

***Dossier d'Architecture Technique Détaillée  
Projet RSX101***

***2019-2020***

---

**Auteur : Fettache Rachik**

**Résumé**

Ce document « Dossier d'architecture Technique » décrit l'infrastructure d'étude intégration basé sur un modèle hiérarchique en trois couches.

## FICHE D'IDENTIFICATION

### INFORMATION GÉNÉRALES

NOM PROJET	PREPARE PAR	SIGNATURE	DATE CREATION	DOCUMENT ID
INFRA Etude / Intégration				

### INFORMATION DOCUMENT

TITRE	DOMAINE / TYPE
	Réseaux
RÉFÉRENTIEL	
EMETTEUR	
Fettache Rachik	
REFERENCE	
DATE D'EDITION	
VERSION EN COURS	
DATE D'APPLICATION	
CONFIDENTIALITE	
Document propriété de Fettache Rachik	

### APPROBATION

RÉDACTEUR		VÉRIFICATEUR		APPROBATEUR	
Nom		Nom		Nom	
Signature (sur le document original seulement)					

(\*) EN CAS D'ABSENCE D'UNE DES PERSONNES, ??? DEVRA DESIGNER UN REMPLACANT AFIN DE NE PAS IMPACTER LE DELAI DE VALIDATION.

### MISE A DISPOSITION / DISTRIBUTION

ENTITÉ PROJET / DÉPARTEMENT	DESTINATAIRE
Cnam RSX 101	Mr Lantoine

## Historique des versions

<i>Version</i>	<i>Date</i>	<i>Auteurs / Redacteurs</i>	<i>Modification</i>
V0.1	08/12/2019	Fettache rachik	Mise en place
V0.2	15/12/2019		Configuration liaison trunk ,access + tests
V0.3	21/12/2019		Configuration vlan vtp+stp + tests
V0.9	24/12/2019		Configuration dhcp +tests
V0.9	3/01/2020		Configuration hsrp +tests
V0.10	10/01/2020		Configuratin routage +tests
V0.11	17/01/2020		Configuration voip +tests
V0.13	29/01/2020		Tests finaux

## Table des matières

1- Terminologie et conventions utilisées	6
1-1 Terminologie	6
1-2 Abréviations	6
2. Introduction	8
3. Description générale du projet	9
3.1 Contexte	9
3.2 Objectifs	9
3.3 Contraintes et attentes	9
4- Architecture générale	10
4-1 Liste des équipements	10
4-1-1 Routeur	10
4-1-2 Switchs cœurs de réseau	10
4-1-3 Switches couche distribution	10
4-1-4 Switchs / access	10
4-1-5 Equipements Terminaux	10
4-2-Paramètres globaux	11
4-2-1 Définition des vlans	11
4-2-2 Définition Réseaux entre les switchs cœurs et routeur	11
4-3 Préparation des équipements	11
4-3-1 Nommer les équipements	11
4-3-2 Interconnexions	12
4-3-3 Sécuriser l'accès à l'IOS cisco	12
5- Architecture détaillée	13
5-1 Présentation de la topologie	13
5-2 Configuration des switchs	13
5-2-1 Sauvegarder les configurations	13
5-2-2 Configuration des vlans	13
5-2-3 Configuration : Trunk	14
5-2-4 Configuration des ports access	16
5-2-5 Configurer des interfaces virtuelles	16
5-3 Mise en place du Protocole VTP	17
5-3-1 Explication du protocole	17
5-3-2 Fonctionnement	17
5-3-3 Configuration vtp	17
5-3-4 Vérification de la prise en compte du protocole vtp	18
5-4 Configuration du Spanning-tree STP	20
5-4-1 Explication du protocole	20
5-4-2 Configuration du protocole	20
5-4-3 Vérifications et tests	21
5-5 Mise en place du protocole DHCP	21
5-5-1 Configuration DHCP	21
5-5-2 Vérification du fonctionnement DHCP	22
5-6 Mise en place du protocole HSRP	23
5-6-1 Principes de HSRP	23
5-6-2 Configuration HRSP	23
5-6-3 Tests et vérifications du fonctionnement	24
5-7 Mise en place du routage	25
5-7-1 Configuration du routage statique	25
5-7-2 Vérification du fonctionnement et tests	27

5-8 Mise en place de La VOIP	28
5-8-1-Configuration de la VOIP	28
5-8-2 Vérifications et tests de fonctionnement	30
5-9 Tests finaux	31
6 Analyse conclusion	33

---

# 1- Terminologie et conventions utilisées

---

## 1-1 Terminologie

ACL : Liste qui permet de filtrer les paquets suivant des critères définis par l'utilisateur.

Commutateur (Switch) : Equipement réseau permettant l'interconnexion d'équipements informatique afin qu'ils puissent communiquer.

Cisco packet tracer : Simulateur de matériel réseau Cisco (routeurs, commutateurs).

IP : Adresse unique attribuée à chaque équipement d'un réseau.

Load Balancer : Technique permettant de répartir la charge entre les différents équipements d'un même groupe.

Firewall (pare-feu) : Système de sécurité permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un autre réseau.

Firmware : logiciel stocké sur un support physique (mémoire morte) d'un appareil électronique et qui permet de le faire fonctionner.

Protocole : Méthode standard ou commune qui permet la communication entre des processus, c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

Réseau : Ensemble des moyens matériels et logiciels mis en œuvre pour assurer les communications entre les différents équipements informatiques.

Routage : Mécanisme qui permet aux données d'un équipement expéditeur d'être acheminées jusqu'à leur destinataire.

Routeur : Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets.

Sauvegarde : Opération qui consiste à copier des données sur un autre support afin qu'il soit possible de les récupérer en cas de problème.

Serveur : Ordinateur qui met ses ressources à la disposition d'autres ordinateurs sous la forme de services.

VIP : Adresse IP virtuelle qui peut être attribué à plusieurs équipements du même type afin de redonder la connexion ou de faire du load balancing.

VLAN : Réseau logique indépendant, permettant la communication entre des équipements, connectés sur le même LAN, comme s'ils se trouvaient sur le même réseau local physique.

