|  |
| --- |
| LIVRABLE 3 :  Plan de déploiement |



Deshani KUMARATHAS

Isaac MAAREK

Youssef DEROUICH

Florian BOULMIER

|  |  |  |
| --- | --- | --- |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| PROJET FUNKYTOWN : BLOC RESEAUX & SYSTEMES  CPI A2 INFO 24/25 |  |  |

sommaire

[INTRODUCTION 1](#_Toc188571763)

Objectif du livrable 3 [1](#_Toc188571764)

[Méthodologie de déploiement 4](#_Toc188571765)

[Processus de déploiement 5](#_Toc188571766)

[Schémas logiques de déploiemment 42](#_Toc188571767)

[Conclusion 46](#_Toc188571768)

INTRODUCTION

Dans le cadre de sa politique numérique, le maire de Funkytown soutient activement les entreprises locales dans leur transformation digitale. Ce projet vise à fournir des infrastructures réseau modernes et adaptées aux besoins des entreprises de la ville, notamment l’ESN eXia, la Bibliothèque municipale, Engie, et Digiplex.

Notre rôle est d’accompagner ces structures dans la conception et le déploiement de leurs réseaux en respectant les spécifications du cahier des charges, tout en garantissant une sécurité et une évolutivité optimales. Pour mener à bien cette mission, nous avons commencé par réaliser un plan d’adressage, fondation de la configuration réseau.

OBJECTIF DU LIVRABLE 3

Le livrable 3 présente la stratégie de déploiement des configurations réseau, assurant la continuité des activités. Ce document comprend :

1. Stratégie de déploiement

* Diagramme GANTT
* Installation et configuration des équipements réseau par site (documentation)
* Interconnexions des sites
* Minimisation des interruptions d’activité

1. Schéma logique des réseaux

* Schéma global des réseaux
* Topologie logique (IPv4/IPv6, VLANs, tunnels)
* Cartographie des équipements et services

1. Validation

* Tests des configurations

METHODOLOGIE DE DEPLOIEMENT

|  |  |
| --- | --- |
| Tâches | Date de rendu |
| Plan d’adressage | 13/01/2025 |
| Maquette réseau | 27/01/2025 |
| Plan de déploiement | 26/01/2025 |
| Outils de gestion de projet | 26/01/2025 |

**Diagramme de Gantt**

Une image contenant texte, capture d’écran, nombre, ligne

Description générée automatiquement

**Planning des interventions par site**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date de début | Date de fin | Site | Intervention | Durée (jours) |
| 12/12/2024 | 14/12/2024 | eXia | Configuration du routeur, switch et borne Wifi | 3 |
| 17/12/2024 | 19/12/2024 | Bibliothèque | Mise en place du réseau public et des configurations des équipements | 3 |
| 20/12/2024 | 30/12/2024 | Engie | Configuration des VLANs et routage inter-VLAN | 7 |
| 31/12/2024 | 17/01/2025 | Digiplex | Installation des VLANs multi-étages et Wifi d’entreprise | 14 |
| 20/01/2025 | 23/01/2025 | Datacenter | Mise en place du tunnel IPv6 et vérification des connexions | 4 |

PROCESSUS DE DEPLOIEMENT

Réseau ESN eXia

Rappel de ce que l’on dispose :

* 1 routeur
* 2 PC fixes
* 1 switch L2
* 1 borne Wifi
* 1 serveur DNS/FTP
* 1 PC portable

**Branchement des éléments du réseau**

**Connexion des appareils** :

* + Les deux PC fixes, le PC portable et le serveur DNS/FTP sont connectés au switch.
  + Le switch est relié au routeur via une interface GigabitEthernet.
  + La borne Wi-Fi (modèle WRT300N Linksys) est branchée au routeur.

Cette architecture permet une communication efficace entre les appareils connectés en filaire et en Wi-Fi.

**Configuration du routeur**

**Étapes de configuration**

**Accéder au mode configuration** :

enable

router#

router#configure terminal

enter configuration commands, one per line. End with CNTL/Z

**Configurer l'interface FastEthernet0/0 ou FastEthernet0/1** :

Router(config)#interface FastEthernet0/0

Router(config-if)#ip address 192.168.1.254 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface FastEthernet0/1

Router(config-if)#ip address 192.168.0.254255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

* **Explication** : L'adresse IP 192.168.1.254 avec un masque de sous-réseau /24 est assignée à l'interface FastEthernet0/0 pour permettre au routeur de communiquer avec le réseau local.

**Configurer les lignes console** :

Router(config)#line console 0

Router(config-line)#password eXiaSecretwWqIRmdf023by

Router(config-line)#login

Router(config-line)#exit

* **Explication** : Cette configuration protège l'accès console avec un mot de passe.

**Configurer un mot de passe secret pour le mode privilégié** :

Router(config)#enable secret zdio867E3NDioM

* + **Explication** : Ce mot de passe est chiffré pour renforcer la sécurité du routeur.

**Configuration du switch**

**Étapes de configuration**

**Accéder au mode configuration** :

Enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

**Configurer les lignes console** :

Switch(config)#line console 0

Switch(config-line)#password CSH23di7210djzU2d

Switch(config-line)#login

Switch(config-line)#exit

* **Explication** : Un mot de passe est défini pour protéger l'accès console au switch.

**Configurer un mot de passe secret pour le mode privilégié** :

Switch(config)#enable secret SDC1yu17zd5K23ZD

* + **Explication** : Ce mot de passe protège l'accès administrateur au switch.

**Configuration de la borne Wi-Fi**

**Informations générales** :

**Modèle utilisé** : Access Point

**Explication** : La borne Wi-Fi utilise l’adresse du réseau pour gérer les connexions des appareils sans fil.

**Configuration sans fil** :

* + **Authentification** : WPA2-PSK (sécurisée pour les réseaux modernes)

**Configuration du serveur DNS/FTP**

**Paramètres FTP**

**Activer le service FTP** :

FTP On

**Créer des utilisateurs** :

Administrator AdminExiaSecretuXzWY RWDNL

Editor EmployeesAccountSecretuWYte RWN

Reader easyPasswordezDYUfg R

* **Explication** :
* Administrator : Droits complets de lecture, écriture, suppression, renommage, et liste.
* Editor : Droits de lecture, écriture, et renommage.
* Reader : Droits de lecture uniquement.

