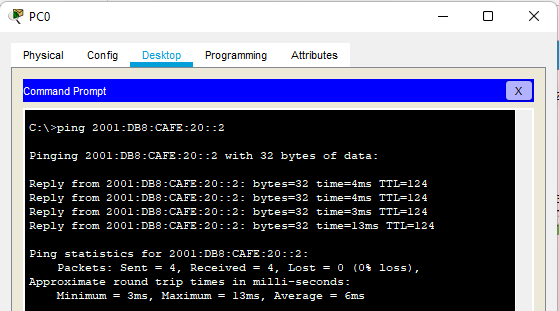


Figure 6. 4 Teste ping Pcs/serveurs (statistique)

Exemple de teste PC/serveurs configurés en auto-config : entre PC6 et Srv4

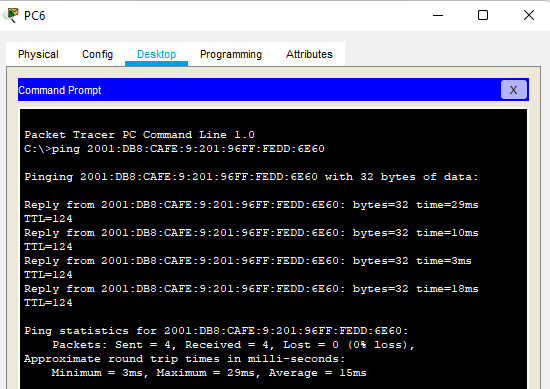


Figure 6. 5 : Teste ping Pcs/serveurs (auto-config)

* Entre Vlans

Exemple teste PC2 (Vlan20) et PC3 (Vlan10).

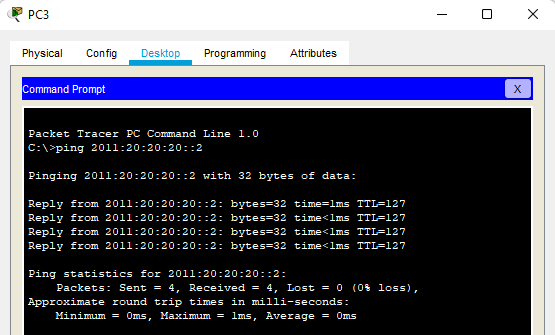
Nous allons pinger le PC3 (Vlan10) avec l’adresse vlan20 du PC2 « 2011:20:20:20::2».

Figure 6. 6 : Teste ping entre Vlans

## SSH

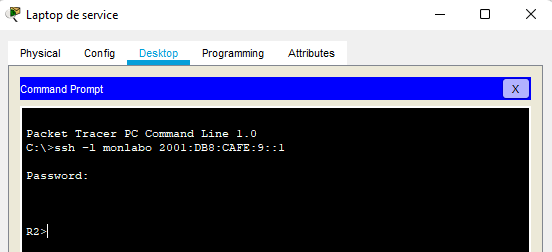
Nous avons installé un service Laptop pour se connecter à distance. En saisissant la commande "ssh –l monlabo 2001:DB8:CAFE:9::1". Pour le test, nous l'avons fait pour le routeur R1. Avec le login "monlabo" et le mot de passe "Az001122".

Figure 6. 7 : Teste ssh

## Email

Nous allons tester en envoyant un e-mail de PC6 à PC0.

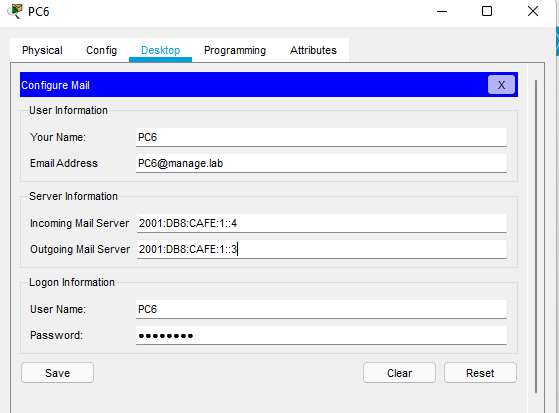
****

Figure 6. 8 : Configuration email PC6

Sur la figure3.34, nous avons configuré le mail avec le nom du PC « PC6 », l'adresse mail « PC6@manage.lab », l’adresse du serveur de réception (l'adresse du serveur Srv email POP3 : 2001:DB8:CAFE:1::4) et l'envoi (l'adresse du serveur Srv email SMTP : 2001:DB8:CAFE:1::3), le nom d’utilisateur dont les utilisateur que nous avons ajouté quand on configurait le service e-mail et le mot de passe.