## 1-2 Abréviations

- **CME**: Call Manager Express
- **DAT**: Document d'Architecture Détaillée
- **DHCP**: Dynamic Host Configuration Protocol
- **DTP : Dynamic Trunking Protocol**
- **E/I** : Etude / Intégration
- **FHRP** : First Hop Routing Protocol
- **IP** : Internet Protocol

- **LAN** : Local Area Network
- **L2** : Layer 2 (couche OSI niveau 2)
- **L3** : Layer 3 (couche OSI niveau 3)
- **SSH** : Secure Shell
- **STP**: Spanning Tree Protocole
- **SVI** : Switch VLAN Interface
- **VLAN**: Virtual Local Area Network ou Virtual LAN
- **VOIP**: Voice over Internet Protocol
- **VIP** : Virtual IP
- **VRRP**: Virtual Router Redundancy Protocol)

---

## 2. Introduction

---

Ce document représente le dossier d'architecture technique (DAT) pour la mise en place d'une architecture réseau. Celle-ci se base sur un modèle appelé « Modèle hiérarchique en 3 couches » ou dénommé dans sa version anglaise « tree-layers hierarchical internetworking design/model », ce modèle a été inventé et diffusé par Cisco. Le fondement de ce modèle est de créer un réseau structuré en 3 couches :

- Couche cœur ou « Core Layer » : Ici, son rôle est de relier les différents réseaux entre eux, on y trouve en général des routeurs ou des switchs de niveau 3. On la dénomme aussi backbone du réseau. Elle doit transférer les données le plus rapidement possible et apporte la connexion à des réseaux externes (MAN ou WAN).
- Couche distribution ou « Distribution layer » : Son rôle est de limiter les zones de broadcast, router les données entre vlan et éviter que certaines données transitent vers certains vlans.
- Couche acces : c'est la dernière couche du modèle. Son rôle est simple mais très important : connecter les périphériques terminaux au réseau.

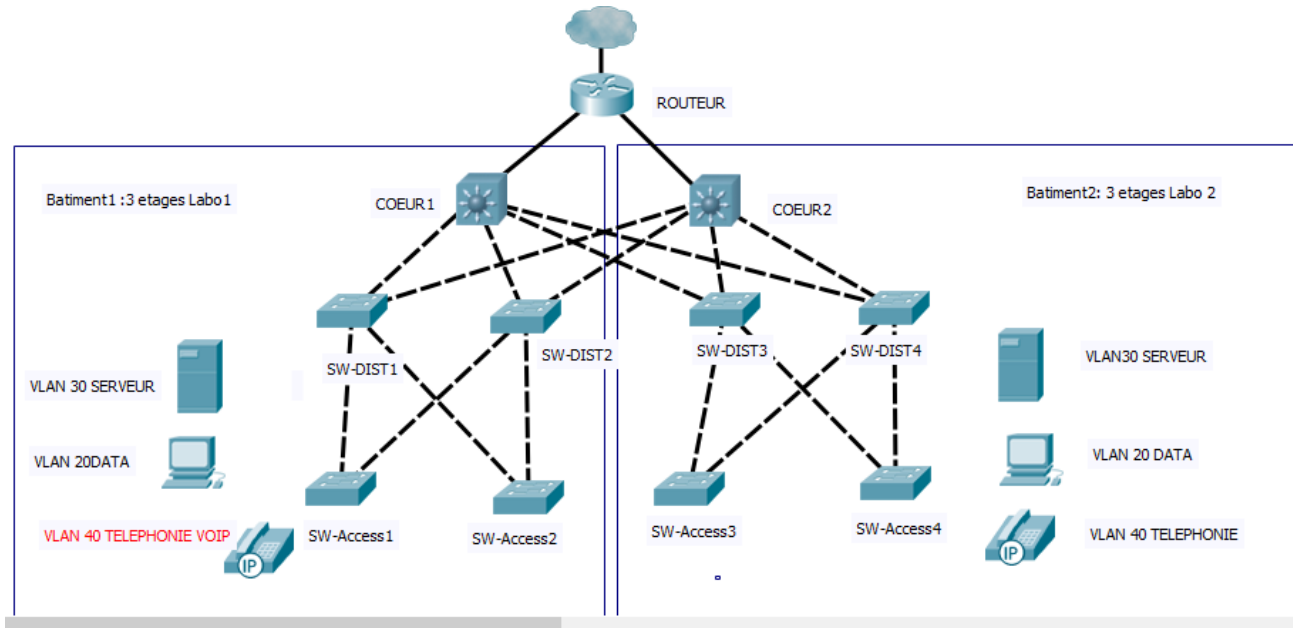
Ce DAT décrit la façon dont cette architecture a été mise en place ainsi que les différentes phases de configuration et de tests afin de s'assurer que le tout soit fonctionnelle. Il mettra en avant la fiabilité des réseaux qui doit par exemple être tolérant aux pannes et donc assurer une continuité de services, celle-ci se réalise par de la redondance qui consiste à doubler les équipements critiques ou doubler les liens vers ces équipements.



## 3. Description générale du projet

### 3.1 Contexte

L'architecture du projet se base sur le schéma suivant :



### 3.2 Objectifs

A partir de cette architecture réseau, l'idée est de réaliser avec un logiciel de simulation tel que cisco packet tracer une topologie qui permettra d'interconnecter les labos 1 et 2. On créera ainsi différents vlans pour que chaque équipement terminal puisse communiquer avec les différents équipements appartenant à son vlan mais aussi assurer du routage intervlan

### 3.3 Contraintes et attentes

L'objectif est de mettre en place une redondance au niveau des switchs afin d'assurer un service continu et d'utiliser des protocoles adéquats. Une panne d'un équipement par exemple ne doit pas empêcher cette continuité de service et permettre ainsi à tout utilisateur de pouvoir utiliser le réseau sans impact négatif dans ses fonctions.

Pour répondre à ces objectifs, il faudra utiliser afin de faciliter le travail des protocoles comme VTP pour propager les vlans, HSRP pour faire du load balancing et le protocole Spanning-tree pour éviter les boucles réseaux et ainsi optimiser le réseau. Il y aura également la configuration du protocole DHCP pour assurer la distribution des adresses IP aux équipements terminaux.