**Paramètres DNS**

**Activer le service DNS** :

DNS On

**Ajouter un enregistrement DNS** :

www.google.com 108.177.127.139

* **Explication** : Cet enregistrement permet de résoudre le nom de domaine www.google.com vers l'adresse IP publique spécifiée.

**Note** : Chaque étape a été validée pour garantir un réseau fonctionnel et sécurisé. La documentation est organisée pour une compréhension claire et une réplicabilité facile.

Pour finir on assigne les adresses de manière statique en se basant sur le tableau ci-dessous :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Appareil** | **Adresse IP** | **Masque de sous-réseau** | **Passerelle par défaut** | **Serveur DNS** |
| **PC0** | 192.168.1.51 | 255.255.255.0 | 192.168.1.254 | 192.168.1.2 |
| **PC1** | 192.168.1.52 | 255.255.255.0 | 192.168.1.254 | 192.168.1.2 |
| **Laptop0** | 192.168.1.53 | 255.255.255.0 | 192.168.1.254 | 192.168.1.2 |
| **Serveur DNS/FTP** | 192.168.1.2 | 255.255.255.0 | 192.168.1.254 | 192.168.1.2 |
| **Borne Wifi** | 192.168.1.3 | 255.255.255.0 | 192.168.1.254 | 192.168.1.2 |

Pour le réseau sans fil WPA2-PSK le mot de passe est Z21de8Z-JK5dh6P-32 et le SSID réseau eXia.

Réseau BIBLIOTHEQUE

Rappel de ce que l’on dispose :

* 1 routeur
* 5 PC fixes
* 1 switch L2
* 1 borne Wifi
* 2 PC portables

**Configuration du routeur**

**Configuration d’un mot de passe pour sécuriser l’accès physique :**

Pour sécuriser l’accès au routeur et empêcher les utilisateurs non autorisés d’accéder directement via la console, un mot de passe a été configuré sur la ligne console.

Enable

Configure terminal

Line console 0

password ud56df0y83UzDE

Login

Exit

* Le mot de passe défini est requis pour accéder au routeur via la console. La commande login active la vérification du mot de passe.

**Définir un mot de passe pour sécuriser le mode privilégié :**

Un mot de passe a été configuré pour restreindre l’accès au mode privilégié où les configurations critiques du routeur peuvent être modifiées.

Enable secret HFuf37YdJ2

* Le mot de passe défini ici est crypté et sera demandé chaque fois que l’utilisateur tentera de passer au mode privilégié via la commande enable.

**Attribuer un nom au routeur pour une identification simplifiée :**

Un nom a été attribué au routeur pour faciliter son identification au sein du réseau.

hostname MyRouter

* Cette commande change le nom par défaut du routeur ("Router") en "MyRouter", ce qui permet une meilleure organisation dans des environnements avec plusieurs périphériques.

**Configurer les interfaces pour établir les connexions réseau**

Les interfaces réseau du routeur ont été configurées pour permettre la communication avec le réseau local (LAN) et l’extérieur (WAN).

**Configuration de l’interface LAN pour le réseau local :**

interface FastEthernet0/0

ip address 192.168.0.254 255.255.255.0

No shutdown

Exit

* Cette configuration attribue l’adresse IP **192.168.0.1** à l’interface LAN et l’active avec la commande *no shutdown*. Cette adresse sera utilisée comme passerelle pour les appareils du réseau local.

**Configuration de l’interface WAN pour la connexion Internet :**

interface GigabitEthernet0/0/0

ip address 10.0.0.1 255.255.255.0

No shutdown

Exit

* L’interface WAN est configurée avec l’adresse **10.0.0.1** pour permettre au routeur de communiquer avec un périphérique externe, tel qu’un modem ou un autre routeur.

**Activer le DHCP pour automatiser l’attribution des adresses IP**

Le serveur DHCP a été activé pour attribuer automatiquement des adresses IP aux appareils du réseau local, simplifiant ainsi leur configuration.

**Exclure les adresses IP réservées :**

ip dhcp excluded-address 192.168.0.1 192.168.0.10

* Les adresses IP entre **192.168.0.1** et **192.168.0.10** sont exclues pour éviter qu’elles ne soient attribuées dynamiquement, car elles sont réservées pour le routeur et d’autres périphériques critiques.

**Créer un pool DHCP pour le réseau local :**

Ip dhcp pool Library

network 192.168.0.0 255.255.255.0

default-router 192.168.0.254

dns-server 8.8.8.8

Exit

* Le pool DHCP nommé "Library" attribue des adresses IP dans le réseau **192.168.0.254/24**, avec le routeur comme passerelle par défaut (**192.168.0.254**) et **8.8.8.8** comme serveur DNS.

**Configurer le NAT pour permettre l’accès à Internet**

Le NAT (Network Address Translation) a été configuré pour traduire les adresses IP internes en une adresse externe, permettant aux appareils locaux d’accéder à Internet.

**Créer une liste d’accès pour définir le réseau interne :**

access-list 1 permit 192.168.0.0 0.0.0.255

* Cette liste d’accès autorise tout le trafic provenant du réseau local **192.168.0.0/24** à utiliser le NAT.

**Configurer le NAT avec surcharge :**

ip nat inside source list 1 interface GigabitEthernet0/0/0 overload

* Le NAT utilise l’adresse IP de l’interface WAN (**GigabitEthernet0/0/0**) pour traduire les adresses IP locales, avec l’option "overload" permettant plusieurs connexions simultanées.

**Définir les interfaces pour le NAT :**

interface FastEthernet0/0

Ip nat inside

exit

interface GigabitEthernet0/0/0

Ip nat outside

Exit

* L’interface LAN (**FastEthernet0/0**) est définie comme "inside" (réseau interne) et l’interface WAN (**GigabitEthernet0/0/0**) comme "outside" (réseau externe).

**Ajouter une route par défaut pour rediriger le trafic Internet :**

Une route par défaut a été ajoutée pour rediriger tout le trafic non local vers la passerelle externe.

IP route 0.0.0.0 0.0.0.0 10.0.0.2

* Cette commande indique que tout le trafic destiné à des adresses non locales doit être redirigé vers l’adresse **10.0.0.2** (passerelle).

**Sauvegarder la configuration pour éviter de la perdre :**

Enfin, la configuration a été sauvegardée pour garantir qu’elle sera conservée après un redémarrage.

copy running-config startup-config

* Cette commande copie la configuration en cours (running-config) dans la mémoire de démarrage (startup-config).