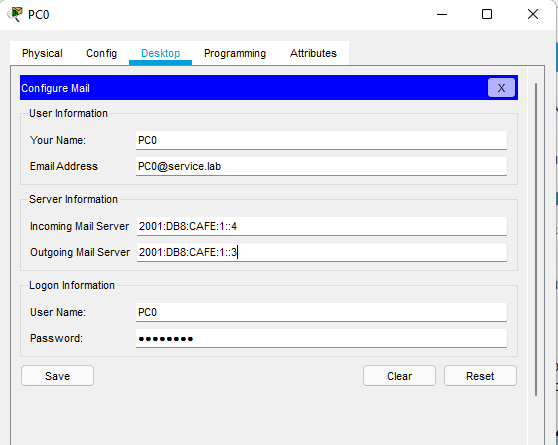
****

Figure 6. 9 : Configuration email PC0

Sur la figure 6.9, nous avons configuré le mail avec le nom du PC « PC0 », l'adresse mail « PC0@service.lab », l’adresse du serveur de réception (l'adresse du serveur Srv email POP3 : 2001:DB8:CAFE:1::4) et l'envoi (l'adresse du serveur Srv email SMTP : 2001:DB8:CAFE:1::3), le nom d’utilisateur dont les utilisateur que nous avons ajouté quand on configurait le service e-mail et le mot de passe.

Ensuite on procède à l'envoi du message, sur PC6 en saisissant l'adresse du destinataire « PC0@service.lab », l’objet « test » et le message test test test ». (Figure 6.10)

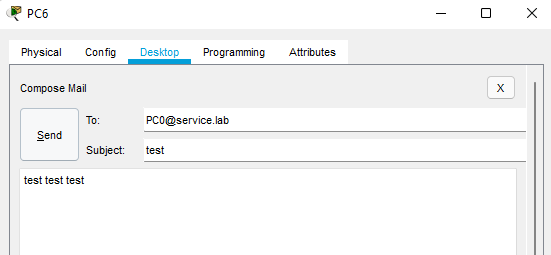


Figure 6. 10 : Teste envoi de mail

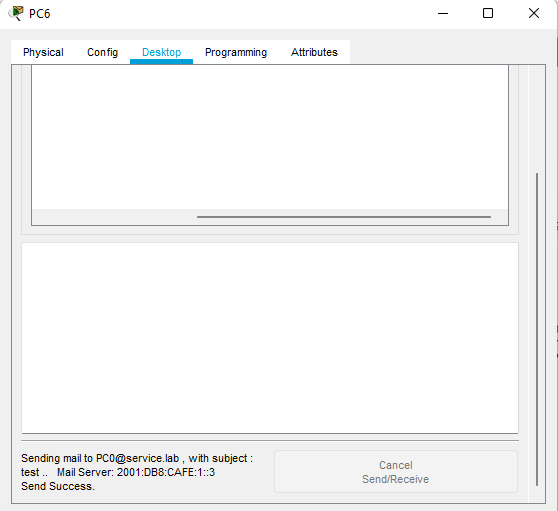
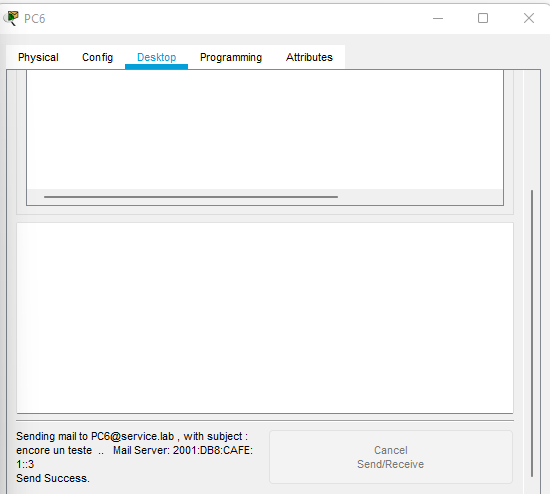