---

## 4- Architecture générale

---

### 4-1 Liste des équipements

#### **4-1-1 Routeur**

- Cisco cisco 2811
- rôle : servira d'accès au wan et la mise en place Voip
- 2 FastEthernet, Wan, console
- quantité : 1

#### **4-1-2 Switchs cœurs de réseau**

- cisco WS-C3560-24PS
- switch de niveau 3, 24 ports FastEthernet, port console, joueront aussi le rôle de routeur.
- quantite :2

#### **4-1-3 Switches couche distribution**

- Cisco WS-C2960-24TT
- SWITCH De niveau 2,24 ports FastEthernet, port console
- Quantite :4

#### **4-1-4 Switchs / access**

- Cisco WS-C2960-24TT
- SWITCH De niveau 2 ,24 ports FastEthernet, port console
- Quantite :4

#### **4-1-5 Equipements Terminaux**

Serveurs, ordinateurs , téléphone voip 7960 (fonctionne comme un switch)

## 4-2-Paramètres globaux

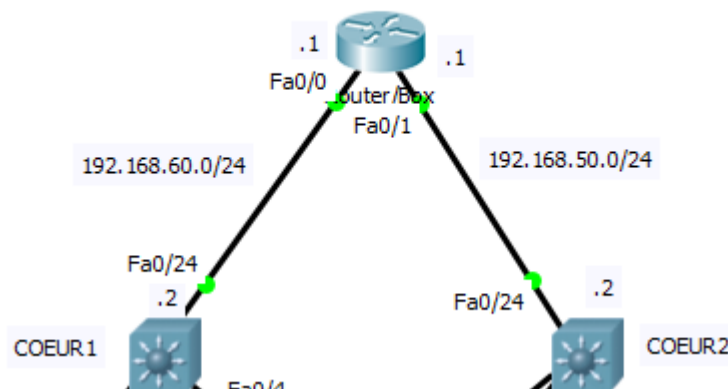
### 4-2-1 Définition des vlans

Je vais définir 4 vlans pour le réseau :

Vlan Id	Reseau	Description
10	192.168.1.0/24	administrateur
20	192.168.2.0/24	data
30	192.168.3.0/24	serveur
40	192.168.4.0/24	Telephone

### 4-2-2 Définition Réseaux entre les switches cœurs et routeur

Je vais également définir des réseaux du côté du routeur/box et des Switchs COEUR1 et 2 :



## 4-3 Préparation des équipements

### 4-3-1 Nommer les équipements

Par défaut, les équipements ont un nom qui ne donnent pas nécessairement une visibilité quand a leur fonction. Il est ainsi utile de renommer les équipements qui se fait e, CLI et en utilisateur privilégié. Ci-dessous, un exemple de la commande :

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname COEUR2
COEUR2(config)#
```

---

### 4-3-2 Interconnexions

Pour relier les différents équipements afin d'assurer la communication, il y a 2 types de cablages torsadés qui ont été utilisés :

- Cable droit : relier des 2 équipements de natures différentes utilisé pour les périphériques terminaux tels que les serveurs et ordinateurs
- Cable croisé : pour relier des équipements de même nature utilisé pour relier les switches entre eux.

### 4-3-3 Sécuriser l'accès à l'IOS cisco

Il faut sécuriser l'accès à l'ios pour éviter le piratage, il est possible de définir un mot de passe pour accéder aux équipements cisco. En effet la commande pour passer en mode privilège « enable » permet de faire beaucoup de choses sur les équipements (effacer fichiers, changer configuration).

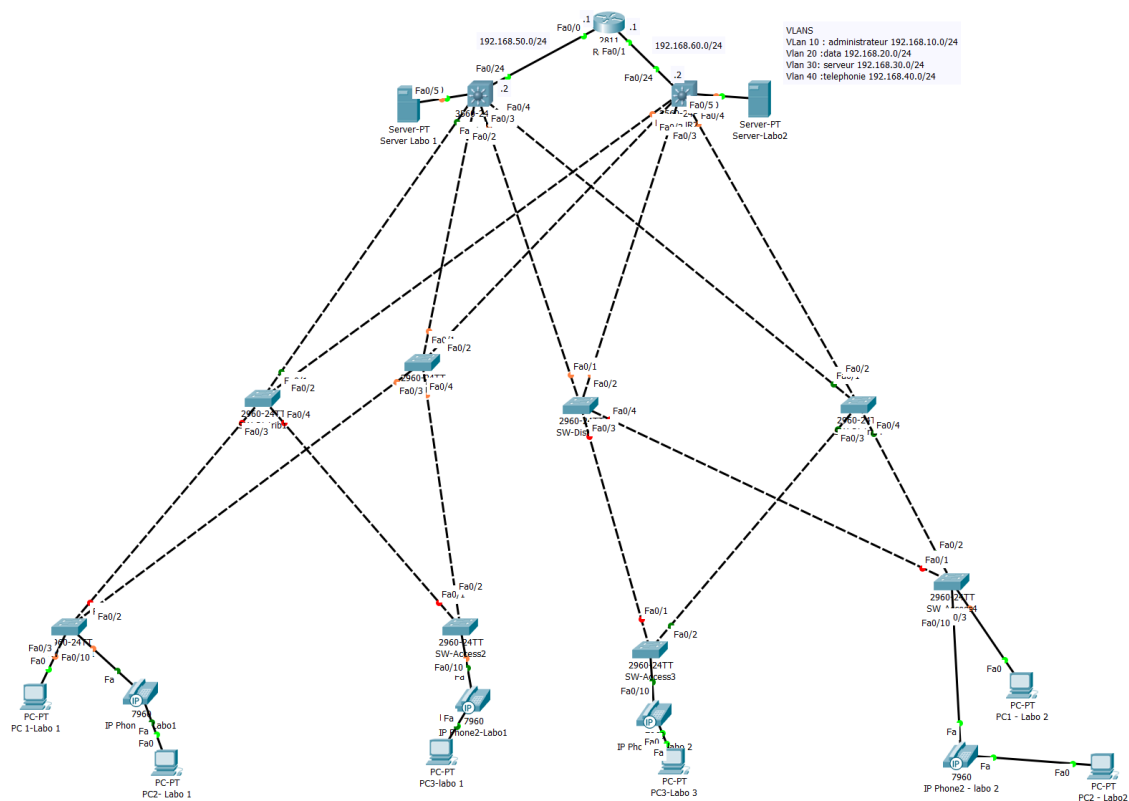
Même si cela n'a pas été fait pour des raisons pratiques ce n'est pas une étape à négliger.

Pour définir un mot de passe : on rentre en mode privilégié, puis en configuration terminal « configure terminal » et on entre la commande « enable password motdepasse ». On peut également ajouter une couche de sécurité en utilisant la fonction « service password-encryption » afin de crypter les mots de passe.

Il faut également sécuriser l'accès au port com des différents équipements, ceci se réalise par l'activation d'un mot de passe quand on souhaite accéder au port en mode console.

## 5- Architecture détaillée

### 5-1 Présentation de la topologie



### 5-2 Configuration des switches

#### 5-2.1 Sauvegarder les configurations

La configuration appelée startup-config est la configuration utilisée au démarrage du switch. La configuration dite running-config est la configuration courante utilisée par le switch. Si une modification de configuration est réalisée, la running-config sera modifiée. Par contre, la startup-config ne sera pas modifiée. Pour modifier la configuration de démarrage, il faudra enregistrer la configuration courante (running-config) dans la startup-config.