Configuration switch

**Configuration d’un mot de passe pour sécuriser l’accès physique :**

Pour sécuriser l’accès au switch et empêcher les utilisateurs non autorisés d’accéder via la console physique, un mot de passe a été configuré.

Enable

Configure terminal

Line console 0

password consolepassword

Login

Exit

* Le mot de passe défini ici sera requis pour toute connexion via la console. La commande login active la vérification du mot de passe.

**Configurer un mot de passe pour sécuriser le mode privilégié :**

Un mot de passe a été défini pour restreindre l’accès au mode privilégié, où les modifications de configuration critiques peuvent être effectuées.

Enable secret U9ZDfyhe23

* Ce mot de passe est crypté et sera demandé lorsque l’utilisateur tentera d’accéder au mode privilégié avec la commande enable.

**Attribuer un nom au switch pour une meilleure identification :**

Un nom a été attribué au switch pour permettre une identification plus facile dans le réseau.

hostname Library\_Switch

* Le switch sera désormais identifié comme "*Library\_Switch*", facilitant son administration dans un environnement avec plusieurs équipements.

**Configurer une adresse IP pour la gestion du switch :**

Pour permettre un accès distant au switch via Telnet ou SSH, une adresse IP a été configurée sur l’interface VLAN 1.

interface vlan 1

Ip address 192.168.0.2 255.255.255.0

No shutdown

Exit

* Cette configuration attribue l’adresse IP **192.168.0.2** au switch, qui sera utilisée pour sa gestion à distance.

**Configurer une passerelle par défaut pour la communication externe :**

Une passerelle par défaut a été configurée pour permettre au switch de communiquer avec des appareils situés hors du réseau local.

Ip default-gateway 192.168.0.254

* Cette passerelle correspond à l’adresse IP du routeur.

**Configurer les ports du switch pour les PCs et la borne Wi-Fi :**

Les ports ont été configurés pour correspondre à leur utilisation spécifique dans le réseau.

**Ports connectés aux PCs (mode accès) :**

Interface range FastEthernet0/1-5

switchport mode access

Exit

* Ces ports sont définis en mode accès pour les appareils du réseau local (les PCs).

**Port connecté au routeur (mode trunk) :**

Interface FastEthernet0/24

switchport mode trunk

Exit

* Le port connecté au routeur est configuré en mode trunk pour transporter plusieurs VLANs si nécessaire.

**Port connecté à la borne Wi-Fi (mode accès) :**

Interface FastEthernet0/6

switchport mode access

Exit

* Le port de la borne Wi-Fi est configuré en mode accès pour la connexion au réseau local.

**Configurer SSH pour un accès distant sécurisé :**

Pour permettre une connexion sécurisée au switch via SSH, les paramètres suivants ont été configurés.

**Définir un nom de domaine :**

Ip domain-name library.local

* Cette commande est requise pour générer les clés RSA nécessaires à SSH.

**Créer un utilisateur avec des privilèges administratifs :**

username admin privilege 15 secret dhuDZp2H9d

* L’utilisateur "admin" a été créé avec un mot de passe sécurisé pour accéder au switch via SSH.

**Générer des clés RSA :**

Crypto key generate rsa

* Lorsque la taille de la clé est demandée, **1024 bits** a été choisi pour assurer un bon niveau de sécurité.

**Configurer les lignes VTY pour SSH uniquement :**

line vty 0 4

transport input ssh

Login local

Exit

* Les connexions distantes via Telnet sont désactivées, et seules les connexions SSH sont autorisées. L’authentification utilise les informations de l’utilisateur local créé précédemment.

**Sauvegarder la configuration pour éviter de la perdre :**

La configuration a été sauvegardée pour s’assurer qu’elle sera conservée après un redémarrage du switch.

copy running-config startup-config

* Cette commande copie la configuration en cours (running-config) dans la mémoire de démarrage (startup-config).

ACCES POINT

**Configuration du SSID pour identifier le réseau Wi-Fi :**

Un **SSID (Service Set Identifier)** a été configuré pour permettre aux appareils sans fil de détecter le réseau Wi-Fi. Ce SSID sera utilisé pour identifier le réseau public de la bibliothèque.

SSID : Library-Wifi

* Le SSID est configuré comme "Library-Wifi". Cela permet aux utilisateurs de reconnaître et de se connecter au réseau Wi-Fi de manière simple.

**Désactivation de la sécurité pour offrir un accès public ouvert :**

La sécurité Wi-Fi a été désactivée pour que le réseau soit ouvert et accessible à tous sans mot de passe.

Authentication: Disabled

Encryption Type: Disabled

* En désactivant l'authentification et le chiffrement, aucun mot de passe n’est requis pour se connecter au réseau Wi-Fi, offrant ainsi un accès facile pour le public.

**Configuration du canal pour éviter les interférences :**

Un canal a été défini pour minimiser les interférences avec d'autres réseaux Wi-Fi dans la même zone.

2.4 GHz Channel : 6

5 GHz Channel : Disabled

* Le canal 6 a été choisi pour le réseau **2.4 GHz**. L'utilisation du réseau **5 GHz** a été désactivée pour simplifier la configuration.

**Activation et portée du signal Wi-Fi :**

Le port correspondant à l’interface Wi-Fi a été activé pour diffuser le signal, et la portée a été ajustée pour couvrir efficacement la zone.

Port Status : On

Coverage Range : 40 meters

* L'activation du port permet au point d'accès de diffuser le signal Wi-Fi. La portée est réglée à 40 mètres pour couvrir la zone cible (bibliothèque).

**Désactivation du serveur DHCP intégré pour éviter les conflits :**

Le serveur DHCP intégré de l'Access Point a été désactivé pour éviter des conflits avec le serveur DHCP principal (routeur).

DHCP Server : Disabled

* Cela permet au routeur de gérer entièrement l’attribution des adresses IP dans le réseau local.

**Configuration du mode bridge pour une intégration au réseau local**

L’Access Point a été configuré en mode bridge pour fonctionner comme une extension du réseau local câblé.

Mode : Bridge

* Le mode bridge permet à l’Access Point de transmettre les requêtes DHCP et de fonctionner comme un relais, intégrant les appareils Wi-Fi directement au réseau local.

**Connexion physique au switch :**

L’Access Point a été connecté physiquement au switch via un port configuré en mode accès.

Switch Port Configuration :

Interface FastEthernet0/6

switchport mode access

* Ce port sur le switch est utilisé pour relier l’Access Point au réseau câblé, permettant la transmission des données entre les appareils Wi-Fi et le réseau local.