Figure 6. 11 : Envoi mail succès

****

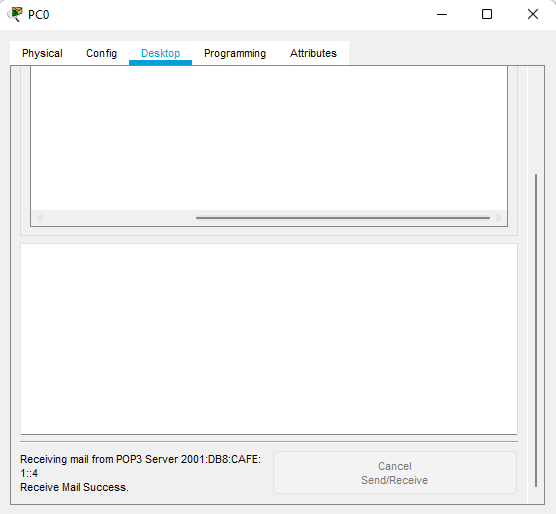


Figure 6. 12 : Reçois mail succès

En observant ces deux figures nous verrons que le mail a bien été envoyé. Sur la figure 6.11, nous voyons que le message a été envoyé avec le message « Send Success » via l'adresse d'envoi «2001:DB8:CAFE:1::3 ». Dans la figure 6.12, nous voyons que l'e-mail a été reçu avec le message "Receive Mail Success »" via l'adresse de réception "2001:DB8:CAFE:1::4".

## WEB

Il suffit de mettre l'adresse ip du serveur web sur un pc qui se trouve sur le système.

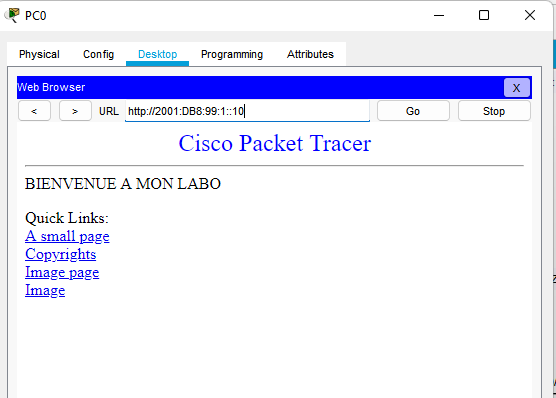


Figure 6. 13 : Teste web

## Routage

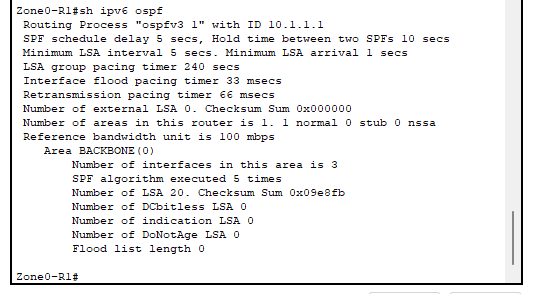


Figure 6. 14 : Information ospf

Pour afficher la table de routage, entrez la commande « sh ipv6 route ».

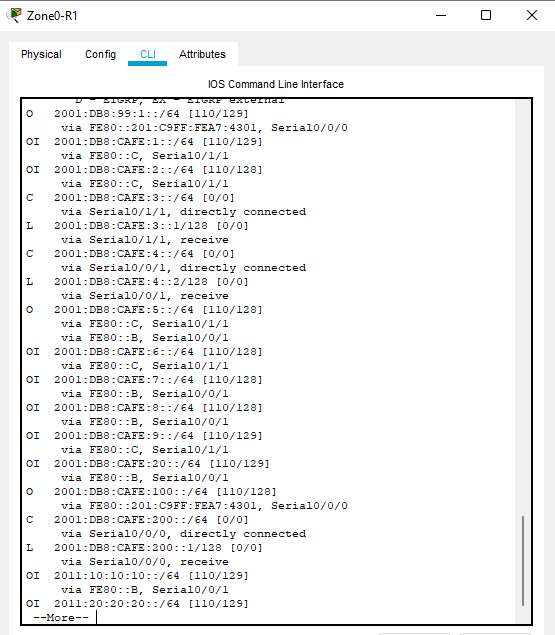


Figure 6. 15 : Table de routage

Nous avons ici la table de routage du routeur Zone0-R1. Le symbole « O » signifie réseaux ospf, « OI » ospf interne, « C » réseaux directement connectés et « L » adresses locales.

# CONCLUSION GENERALE

La mise en place d’un modèle type de configuration d’un réseau multizone sous ospfv3 était l'objectif principal de notre projet. En effet, on a essayé de concevoir une solution pour la préparation d’un dossier technique du projet, la maquette et sa mise en œuvre.

Ce projet a traité tous les aspects de multizone ainsi que sa mise en place par la proposition d'un modèle type d'architecture, de conception et de réalisation.

OSPFv3 présente de nombreux avantages mais il doit en conserver de nombreux défis et surmonter certaines difficultés techniques, notamment la configuration de certaines technologies.