```
COEUR1#copy running-config start
COEUR1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

#### 5-2-2 Configuration des vlans

Chaque vlan correspondant à un sous réseau, je choisirai le numéro du vlan par rapport à l'adresse du réseau et ensuite je vais leur donner un nom :

```
COEUR1(config)#vlan 10
COEUR1(config-vlan)#name administration
COEUR1(config-vlan)#vlan 20
COEUR1(config-vlan)#name data
COEUR1(config-vlan)#vlan 30
COEUR1(config-vlan)#name serveur
COEUR1(config-vlan)#vlan 40
COEUR1(config-vlan)#name telephonie
COEUR1(config-vlan)#exit
```

## **Vlan d'administration**

Les vlans permettent de segmenter le réseau, de définir des domaines broadcast et de le sécuriser. Lorsqu'on se connecte à un équipement depuis l'utilitaire cisco packet tracer, il s'agit d'une simulation d'une connexion physique, mais en réalité il faudra prendre le contrôle à distance via telnet ou ssh par exemple.

C'est à partir de là qu'on trouve l'utilité primordiale d'un vlan administration en le configurant via des interfaces virtuelles pour l'administration. On créera donc des interfaces virtuelles et des routes permettant d'accéder aux différents vlans en leur donnant une IP.

## **Vlan natif**

Par défaut le vlan natif est le vlan 1 sur les switchs cisco, par mesure de sécurité il faut choisir un vlan vide qui n'a pas de port affecté comme vlan natif. Ce vlan permet d'isoler le trafic des protocoles comme **DTP**, **STP**, etc.

### **Configuration des interconnexions :**

Après le branchement des différents switchs, il faut paramétrer les ports de chaque switch. Ces ports auront 2 types de

- Trunk
- Access

### **5-2-3 Configuration : Trunk**

Le Trunk est un mécanisme qui permet à des **switchs** interconnectés de faire passer les **paquets** appartenant à **plusieurs Vlans**.

Quand on parle de Trunk, on a deux notions qui existent :

- La notion de Liaison Trunk : c'est la liaison qui existe entre deux commutateurs.
- La notion de Port en mode Trunk : c'est le port qui permet de réaliser la Liaison Trunk.

Les ports en mode trunk ce sont des ports qui appartiennent a tous les vlans, pour avoir une liaison Trunk, il faut donc que les deux ports soient en mode Trunk. Etant donné que plusieurs ports sont reliés aux autres switchs par des liaisons trunk, il faut signifier que ceux-ci seront donc en mode trunk, ci-dessous la configuration des interfaces de fa0/1 à fa0/4 :

```
COEUR1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COEUR1(config)#interface range f0/1-4
COEUR1(config-if-range)#switchport trunk encapsulation dot1Q
COEUR1(config-if-range)#switchport mode trunk
```

Le swithc a bien pris le changement en compte :

```
COEUR1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
|
```

On peut vérifier que les configurations des ports trunks est effective, par la commande « show interfaces trunk » :

```
COEUR1#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.lq	trunking	1
Fa0/2	on	802.lq	trunking	1
Fa0/3	on	802.lq	trunking	1
Fa0/4	on	802.lq	trunking	1
Gig0/2	on	802.lq	trunking	1

Il est arrivé aussi que la commande switchport mode trunk ne peut se réaliser et renvoie un message d'erreur :

```
COEUR1(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is
"Auto" can not be configured to "trunk" mode.
```

Ceci s'explique par le fait que les interfaces sont configurées en dynamic auto mode, cela utilise DTP pour negocier 2 choses :

- Le mode du lien (trunk ou access)
- Encapsulation (ISL ou 8021.Q)

Donc avant d'explicitement indiquer que l'interface est en mode trunk (switchport mode trunk), il est nécessaire au préalable de spécifier par ligne de commande « switchport trunk encapsulation dot1Q » quel type d'encapsulation est utilisé.

#### 5-2-4 Configuration des ports access

Il faut maintenant assigner des aux vlans, sur chaque switch de la couche access dans l'intervalle des interfaces fastEthernet de 3 à 6 pour les data, les port fa0/10 pour les téléphones voip et data. Sur la couche distribution les serveurs sur les ports fa0/.

```
SW-Access1(config)#interface range fa0/3-6
SW-Access1(config-if-range)#switchport mode access
SW-Access1(config-if-range)#switchport access vlan 20
```

Figure 1 : Configuration port access sur switch acces 1

L'utilité est de pouvoir brancher un téléphone avec un ordinateur appartenant au vlan data, il faut indiquer que le port du switch ou sont branchés les equipments doit laisser passer la voip comme les données, ceci se réalise par les commandes suivantes :

```
SW-Access1(config)#interface fa0/10
SW-Access1(config-if)#switchport mode access
SW-Access1(config-if)#switchport voice vlan 40
SW-Access1(config-if)#switchport access vlan 20

SW-Access2(config)#interface range fa0/3-6
SW-Access2(config-if-range)#switchport mode access
SW-Access2(config-if-range)#switchport access vlan 20

SW-Distrib1(config)#interface fa0/5
SW-Distrib1(config-if)#switchport mode access
SW-Distrib1(config-if)#switchport access vlan 30
```

#### 5-2-5 Configurer des interfaces virtuelles

Pour vous connecter au switch, il faut lui ajouter une interface virtuelle (ou VLAN interface), cela rend possible l'ajout d'une adresse IP aux différents switchs. Cela se fait par les commandes suivantes :

```
COEUR2(config)#interface vlan 10
COEUR2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed
state to up