Réseau ENGIE

Rappel de ce que l’on dispose :

* 1 routeur
* 25 PC fixes
* 2 switch L2
* 2 bornes Wifi
* 1 serveur DHCP/DNS
* 4 PC portables
* 2 téléphones portables

**Configuration des Switchs**

**Switch 1 (Serveur VTP)**

**Configurer le mode VTP et le domaine :**

Switch1> enable

Switch1# configure terminal

Switch1(config)# vtp mode server

Switch1(config)# vtp domain Engie

Switch1(config)# vtp password cisco

* Ici, on passe en mode serveur VTP, on définit le domaine VTP et on configure un mot de passe pour sécuriser les mises à jour VTP.

**Création des VLANs sur le switch principal :**

Connectez-vous au switch via une console ou SSH et configurez les VLANs.

Switch> enable

Switch# configure terminal

Switch(config)# vlan 10

Switch(config-vlan)# name Technique

Switch(config-vlan)# exit

Switch(config)# vlan 11

Switch(config-vlan)# name Commercial

Switch(config-vlan)# exit

Switch(config)# vlan 12

Switch(config-vlan)# name Wifi-invites

Switch(config-vlan)# exit

* Création des trois VLANs (10,11,12) et attribution d’un nom pour chaque VLANs, ici Technique, Commercial, Wifi-invites.

**Switch 2 (client VTP)**

**Configurer le mode VTP et le domaine :**

Switch2> enable

Switch2# configure terminal

Switch2(config)# vtp mode client

Switch2(config)# vtp domain Engie

Switch2(config)# vtp password cisco

**Vérification de la configuration VLAN :**

Utiliser une commande qui affichera une liste des VLAN.

Switch(config)#do show vlan brief

* Une liste apparaitra, toutes les VLANs existante sont affichés dans l’ordre. Cela nous permettra également de vérifier si les ports ont bien été affecté aux bonnes VLANs.

**Assignation des ports aux VLANs grâce au mode Access :**

Attribuer les ports du switch aux VLANs correspondants. Sur les deux switchs.

Switch>enable

Switch#config t

Switch(config)#interface fa0/1

Switch(config)#switchport mode access

Switch(config)#switchport access vlan 10

Switch(config)#exit

Switch(config)#

Switch(config)#interface fa0/2

Switch(config)#switchport mode access

Switch(config)#switchport access vlan 11

Switch(config)#exit

* Ici, on relie les ports (FastEthernet 0/1…) a la VLAN qui correspond. L’exemple ci-dessus fonctionne pour les ports Fa0/1 et Fa0/2.

**Sauvegarder l’état des VLANs :**

On utilise ici deux commandes pour sauvegarder les VLANs.

Switch#write

Switch#copy running-config startup-config

* Elles sont conseillées d’être utilisé après chaque mise à jour des VLAN sur le switch, cela permettra d’éviter tout problème.

**Configuration en mode trunk :**

On utilise la commande ci-dessous pour mettre un port en mode trunk.

Switch>enable

Switch#config t

Switch(config)#interface gig0/1

Switch(config)#switchport mode trunk

Switch(config)#switchport trunk allowed vlan all

Switch(config)#exit

**Configuration des interfaces VLAN sur le switch 1 :**

Switch(config)# interface vlan 10

Switch(config-if)# ip address 192.168.10.0 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# interface vlan 11

Switch(config-if)# ip address 192.168.11.0 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# interface vlan 12

Switch(config-if)# ip address 192.168.12.0 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

**Configurer les interfaces VLAN sur Switch 2 :**

Les interfaces VLAN seront automatiquement configurées via VTP.

**Vérifier l'état du VTP :**

Switch# show vtp status

**Vérifier les trunks :**

Switch# show interfaces trunk

**Configuration du routeur**

**Configurer les sous-interfaces pour chaque VLAN sur l'interface connectée aux switchs (fa0/1) :**

**VLAN 10 :**

Router(config)# interface fa0/1.10

Router(config-subif)# encapsulation dot1Q 10

Router(config-subif)# ip address 192.168.10.1 255.255.255.0

Router(config-subif)# no shutdown

Router(config-subif)# ip helper-address 192.168.0.226

Router(config-subif)# exit

**VLAN 11 :**

Router(config)# interface fa0/1.11

Router(config-subif)# encapsulation dot1Q 11

Router(config-subif)# ip address 192.168.11.1 255.255.255.0

Router(config-subif)# no shutdown

Router(config-subif)# ip helper-address 192.168.0.226

Router(config-subif)# exit

**VLAN 12 :**

Router(config)# interface fa0/1.12

Router(config-subif)# encapsulation dot1Q 12

Router(config-subif)# ip address 192.168.12.1 255.255.255.0

Router(config-subif)# no shutdown

Router(config-subif)# ip helper-address 192.168.0.226

Router(config-subif)# exit

**Vérifier les sous-interfaces sur le routeur :**

Router# show ip interface brief

Router# write memory

**Configuration du Serveur DHCP :**

**Pour configurer l'adresse IP du serveur :**

1. Il faut cliquer sur le serveur, puis aller dans l'onglet "Config".
2. Sélectionné "Interface" et configurer l'adresse IP 192.168.0.226 avec le masque de sous-réseau 255.255.255.0.
3. Mettre l’adresse IP 192.168.0.254 (l’adresse IP du routeur sur le port fa0/2) comme passerelle par défaut.

**Pour activer le service DHCP :**

1. Dans l'onglet "Services", sélectionner "DHCP".
2. Activer le service DHCP en cliquant sur le bouton "On".
3. Configurer les pools DHCP pour chaque VLAN.

**Configuration des pool DHCP :**

**VLAN 10 :**

Router(config)#ip dhcp pool VLAN10

Router(config-subif)# network 192.168.10.0 255.255.255.0

Router(config-subif)# default-router 192.168.10.1

Router(config-subif)# dns-server 192.168.0.226

Router(config-subif)# exit

**VLAN 11 :**

Router(config)#ip dhcp pool VLAN11

Router(config-subif)# network 192.168.11.0 255.255.255.0

Router(config-subif)# default-router 192.168.11.1

Router(config-subif)# dns-server 192.168.0.226

Router(config-subif)# exit

**VLAN 12 :**

Router(config)#ip dhcp pool VLAN12

Router(config-subif)# network 192.168.12.0 255.255.255.0

Router(config-subif)# default-router 192.168.12.1

Router(config-subif)# dns-server 192.168.0.226

Router(config-subif)# exit

**Configuration des PC pour utiliser DHCP**

Dans l'onglet "Desktop" de chaque PC, sélectionner « IP Configuration" et cocher "DHCP".