Malgré quelques inconvénients, il reste une bonne solution en termes d'intégration, de fiabilité, d'évolutivité et de coût. Il permet également une grande mobilité en l'associant à d'autres technologies ainsi qu'à sa configuration multizone. On ne peut que se réjouir de vivre le développement de ses différentes technologies.

On peut donc sans doute penser que bientôt les réseaux seront tous configurés avec l'ospfv3 et que le protocole IPV6 deviendra un jour un standard unique permettant l'interopérabilité des réseaux mondiaux.

Ce projet a été une expérience fructueuse qui nous a permis de mieux aborder le protocole IPV6. Cela nous a permis de savoir gérer et optimiser le temps dans le viser à en tirer le meilleur parti.

# REFERENCES

# BIBLIOGRAPHIE

Chrtophe. (s. d.). *La théorie des réseaux locaux et étendus*. Récupéré sur developpez.com: https://hautrive.developpez.com/reseaux/?page=page\_14

Eric. (2018, Mai 14). *Quels sont les avantages d’une ipv6 ?* Récupéré sur Blog LWS: https://blog.lws-hosting.com/divers/quels-sont-les-avantages-dun-ipv6

Goffinet, F. (2020, aout 10). *Introduction au protocole de routage dynamique OSPF*. Récupéré sur cisco.goffinet.org: https://cisco.goffinet.org/ccna/ospf/introduction-au-protocole-routage-dynamique-ospf/

Goffinet, F. (2020, août 10). *Technologies et topologies WAN*. Récupéré sur cisco.goffinet.org: https://cisco.goffinet.org/ccna/wan/technologies-topologies-wan/

Informatiques, C. (s. d.). *Les types d'authentification dans OSPF*. Récupéré sur ordinateur.cc: http://www.ordinateur.cc/r%C3%A9seaux/Routeurs/80283.html

Morin, M.-D. (2018). *Routage OSPF à zones multiples pour CCNA*. Récupéré sur SlidePlayer: https://slideplayer.fr/slide/11353855/

TSHIMANGA, D. (2012). *Etude d'implémentation d'une solution VOIP sécurisée dans un réseau informatique d'entreprise. Cas de l'ISTA de Kinshasa. Mémoire d'ingénieur, INSTITUT SUPERIEUR DE TECHNIQUES APPLIQUEES de KINSHASA, 16-21.* Récupéré sur Memoire Online: https://www.memoireonline.com/09/13/7361/m\_Etude-dimplementation-dune-solution-VOIP-securisee-dans-un-reseau-informatique-dentrepr9.html#:~:text=La%20classification%20se%20fait%20par,Classification%20selon%20la%20topologie.

# WEBGRAPHIE

[W1] <https://slideplayer.fr/slide/11353855/> consulté le 6 février 2022 à 9h50.

[W2] <https://www.networklab.fr/les-differents-types-de-zones-ospf/> consulté le 16 février 2022 à 11h20.

[W3] https://www.memoireonline.com/09/13/7361/m\_Etude-dimplementation-dune-solution-VOIP-securisee-dans-un-reseau-informatique-dentrepr9.html consulté le 20 mars 2022 à 15h10.

[W4] <https://hautrive.developpez.com/reseaux/?page=page_14> consulté le 20 février 2022 à 16h39.

[W5] <https://fr.wikipedia.org/wiki/Fournisseur_d%27acc%C3%A8s_%C3%A0_Internet> consulté le 5 mars 2022 à 14h20.

[W6] <https://cisco.goffinet.org/categories/ipv6> consulté le 5 mars 2022 à 20h50.

[W7] <http://cisco.ofppt.info/ccna3/course/module6/6.1.1.2/6.1.1.2.html> consulté le 5 mars 2022 à 19h30.

[W8] <https://cisco.goffinet.org/ccna/ipv6/adresses-ipv6-multicast/> consulté le 8 mars 2022 à 22h16.

[W9] <https://cisco.goffinet.org/ccna/ipv6/adresses-ipv6-unicast/> consulté le 13 mars 2022 à 10h30.

[W10] <http://livre.g6.asso.fr/index.php?title=Plans_d%27adressage&oldid=1336> consulté le 13 mars 2022 à 15h20.

[W11] <https://docs.microsoft.com/fr-fr/dotnet/framework/network-programming/ipv6-addressing> consulté le 17 mars 2022 à 17h10.

[W12] <https://www.it-connect.fr/chapitres/ipv6-normes-et-definitions/> consulté le 17 mars 2022 à 00h45.