COEUR2(config-if)#ip address 192.168.10.3
% Incomplete command.
COEUR2(config-if)#ip address 192.168.10.3 255.255.255.0
```

Figure 2 : Configurer une Interface virtuelle sur le switch coeur2



## 5-3 Mise en place du Protocole VTP

### 5-3-1 Explication du protocole

Pour Configurer et gérer les vlans pour un grand nombre de commutateurs peut être fastidieux lors de la présence d'un grand nombre de vlans. Pour cette raison Cisco a développé un protocole appelé **VTP (VLAN Trunking Protocol)**.

VTP est un protocole qui permet la création, modification et suppression de vlan sur les commutateurs qui sont dans un même domaine.

Il existe 3 modes VTP qui peut être configurer au niveau du switch :

- **Mode server** : Le commutateur en mode VTP server est le seul qui a la possibilité de faire la création, modification et suppression des vlans et à propager ces infos dans le domaine. Dans un domaine il doit y avoir au moins un commutateur en mode VTP server.
- **Mode client** : Le commutateur en mode VTP client ne peut pas créer ni modifier ou supprimer des vlans. Il se base sur les messages VTP reçus pour mettre à jour sa base de données des vlans. Il a la possibilité de transmettre les **messages VTP** qu'il a reçus à ses voisins.
- **Mode transparent** : Le commutateur en mode transparent peut créer, modifier et supprimer des vlans. Mais il ne partage pas ces modifications avec les autres commutateurs. Il reçoit les messages VTP et les transmet. Mais il ne tient pas compte de ses messages VTP.

### 5-3-2 Fonctionnement

Je me servirai pour la suite que des modes serveurs et client. La création, modification et suppression se fait à partir d'un commutateur en mode VTP Serveur et ce commutateur se charge de transmettre ces infos à l'ensemble des autres commutateurs qui sont dans le domaine VTP.

Il fonctionne au niveau de la couche 2 du modèle OSI et les paquets VTP sont véhiculés uniquement sur les ports en mode Trunk.

### 5-3-3 Configuration vtp

Les étapes pour la configuration des vtp sont au nombre de 4 :

- 1-activer la version 2 de VTP

*Switch(config)#vtp version 2 (la plus récente)*

- 2-configurer un domaine VTP

*Switch(config)# vtp domain { nom de domaine } : pour définir un groupe*

- 3-configurer le mode

*Switch(config)# vtp mode {server / client / transparent}*

- 4-Configurer un mot de passe

*Switch(config)#vtp password { mot passe } :Va permettre de sécuriser le réseau vtp*

### **Placer le switch COEUR1 en mode serveur :**

```
COEUR1(config)#vtp version 2
COEUR1(config)#vtp domain labo
Changing VTP domain name from NULL to labo
COEUR1(config)#vtp mode server
Device mode already VTP SERVER.
COEUR1(config)#vtp password labo
Setting device VLAN database password to labo
COEUR1(config)#
```

---

Si on se rend dans n'importe quel des switches, on se rend compte que ceux-ci ne connaissent pas les vlans indiqués dans le switch COEUR1, il faudra donc placer chaque switch en mode client.

### **Placer un switch en mode client :**

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp version 2
Switch(config)#vtp domain labo
Domain name already set to labo.
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#vtp password labo
Setting device VLAN database password to labo
```

### **5-3-4 Vérification de la prise en compte du protocole vtp**

Pour vérifier la prise en compte des vlans au niveau de chaque switch après la configuration des interconnexions, bien sûr il faudra procéder à cette vérification sur chaque switch, pour cela il faudra lancer la commande « show vlan brief » :

```
COEUR1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1
10	administration	active	
20	data	active	
30	serveur	active	
40	telephonie	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Après avoir vérifié que le protocole vtp a bien joué son rôle, pour les tests je vais tester la connectivité en effectuant un ping avec la configuration ci-dessous :

Ping de Pc1-Labo 1 192.168.20.1/24 à pc2- Labo 31 192.168.20.2/24

Ping de serveur 192.168.30.1/24 - serveur 2 : 192.168.30.2

Les résultats sont concluants, les tests de ping sont donnés ci-dessous :

<pre>Packet Tracer PC Command Line 1.0 C:\&gt;ping 192.168.20.2  Pinging 192.168.20.2 with 32 bytes of data:  Reply from 192.168.20.2: bytes=32 time=13ms TTL=128 Reply from 192.168.20.2: bytes=32 time&lt;1ms TTL=128 Reply from 192.168.20.2: bytes=32 time=21ms TTL=128 Reply from 192.168.20.2: bytes=32 time=12ms TTL=128  Ping statistics for 192.168.20.2:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:     Minimum = 0ms, Maximum = 21ms, Average = 11ms</pre>	<pre>Packet Tracer SERVER Command Line 1.0 C:\&gt;ping 192.168.30.2  Pinging 192.168.30.2 with 32 bytes of data:  Reply from 192.168.30.2: bytes=32 time=18ms TTL=128 Reply from 192.168.30.2: bytes=32 time&lt;1ms TTL=128 Reply from 192.168.30.2: bytes=32 time&lt;1ms TTL=128 Reply from 192.168.30.2: bytes=32 time&lt;1ms TTL=128  Ping statistics for 192.168.30.2:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:     Minimum = 0ms, Maximum = 18ms, Average = 4ms</pre>
--	---

Par contre la communication entre les vlans ne peut pas s'opérer, il faudra donc définir un routeur et une passerelle pour faire du routage intervlan. Ci-dessous un test de connectivité par un ping entre 2 équipements appartenant à des vlans différents (de vlan 20 à vlan 30) :

```
C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

## 5-4 Configuration du Spanning-tree STP

### 5-4-1 Explication du protocole

Le spanning tree (STP) protocole de couche 2 en lien avec les switches, il permet de créer un chemin sans boucle dans un environnement redondant, ce mécanisme est mis en place par défaut sur les switches cisco via un algorithme. Il fonctionne de la façon suivante :

- émission de messages BPDU et election d'un switch maître ou bridge root, il est le point central. Cette election se base sur l'identifiant id composé de la priorité et l'adresse mac
- sélection d'un root port sur les switches non root, ce port est déterminé par le chemin le plus court (défini en terme de bande passante avec un cout) vers le Bridge Root
- sélection d'un port désigné Designated Port (1 seul par segment) et un port blocking qui est bloqué par spanning tree

### 5-4-2 Configuration du protocole

J'ai choisi pour une raison d'optimisation d'accorder le spanning-tree avec HSRP : le cœur 1 sera actif en hsrp, il faudra l'élire comme root bridge, et le cœur 2 sera alors le backup root.

Pour se faire, on va appliquer le spanning tree par les commandes suivantes :

```
COEUR1(config)#spanning-tree vlan 10 root secondary
```

```
COEUR1(config)#spanning-tree vlan 20 root secondary
```

```
COEUR1(config)#spanning-tree vlan 30 root secondary
```

```
COEUR1(config)#spanning-tree vlan 40 root secondary
```

```
COEUR2(config)#spanning-tree vlan 10 root secondary
```

```
COEUR2(config)#spanning-tree vlan 20 root secondary
```

```
COEUR2(config)#spanning-tree vlan 30 root secondary
```

```
COEUR2(config)#spanning-tree vlan 40 root secondary
```

### 5-4-3 Vérifications et tests

Pour la vérification, la commande show spanning-tree permet de vérifier si les commandes ont bien été prise en compte :