Configuration de SSH sur le Routeur

**Configurer le nom d'hôte et le domaine IP :**

Router> enable

Router# configure terminal

Router(config)# hostname Router\_Engie

Router(config)# enable secret cisco

Router(config)# ip domain-name Engie

* Ici, on configure le nom d'hôte et le domaine IP pour le routeur.

**Générer les clés RSA pour SSH :**

Router(config)# crypto key generate rsa

Router(config)# ip ssh version 2

* Ici, on génère des clés RSA pour sécuriser les connexions SSH.

**Configuration AAA (Authentication, Authorization, and Accounting) :**

Router(config)# aaa new-model

Router(config)# aaa authentication login default local

* Ici, on configure AAA pour renforcer la sécurité et la gestion des accès.

**Configurer les lignes VTY pour utiliser SSH :**

Router(config)# line vty 0 4

Router(config-line)# transport input ssh

Router(config-line)# aaa authentication login default local

* Ici, on configure les lignes VTY pour utiliser SSH et AAA.

**Créer un utilisateur avec des privilèges élevés :**

Router(config)# username admin privilege 15 secret cisco

* Ici, on crée un utilisateur avec des privilèges élevés pour l'administration du routeur.

**Sécuriser le port console :**

Router(config)# line console 0

Router(config-line)# password cisco

Router(config-line)# end

* Ici, on sécurise le port console pour empêcher les accès non autorisés.

**Enregistrer la configuration :**

Router# write memory

* Ici, on sauvegarde la configuration dans la mémoire non volatile.

Réseau DIGIPLEX

Rappel du matériel disponible :

* 1 routeur
* 15 PC fixes
* 3 switchs L2
* 2 switchs L3
* 4 bornes Wifi
* 3 serveurs dédiés
* 5 PC portables

RDC

**Configuration du Switch L3 au RDC (DIGI\_SWL3\_RDC)**

**Configuration des VLANs avec le VTP :**

Pour gérer les VLANs de façon centralisée, le switch L3 a été configuré en **serveur VTP** avec le domaine **DIGIPLEX** et un mot de passe pour sécuriser les échanges.

configure terminal

hostname DIGI\_SWL3\_RDC

vtp mode server

vtp domain DIGIPLEX

vtp password securepass

* exit
* Les VLANs ont été créés localement sur ce switch.

configure terminal

vlan 10

name Conception

vlan 20

name Commercial

vlan 30

name Ressources\_Humaine

vlan 40

name Hotline

vlan 50

name Wifi\_Enterprise

vlan 60

name Wifi\_Invites

vlan 70

name Server

vlan 80

name Management

exit

**Configuration des trunks pour transporter les VLANs :**

Des trunks ont été configurés pour permettre la communication entre les switches du RDC et avec le routeur.

interface FastEthernet0/1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

interface FastEthernet0/2

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

**Configuration du VLAN de management :**

Une adresse IP a été attribuée au VLAN 80 pour permettre la gestion à distance du switch via SSH.

interface vlan 80

ip address 192.168.80.1 255.255.255.0

no shutdown

exit

ip domain-name DIGIPLEX.local

crypto key generate rsa

1024

line vty 0 4

transport input ssh

login local

exit

username admin privilege 15 secret strongpassword

**Configuration des Switchs L2 au RDC**

**Configuration des VLANs avec le VTP :**

Les deux switches L2 du RDC ont été configurés en **mode client VTP** pour synchroniser automatiquement les VLANs créés sur le switch L3.

**Commandes (sur chaque switch L2) :**

Configure terminal

hostname DIGI\_SWL2\_RDC\_X # Remplacez "X" par 01 ou 02

vtp mode client

vtp domain DIGIPLEX

vtp password securepass

Exit

**Configuration des trunks :**

Des trunks ont été configurés pour permettre la communication entre chaque switch L2 et le switch L3.

interface FastEthernet0/1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

**Configuration du Routeur (DIGI\_ROUTER)**

**Configuration des sous-interfaces pour le routage inter-VLAN :**

Des sous-interfaces ont été créées pour chaque VLAN afin de permettre la communication inter-VLAN. Chaque sous-interface a reçu une adresse IP correspondant à la passerelle de son VLAN.

interface FastEthernet0/1.10

encapsulation dot1q 10

ip address 192.168.10.1 255.255.255.0

interface FastEthernet0/1.20

encapsulation dot1q 20

ip address 192.168.20.1 255.255.255.0

interface FastEthernet0/1.30

encapsulation dot1q 30

ip address 192.168.30.1 255.255.255.0

interface FastEthernet0/1.40

encapsulation dot1q 40

ip address 192.168.40.1 255.255.255.0

**Configuration du NAT pour l'accès Internet :**

Le NAT a été configuré pour permettre aux VLANs d'accéder à Internet via l'interface WAN.

interface FastEthernet0/0

ip address 68.101.36.129 255.255.255.0

ip nat outside

no shutdown

interface FastEthernet0/1

ip nat inside

no shutdown

ip nat inside source list 1 interface FastEthernet0/0 overload

access-list 1 permit 192.168.0.0 0.0.255.255

**Configuration du DHCP :**

Le routeur a été configuré pour fournir des adresses IP dynamiques aux clients des différents VLANs.

ip dhcp excluded-address 192.168.10.1 192.168.10.10

ip dhcp pool VLAN10

network 192.168.10.0 255.255.255.0

default-router 192.168.10.1

dns-server 192.168.70.3

ip dhcp excluded-address 192.168.20.1 192.168.20.10

ip dhcp pool VLAN20

network 192.168.20.0 255.255.255.0

default-router 192.168.20.1

dns-server 192.168.70.3

**Switch L3 (DIGI\_SWL3\_RDC)**

Le switch L3 du RDC est le cœur du réseau. Il gère les VLANs en tant que serveur VTP et assure la communication entre les différents VLANs via des trunks et son interconnexion avec le routeur. Il est aussi configuré pour permettre une gestion sécurisée grâce à une IP sur le VLAN 80 et l'accès SSH.

**Switch L2 Principal (DIGI\_SWL2\_RDC\_01)**

Ce switch est connecté au switch L3 et synchronise les VLANs via VTP en mode client. Il transporte les données des VLANs grâce aux trunks configurés avec le switch L3 et les autres switches du RDC.