VLAN0020										VLAN0020											
Spanning tree enabled protocol ieee										Spanning tree enabled protocol ieee											
Root ID		Priority	24596		Address		000A.F314.EC5B				Root ID		Priority	24596		Address		000A.F314.EC5B			
This bridge is the root											This bridge is the root										
Hello Time		2 sec	Max Age		20 sec	Forward Delay		15 sec		Hello Time		2 sec	Max Age		20 sec	Forward Delay		15 sec			
Bridge ID										Bridge ID											
Priority		24596		(priority 24576 sys-id-ext 20)						Priority		28692		(priority 28672 sys-id-ext 20)							
Address		000A.F314.EC5B								Address		0005.5E27.5399									
Hello Time		2 sec	Max Age		20 sec	Forward Delay		15 sec		Hello Time		2 sec	Max Age		20 sec	Forward Delay		15 sec			
Aging Time		20								Aging Time		20									
Interface		Role	Sts	Cost	Prio.Nbr		Type			Interface		Role	Sts	Cost	Prio.Nbr		Type				
-----		-----			-----					-----		-----			-----						
Fa0/3		Desg	LRN	19	128.3		P2p			Fa0/1		Desg	LSN	19	128.1		P2p				
Fa0/1		Desg	LRN	19	128.1		P2p			Fa0/3		Root	FWD	19	128.3		P2p				
Fa0/2		Desg	LRN	19	128.2		P2p			Fa0/4		Altn	BLK	19	128.4		P2p				
Fa0/4		Desg	LRN	19	128.4		P2p			Fa0/2		Altn	BLK	19	128.2		P2p				

Figure 3 - Commande show spanning-tree vlan 20; à gauche bridge root, à droite backup root (cœur1 et cœur2)

## 5-5 Mise en place du protocole DHCP

### 5-5-1 Configuration DHCP

La prise en charge du service DHCP sera réalisé par les switchs COEUR1 et COEUR2 (en cas de panne par exemple sur le COEUR1). J'ai choisi de le configurer ainsi car si le routeur /box tombe en panne le réseau continuera de fonctionner sauf pour la VOIP , c'est pour cette raison que j'ai choisi de configurer le protocole DHCP pour la VOIP à part car nécessite le routeur 18

Pour chaque vlan le serveur dhcp devra donc attribuer une adresse sur la plage IP spécifiée. Pour chacune des plages, j'ai choisi d'exclure les 15 premières adresses afin de faciliter les tests.

Il faut donc créer les pools de distribution pour les sous interfaces vlan et indiquer la passerelle par défaut :

```

-----
COEUR2(config)#ip dhcp pool administration
COEUR2(dhcp-config)#network 192.168.10.0 255.255.255.0
COEUR2(dhcp-config)#default-router 192.168.10.1
COEUR2(dhcp-config)#ip dhcp pool server
COEUR2(dhcp-config)#network 192.168.30.0 255.255.255.0
COEUR2(dhcp-config)#default-router 192.168.30.1
COEUR2(dhcp-config)#ip dhcp pool data
COEUR2(dhcp-config)#network 192.168.20.0 255.255.255.0
COEUR2(dhcp-config)#def
COEUR2(dhcp-config)#default-router 192.168.20.1
COEUR2(dhcp-config)#ip dhcp excluded-address 192.168.10.1
192.168.10.10
COEUR2(config)#ip dhcp excluded-address 192.168.20.1
192.168.20.10
COEUR2(config)#ip dhcp excluded-address 192.168.30.1
192.168.30.10
-----

```

On peut ensuite vérifier par la commande suivante que la configuration dhcp a bien été prise en compte : COEUR1#show ip dhcp pool

```
COEUR2#show ip dhcp pool

Pool data :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 254
Leased addresses                  : 0
Excluded addresses                : 5
Pending event                     : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
192.168.20.1      192.168.20.1 - 192.168.20.254  0 / 5 / 254
```

Figure 4: Commande ip dhcp pool :exemple pool dhcp data

### 5-5-2 Vérification du fonctionnement DHCP

Il faut vérifier le fonctionnement du serveur DHCP en lançant respectivement les commandes « ipconfig /release » « ipconfig /renew » les périphériques terminaux :

ipconfig /release : libère la configuration DHCP actuelle puis annule la configuration de l'adresse IP.

ipconfig /renew : Renouvelle la configuration DHCP des périphériques

C:\>ipconfig /release	C:\>ipconfig /renew
IP Address.....: 0.0.0.0	IP Address.....: 192.168.20.11
Subnet Mask.....: 0.0.0.0	Subnet Mask.....: 255.255.255.0
Default Gateway...: 0.0.0.0	Default Gateway...: 192.168.20.1
DNS Server.....: 0.0.0.0	DNS Server.....: 0.0.0.0

Figure 5 : Renouveler l'adresse ip d'un périphérique terminal avec DHCP

J'ai également fait un test de ping pour vérifier la connectivité entre les machines, ci-dessous un exemple de ping entre un pc du labo 1 et un pc du labo 2 :

```
C:\>ping 192.168.20.21

Pinging 192.168.20.21 with 32 bytes of data:

Reply from 192.168.20.21: bytes=32 time=28ms TTL=128
Reply from 192.168.20.21: bytes=32 time=60ms TTL=128
Reply from 192.168.20.21: bytes=32 time=24ms TTL=128
Reply from 192.168.20.21: bytes=32 time=13ms TTL=128

Ping statistics for 192.168.20.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 60ms, Average = 31ms
```

## 5-6 Mise en place du protocole HSRP

### 5-6-1 Principes de HSRP

Pour assurer le redoncance et une haute disponibilit  d'une passerelle d'un r seau, ici je vais utiliser HSRP qui est un protocole CISCO. Ce protocole est mis en place sur les 2 switchs c eurs COEUR1 et COEUR2 (switch de niveau 3). Le but est qu'une possible panne d'un des 2 c eurs ne perturbe pas le r seau en le rendant toujours disponible. A noter qu'il existe 2 autres protocoles similaires a HSRP qui sont VRRP et GLBB.

Le principe est que l'un des 2 switchs c eurs sera Actif et le switch Coeur2 de secours sera en standby. Le switch COEUR1 actif assure le r le de passerelle par d faut pour les vlans. S'il vient   tomber en panne, le switch COEUR2 prendra le relais, le groupe de switchs est alors appel  le « StandBy Group ».

Au sein de ces groupes, le routeur actif envoie des messageshello toutes les 3 secondes, apr s 10 secondes sans message hello du routeur actif, il sera consid r  comme HS.C 'est   ce moment que le routeur standby prendra le relais et deviendra actif.

Entre les 2 switches, le but est de creer une passerelle virtuelle pour chaque vlan, celle-ci aura sa propre adresse ip qui sera une ip virtuelle, et  galement une adresse mac virtuelle.

### 5-6-2 Configuration HRSP

Apr s avoir cr e les interfaces virtuelles pour chaque vlan en leur assignant une adresse ip sur les switchs COEUR1 et COEUR2, il faudra choisir une IP virtuelle et une priorit . Pour chaque vlan le switch COEUR1 jouera le r le de routeur actif, il faut choisir une ip virtuelle et une priorit  :

```
COEUR1(config-if)#interface vlan 20
COEUR1(config-if)#ip address 192.168.20.2 255.255.255.0
COEUR1(config-if)#standby 20 ip 192.168.20.1
COEUR1(config-if)#standby 20 priority 150|
```

Le num ro 20 dans la commande « standby 20 ip 192.168.20.1 » correspond au numero du StandBy group, la priorit  par d faut est de 100 avec la commande « standby 20 priority 150 » : le switch COEUR1 devient alors salors actif.

La commande « standby preempt » est une option qui permet au switch actif de reprendre son r le apr s une panne. Le routeur Standby qui rempla ait le routeur actif lors d'une panne de ce dernier, redeviendra en mode standby si le routeur actif revient en ligne.

Il faut maintenant configurer le switch C EUR 2 pour qu'il soit en standby, on remarque qu'ici on ne mettera pas de priorit  et que son statut passe   standby :



```
COEUR2(config)#interface vlan 10
COEUR2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed
state to up

COEUR2(config-if)#ip address 192.168.10.3
% Incomplete command.
COEUR2(config-if)#ip address 192.168.10.3 255.255.255.0
COEUR2(config-if)#standby 10 ip 192.168.10.1
COEUR2(config-if)#standby 10 preempt
COEUR2(config-if)#
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
```

Figure 6 : Configuration hsrp sur le coeur2 et l'interface virtuelle vlan 10

### 5-6-3 Tests et vérifications du fonctionnement

On peut vérifier par la commande « show standby » que toutes ces configurations ont été prise en compte :

<pre>COEUR1#show standby Vlan20 - Group 20 State is Active   6 state changes, last state change 05:27:30 Virtual IP address is 192.168.20.1 Active virtual MAC address is 0000.0C07.AC14   Local virtual MAC address is 0000.0C07.AC14 (vl default) Hello time 3 sec, hold time 10 sec   Next hello sent in 2.145 secs Preemption enabled Active router is local Standby router is 192.168.20.3 Priority 150 (configured 150) Group name is hsrp-Vl2-20 (default) ... ..</pre>	<pre>COEUR2#show standby Vlan10 - Group 10 State is Standby   6 state changes, last state change 05:21:34 Virtual IP address is 192.168.10.1 Active virtual MAC address is 0000.0C07.ACOA   Local virtual MAC address is 0000.0C07.ACOA (vl default) Hello time 3 sec, hold time 10 sec   Next hello sent in 1.777 secs Preemption enabled Active router is 192.168.10.2 Standby router is local Priority 100 (default 100) Group name is hsrp-Vl1-10 (default)</pre>
--	---

Je vais maintenant simuler que le switch CŒUR 1 tombe en panne en désactivant tous ses ports : Je remarque que *le* switch COEUR2 a pris automatiquement le relais, il passe de l'état standby à active , on aperçoit les messages suivants sur le switch COEUR2 :

```
%HSRP-6-STATECHANGE: Vlan20 Grp 20 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan30 Grp 30 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan20 Grp 20 state Standby -> Active

%HSRP-6-STATECHANGE: Vlan30 Grp 30 state Standby -> Active
```

J'ai également effectué des tests de connectivité avec des pings sur l'adresse virtuelle du vlan 20 192.168.20.1 à partir d'un pc appartenant à ce vlan :

```
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time=3ms TTL=255

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms
```



## 5-7 Mise en place du routage

Par défaut un switch de niveau 3 n'est pas capable de faire du routage, il faudra donc activer cette fonction. Il rendra ainsi possible la communication ou l'échange d'information entre les différents vlans, ceci s'appelle le routage inter-vlan.

La commande « ip routing » permettra d'activer cette fonction de routage, sans elle le switch ne pourra pas assurer le routage.

En observant la table de routage en entrant la commande show ip route, on constate que les vlans ont bien été ajoutés à la table de routage du COEUR1 et COEUR2 :

```
COEUR1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
C    192.168.30.0/24 is directly connected, Vlan30
C    192.168.40.0/24 is directly connected, Vlan40
```

### 5-7-1 Configuration du routage statique

#### 5-7-1-1 Configuration des interfaces

##### **Interfaces des switchs COEUR 1 et 2**

Il faut maintenant configurer les 2 interfaces fa0/24 des switchs COEUR1 et COEUR2 étant directement connecté au routeur en tant qu'interface routée en entrant la commande « no switchport », et également leur attribuer une adresse ip avec le masque de sous réseau

```
COEUR1(config)#interface fa0/24
COEUR1(config-if)#no switchport
```

```
COEUR1(config-if)#ip address 192.168.60.2 255.255.255.0
```

```
COEUR2(config)#interface fa0/24
COEUR2(config-if)#no switchport
```

```
COEUR2(config-if)#ip address 192.168.50.2 255.255.255.0
```

## **Interfaces ROUTEUR**

Du côté du routeur, il faut également attribuer une adresse ip pour chaque interface et ne pas oublier de monter l'interface :

```
ROUTEUR(config)#interface fa0/1
ROUTEUR(config-if)#ip address 192.168.50.1 255.255.255.0
ROUTEUR(config-if)#no shut
```

```
ROUTEUR(config)#interface fa0/0
ROUTEUR(config-if)#ip address 192.168.60.1 255.255.255.0
ROUTEUR(config-if)#no shut
```

### **5-7-7-2 Création d'une route statique**

A ce stade le routeur n'a aucune connaissance des réseaux Vlans, et les switchs COEUR1 et 2 ne connaissent pas les réseaux WAN ou MAN par exemple. Il faut donc mettre en place du routage statique ou dynamique pour faire apprendre ces réseaux.