**Switch L2 Secondaire (DIGI\_SWL2\_RDC\_02)**

Le second switch L2 fonctionne de manière similaire au premier. Il est configuré pour recevoir les VLANs via VTP et permet la communication avec les autres équipements du RDC grâce à ses trunks.

**Routeur (DIGI\_ROUTER)**

Le routeur connecte le réseau interne au monde extérieur en gérant l'accès Internet grâce au NAT. Il permet également le routage inter-VLAN grâce à ses sous-interfaces configurées pour chaque VLAN et fournit des adresses IP dynamiques via DHCP.

ETAGE 1

À l'étage 1, nous avons configuré un switch principal (level 2) et deux switches secondaires pour permettre la communication entre les VLANs et garantir une redondance grâce à l'agrégation de liens. Le but est d'assurer une gestion centralisée des VLANs tout en permettant un accès distant via SSH pour la maintenance.

**Synchronisation VTP et configuration des VLANs pour centralisation :**

configure terminal

hostname DIGI\_SWL2\_E1\_01

vtp mode client

vtp domain DIGIPLEX

vtp password securepass

exit

* Cette configuration met en place la synchronisation avec le domaine VTP pour recevoir automatiquement les VLANs depuis le switch L3 au RDC. En mode client, ce switch ne peut pas créer de VLANs localement, ce qui garantit une gestion centralisée des modifications via le serveur VTP du RDC.

**Configuration des trunks pour transporter les VLANs :**

interface FastEthernet0/1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

interface FastEthernet0/2

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

interface FastEthernet0/3

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

* Les trunks configurés permettent au switch principal de transporter les données des VLANs entre le routeur et les switches secondaires de l'étage. Chaque port est configuré pour transporter tous les VLANs (10, 20, ..., 80).

interface FastEthernet0/12

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

**Configuration de l’agrégation de liens (EtherChannel) :**

interface Port-channel1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

interface FastEthernet0/4

channel-group 1 mode active

interface FastEthernet0/5

channel-group 1 mode active

exit

* Pour améliorer la redondance et la bande passante, deux liens physiques (FastEthernet0/4 et FastEthernet0/5) ont été agrégés en un seul lien logique appelé Port-Channel 1. Cela garantit que si un lien tombe, le second prend automatiquement le relais.

**Configuration du VLAN de management pour accès distant :**

interface vlan 80

ip address 192.168.80.2 255.255.255.0

no shutdown

exit

ip domain-name DIGIPLEX.local

crypto key generate rsa

1024

line vty 0 4

transport input ssh

login local

exit

username admin privilege 15 secret strongpassword

* Le VLAN 80 est utilisé pour la gestion du switch. Une adresse IP statique (192.168.80.2) est attribuée, et le protocole SSH est activé pour sécuriser l’accès distant.

Ces configurations permettent au switch principal de l’étage 1 de recevoir les VLANs via le VTP, de transporter les données entre les équipements grâce aux trunks, et de permettre une gestion à distance via SSH. L’agrégation de liens ajoute de la redondance, ce qui améliore la résilience du réseau.

**Configuration des trunks pour les switchs secondaires :**

Pour les switches secondaires de l'étage 1, nous avons ouvert les ports en mode trunk, activé l'encapsulation **802.1q** et autorisé tous les VLANs à passer. Cela permet de transporter les données inter-VLAN entre le switch principal et les secondaires pour garantir une communication fluide.

interface FastEthernet0/1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

* Ces trunks assurent que les VLANs définis au niveau du switch principal et du routeur sont accessibles sur tous les équipements de l'étage, permettant une communication inter-VLAN efficace.

ETAGE 2

À l'étage 2, nous avons configuré un switch principal et deux switches secondaires pour permettre la synchronisation des VLANs via VTP, l'acheminement des données inter-VLAN à travers les trunks, et la redondance via l'agrégation de liens. L'objectif est de garantir la continuité du réseau tout en centralisant la gestion des VLANs.

**Synchronisation VTP et configuration des VLANs pour centralisation :**

configure terminal

hostname DIGI\_SWL2\_E2\_01

vtp mode client

vtp domain DIGIPLEX

vtp password securepass

exit

* Le switch principal de l'étage 2 est configuré en mode **client VTP** pour synchroniser automatiquement les VLANs depuis le serveur VTP du RDC. Cette configuration garantit que les VLANs sont cohérents sur tout le réseau et évite les modifications locales qui pourraient perturber la centralisation.

**Configuration des trunks pour transporter les VLANs :**

interface FastEthernet0/1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

interface FastEthernet0/2

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

interface FastEthernet0/3

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

* Les trunks permettent de transporter tous les VLANs définis (10, 20, ..., 80) entre le routeur, le switch principal et les secondaires de l'étage 2. Chaque lien est configuré pour prendre en charge l'encapsulation **802.1q**.

**Configuration de l’agrégation de liens (EtherChannel) :**

interface Port-channel1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

interface FastEthernet0/4

channel-group 1 mode active

interface FastEthernet0/5

channel-group 1 mode active

exit

* L’agrégation de liens est configurée pour améliorer la résilience et la bande passante entre le switch principal et les secondaires. Les ports **FastEthernet0/4** et **FastEthernet0/5** sont regroupés pour former un lien logique.

**Configuration du VLAN de management pour accès distant :**

interface vlan 80

ip address 192.168.80.3 255.255.255.0

no shutdown

exit

ip domain-name DIGIPLEX.local

crypto key generate rsa

1024

line vty 0 4

transport input ssh

login local

exit

username admin privilege 15 secret strongpassword

* Le VLAN 80 est configuré pour permettre la gestion distante du switch principal via SSH. Une adresse IP statique (192.168.80.3) est attribuée à l’interface VLAN 80 pour garantir un accès sécurisé et efficace.

**Configuration des switches secondaires :**

Pour les switches secondaires, les ports connectés au switch principal sont configurés en mode trunk, avec encapsulation **802.1q**, pour transporter les VLANs.

interface FastEthernet0/1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

* Les trunks configurés sur les switches secondaires assurent que les données des VLANs définis au niveau principal circulent efficacement à travers tout l'étage.

interface FastEthernet0/2

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

ETAGE 3

À l'étage 3, nous avons configuré un switch principal et deux switches secondaires pour garantir la synchronisation des VLANs avec le réseau global via VTP, le transport des données entre les VLANs grâce aux trunks, et la redondance par l'agrégation de liens. L'objectif est d'assurer une gestion efficace du réseau et une continuité de service.

**Synchronisation VTP et configuration des VLANs pour centralisation :**

configure terminal

hostname DIGI\_SWL2\_E3\_01

vtp mode client

vtp domain DIGIPLEX

vtp password securepass

exit

* Le switch principal de l'étage 3 est configuré en **client VTP** pour recevoir les VLANs depuis le serveur VTP situé au RDC. Cette configuration garantit que les VLANs sont correctement propagés à l'ensemble des équipements du réseau et empêche toute modification locale non souhaitée.

**Configuration des trunks pour transporter les VLANs :**

interface FastEthernet0/1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

interface FastEthernet0/2

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

interface FastEthernet0/3

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

* Les trunks configurés sur le switch principal permettent de transporter tous les VLANs définis (10, 20, ..., 80) entre le routeur, le switch principal et les secondaires. L'encapsulation **802.1q** est utilisée pour prendre en charge plusieurs VLANs sur un seul lien physique.

**Configuration de l’agrégation de liens (EtherChannel) :**

interface Port-channel1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

interface FastEthernet0/4

channel-group 1 mode active

interface FastEthernet0/5

channel-group 1 mode active

exit

* L'agrégation de liens permet d'améliorer la résilience et la bande passante entre le switch principal et les secondaires. Les ports **FastEthernet0/4** et **FastEthernet0/5** sont agrégés pour former un lien logique unique (Port-Channel 1).

**Configuration du VLAN de management pour accès distant :**

interface vlan 80

ip address 192.168.80.4 255.255.255.0

no shutdown

exit

ip domain-name DIGIPLEX.local

crypto key generate rsa

1024

line vty 0 4

transport input ssh

login local

exit

username admin privilege 15 secret strongpassword

* Le VLAN 80 est configuré pour permettre une gestion distante et sécurisée du switch principal via SSH. Une adresse IP statique (192.168.80.4) est attribuée à l'interface VLAN 80 pour garantir un accès sécurisé.

**Configuration des switchs secondaires :**

Les switches secondaires sont configurés pour transporter les VLANs via des trunks reliant le switch principal. Cette configuration garantit que les données des VLANs circulent efficacement à travers tout l'étage.

interface FastEthernet0/1

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

No shutdown

* Les ports configurés en trunks sur les switches secondaires assurent une connectivité cohérente entre les VLANs de l'étage 3 et les autres étages.

interface FastEthernet0/10

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan all

no shutdown

Réseau DATACENTER

Le matériel disponible est le suivant :

* 1 serveur Meraki hébergé dans le cloud
* 1 routeur
* Plusieurs postes clients connectés

Dans un premier temps on va mettre en place OSPF afin de relier tous les routeurs car ils sont tous reliés au DSLAM.

**Sur le routeur DSLAM :**

Enable

Configure terminal

router OSPF 1

network 131.50.62.245 0.0.0.255 area 0

network 10.0.0.254 0.0.0.255 area 0

network 68.101.36.129 0.0.0.255 area 0

network 45.80.255.33 0.0.0.255 area 0

Exit

Avec dans l’ordre eXia, la BIBLIOTHEQUE, DIGIPLEX et enfin ENGIE.

**Chez eXia :**

Enable

Configure terminal

Router OSPF 1  
network 131.50.62.254 0.0.0.255 area 0

Exit

**Chez BIBLIOTHEQUE :**

Enable

Configure terminal

router OSPF 1

network 10.0.0.254 0.0.0.255 area 0

Exit

**Chez DIGIPLEX :**

Enable

Configure terminal

router OSPF 1

network 68.101.36.254 0.0.0.255 area 0

exit

**Chez ENGIE :**

Enable

Configure terminal

router OSPF 1

network 45.80.255.254 0.0.0.255 area 0

exit

Ensuite il faut active l’OSPFv3 sur chacun des routeurs FAI du datacenter :

**Sur le FAI RT 01, on le met sur les ports FastEthernet0/0, Serial0/0/0 et Serial0/0/1 :**

ip cef

ipv6 unicast-routing

ipv6 cef  
interface FastEthernet0/0

ipv6 address 2001:DB8:6000::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

interface Serial0/0/0

ipv6 address 2001:DB8:A000::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

interface Serial0/0/1

ipv6 address 2001:DB8:8000::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

ipv6 router OSPF 1

router-id 3.3.3.3

end

copy running-config startup-config

**Sur le FAI RT 02, on le met sur les ports FastEthernet0/0, Serial0/0/0, Serial0/0/1 :**

ip cef

ipv6 unicast-routing

ipv6 cef  
interface FastEthernet0/0

ipv6 address 2001:DB8:6000::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit  
interface Serial0/0/0

ipv6 address 2001:DB8:A000::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit  
interface Serial0/0/1

ipv6 address 2001:DB8:8000::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

ipv6 router OSPF 1

router-id 3.3.3.3

exit

exit

copy running-config startup-config

**Sur le FAI RT 03, on le met sur les ports Serial0/0/0, Serial0/0/1, Serial0/1/0 :**

ip cef

ipv6 unicast-routing

ipv6 cef

interface Serial0/0/0

ipv6 address 2001:DB8:E000::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

interface Serial0/0/1

ipv6 address 2001:DB8:B000::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

interface Serial0/1/0

ipv6 address 2001:DB8:C000::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

ipv6 router OSPF 1

router-id 5.5.5.5

exit

exit

copy running-config startup-config

**Sur le FAI RT 04, on le met sur les ports Serial0/0/0, Serial0/0/1, Serial0/1/0 :**

ip cef

ipv6 unicast-routing

ipv6 cef

interface Serial0/0/0

ipv6 address 2001:DB8:E100::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit  
interface Serial0/0/1

ipv6 address 2001:DB8:A600::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

interface Serial0/1/0

ipv6 address 2001:DB8:A700::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

ipv6 router OSPF 1

router-id 6.6.6.6

exit

exit

copy running-config startup-config

**Sur le FAI RT 05, on le met sur les ports Serial0/0/0, Serial0/0/1, Serial0/1/0 :**

ip cef

ipv6 unicast-routing

ipv6 cef

interface Serial0/0/0

ipv6 address 2001:DB8:A200::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

interface Serial0/0/1

ipv6 address 2001:DB8:D000::2/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

interface Serial0/1/0

ipv6 address 2001:DB8:A500::1/64

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

ipv6 router OSPF 1

router-id 7.7.7.7

exit

exit copy running-config startup-config

**A présent on configure sur le routeur du réseau eXia le tunnel ainsi que l’OSPFv3 IPv6 :**

ip cef

ipv6 unicast-routing

ipv6 cef

interface Tunnel0

no ip address

mtu 1476

ipv6 address 2001:DB8:3000::1/64

tunnel source GigabitEthernet0/0/0

tunnel destination 90.154.127.203

tunnel mode ipv6ip

exit  
ipv6 route 2001:DB8:1000::1/64 2001:DB8:3000::2

interface FastEthernet0/0

ipv6 address 2001:DB8:2000::1/64

ipv6 enable

ipv6 OSPF 1 area 0

exit

interface GigabitEthernet0/0/0

ipv6 address 2001:DB8:4000::1/64

ipv6 enable

ipv6 OSPF network point-to-point

ipv6 OSPF 1 area 0

exit

ipv6 router OSPF 1

router-id 1.1.1.3

exit

ipv6 route ::/0 2001:DB8:3000::2

exit

copy running-config startup-config

**On va également activement l’OSPFv3 et le tunnel sur le routeur Meraki :**

ip cef

ipv6 unicast-routing

ipv6 cef

interface Tunnel0

no ip address

mtu 1476

ipv6 address 2001:DB8:3000::2/64

tunnel source Serial0/0/0

tunnel destination 131.50.62.245

tunnel mode ipv6ip

exit

interface Serial0/0/0

ipv6 address 2001:DB8:E000::2/64

ipv6 OSPF 1 area 0

exit

interface GigabitEthernet0/2/0

ipv6 address 2001:DB8:1000::1/64

ipv6 OSPF 1 area 0

exit

ipv6 router OSPF 1

router-id 8.8.8.8

exit

ipv6 route ::/0 2001:DB8:3000::1

ipv6 route 2001:DB8:1000::/64 GigabitEthernet0/2/0

exit

copy running-config startup-config

**Maintenant on va sur le DSLAM qui relie tous nos réseaux et on va activer l’OSPFv3 :**

ip cef

ipv6 unicast-routing

ipv6 cef

interface FastEthernet0/0

ipv6 address 2001:DB8:A300::1/64

ipv6 ospf network point-to-point

ipv6 ospf 1 area 0

exit

interface GigabitEthernet0/1/0

ipv6 address 2001:DB8:AB00::1/64

ipv6 ospf network point-to-point

ipv6 ospf 1 area 0

exit

ipv6 router ospf 1

router-id 1.1.1.2

exit

exit

copy running-config startup-config

Enfin, sur le WAN on active également l’OSPFv3 :

ip cef

ipv6 unicast-routing

ipv6 cef

interface GigabitEthernet0/0/0

ipv6 address 2001:DB8:BB00::1/64

ipv6 ospf 1 area 0

exit

interface Serial0/1/0

ipv6 address 2001:DB8:5000::1/64

ipv6 ospf network point-to-point

ipv6 ospf 1 area 0

exit

interface GigabitEthernet0/2/0

ipv6 address 2001:DB8:BA00::1/64

ipv6 ospf 1 area 0

exit

interface FastEthernet1/0

ipv6 address 2001:DB8:A400::1/64

ipv6 ospf network point-to-point

ipv6 ospf 1 area 0

exit

ipv6 router ospf 1

router-id 2.2.2.2

exit

exit

copy running-config startup-config

**Enfin, on active l’OSPFv3 sur le WAN :**

ip cef

ipv6 unicast-routing

ipv6 cef

interface GigabitEthernet0/0/0

ipv6 address 2001:DB8:BB00::1/64

ipv6 ospf 1 area 0

exit

interface Serial0/1/0

ipv6 address 2001:DB8:5000::1/64

ipv6 ospf network point-to-point

ipv6 ospf 1 area 0

exit

interface GigabitEthernet0/2/0

ipv6 address 2001:DB8:BA00::1/64

ipv6 ospf 1 area 0

exit

interface FastEthernet1/0

ipv6 address 2001:DB8:A400::1/64

ipv6 ospf network point-to-point

ipv6 ospf 1 area 0

exit

ipv6 router ospf 1

router-id 2.2.2.2

exit

exit

copy running-config startup-config

Maintenant que l’OSPF est configuré, il est possible que les routes soient déterminées de manière dynamique. Tous les appareils sont désormais interconnectés et il n’y a plus besoin d’autres configurations afin que chacun des sites se connectent l’un à l’autre. L’accès web est également configuré ce qui permet à tous les sites de se connecter au world wide web. Le tunnel fonctionne également afin d’améliorer la réactivité et la sécurisation du lien entre le serveur cloud eXia et l’entreprise.

SCHEMAS LOGIQUES DES RÉSEAUX

Réseau ESN eXia

Une image contenant texte, diagramme, capture d’écran, ligne

Description générée automatiquement

Réseau BIBLIOTHEQUE

Une image contenant diagramme, ligne, capture d’écran

Description générée automatiquement

Réseau ENGIE

Une image contenant capture d’écran, diagramme, ligne, Parallèle

Description générée automatiquement

Réseau DIGIPLEX

Rez-de-chaussée

Une image contenant texte, diagramme, capture d’écran, cercle

Description générée automatiquement

1er étage

Une image contenant texte, diagramme, cercle, capture d’écran

Description générée automatiquement

2ème étage

Une image contenant texte, illustration, conception

Description générée automatiquement

3ème étage

Une image contenant texte, diagramme, Montgolfière, cercle

Description générée automatiquement

Réseau DATACENTER

Une image contenant capture d’écran, ligne

Description générée automatiquement

CONCLUSION

Le livrable 3 marque une étape cruciale dans la concrétisation du projet Funkytown. En élaborant un plan de déploiement détaillé, nous avons mis en place une stratégie claire et optimisée pour l’installation et la configuration des infrastructures réseau sur les cinq sites. Ce plan garantit la continuité des opérations, la minimisation des interruptions et une coordination efficace entre les différents acteurs du projet. Avec des outils comme le diagramme de Gantt et le réseau PERT, nous avons assuré une vision temporelle précise et une gestion rigoureuse des ressources. Cette approche méthodique nous permet d’assurer un déploiement fiable, en respectant les objectifs initiaux de performance, de sécurité et de connectivité pour les entreprises de Funkytown.

ANNEXES TECHNIQUES

Packet Tracer

CCNA