#### **Du côté du routeur**

La commande ip route va permettre de créer une route statique pour permettre au routeur comment joindre les réseaux derrière les switchs COEUR1 et COEUR2 :

```
Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.50.2
```

créer une route statique      réseau à atteindre      masque      adresse ip du saut suivant

Figure 7 : Commande ip route à partir du routeur

Bien entendu, cette configuration de route statique est à faire pour tous les vlans et sur les 2 adresses ip du saut suivant des coeur1 et coeur2 :

```
Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.50.2
Router(config)#ip route 192.168.30.0 255.255.255.0 192.168.50.2
Router(config)#ip route 192.168.40.0 255.255.255.0 192.168.50.2
Router(config)#ip route 192.168.10.0 255.255.255.0 192.168.50.2

Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.60.2
Router(config)#ip route 192.168.10.0 255.255.255.0 192.168.60.2
Router(config)#ip route 192.168.30.0 255.255.255.0 192.168.60.2
Router(config)#ip route 192.168.40.0 255.255.255.0 192.168.60.2
```

En tapant la commande show ip route pour afficher la table du routage du routeur, on constate que le routeur connaît automatiquement maintenant les réseaux auxquelles ces interfaces sont connectées :

```
S 192.168.10.0/24 [1/0] via 192.168.60.2
    [1/0] via 192.168.50.2
S 192.168.20.0/24 [1/0] via 192.168.60.2
    [1/0] via 192.168.50.2
S 192.168.30.0/24 [1/0] via 192.168.60.2
    [1/0] via 192.168.50.2
S 192.168.40.0/24 [1/0] via 192.168.60.2
C 192.168.50.0/24 is directly connected, FastEthernet0/1
C 192.168.60.0/24 is directly connected, FastEthernet0/0
```

### Du coté des switches cœurs 1 et 2 : Route statique par défaut

Il faut maintenant pouvoir rediriger les traffic des différents vlans vers le wan. J'indique ici au switch cœur dès qu'il recoit une trame qu'il ne connaît pas de l'envoyer vers la box /routeur on va pour se faire créer une route statique par défaut vers le routeur :

```
COEUR2(config)#ip route 0.0.0.0 0.0.0.0 192.168.50.1
```

```
COEUR1(config)#ip route 0.0.0.0 0.0.0.0 192.168.60.1
```

On a donc maintenant la route par défaut qui est mise en place sur chacun des cœurs en entrant la commande show ip route sur les switches cœurs :

```
Gateway of last resort is 192.168.50.1 to network 0.0.0.0
```

```
C 192.168.10.0/24 is directly connected, Vlan10
C 192.168.20.0/24 is directly connected, Vlan20
C 192.168.30.0/24 is directly connected, Vlan30
C 192.168.40.0/24 is directly connected, Vlan40
C 192.168.50.0/24 is directly connected, FastEthernet0/24
S* 0.0.0.0/0 [1/0] via 192.168.50.1
```

```
Gateway of last resort is 192.168.60.1 to network 0.0.0.0
```

```
C 192.168.10.0/24 is directly connected, Vlan10
C 192.168.20.0/24 is directly connected, Vlan20
C 192.168.30.0/24 is directly connected, Vlan30
C 192.168.40.0/24 is directly connected, Vlan40
C 192.168.60.0/24 is directly connected, FastEthernet0/24
S* 0.0.0.0/0 [1/0] via 192.168.60.1
```

### 5-7-2 Vérification du fonctionnement et tests

Je vais créer une adresse de loopback en 1.1.1.1/24 pour simuler le routeur internet car une loopback repondra toujours a un ping, ceci se fait par la commande ci-dessous :

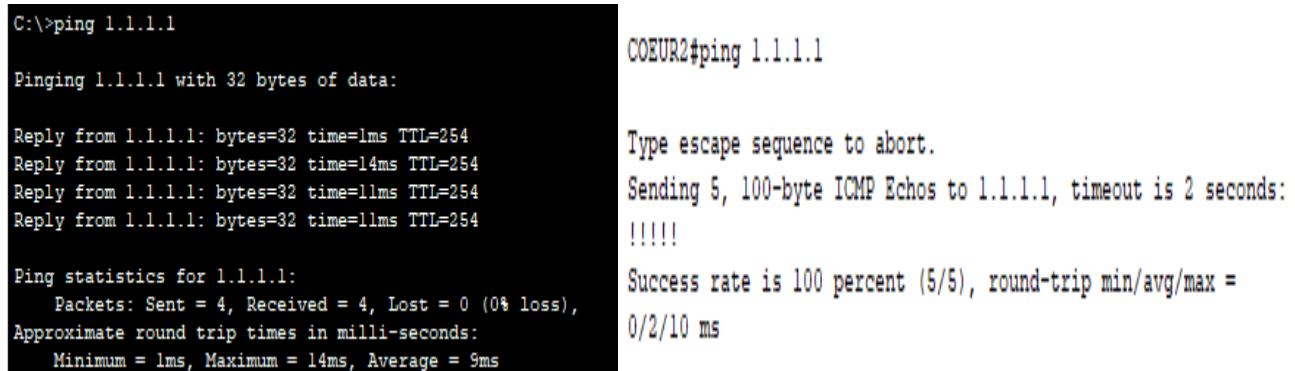
```
Router(config)#interface loopback 0

Router(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up

Router(config-if)#ip address 1.1.1.1 255.255.255.0
```

Pour tester la connectivité, j'effectue un ping de différents équipements du réseau :



```
C:\>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:

Reply from 1.1.1.1: bytes=32 time=1ms TTL=254
Reply from 1.1.1.1: bytes=32 time=14ms TTL=254
Reply from 1.1.1.1: bytes=32 time=11ms TTL=254
Reply from 1.1.1.1: bytes=32 time=11ms TTL=254

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 14ms, Average = 9ms

COEUR2#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/2/10 ms
```

Figure 8 : Test ping de l'interface loopback 1.1.1.1/24 (à gauche à partir d'un pc du vlan 20 , à droite à partir du coeur2)

Les résultats sont concluants, il me faut maintenant paramétrer la VOIP sur le routeur et les différents switches.

## 5-8 Mise en place de La VOIP

### 5-8-1-Configuration de la VOIP

#### 5-8-1-1 Configuration DHCP et TFTP

Pour utiliser le protocole DHCP et assigner des adresses IP aux différents IP Phones, il est indispensable d'indiquer que la passerelle par défaut est le routeur car lui seul permet de configurer le service de téléphonie « Call Manager Express » pour activer le support VOIP sur le réseau.

La commande « option 150 ip 192.168.60.1 » indique qu'un serveur TFTP est utilisé pour permettre aux téléphones d'obtenir le firmware et certains fichiers de configuration du routeur, cela se fait par l'option 150 du DHCP.

```
COEUR1(config)#interface vlan 40
COEUR1(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up

COEUR1(config-if)#ip address 192.168.40.1 255.255.255.0
COEUR1(config-if)#no shut
COEUR1(config-if)#ip dhcp pool voice
COEUR1(dhcp-config)#network 192.168.40.0 255.255.255.0
COEUR1(dhcp-config)#default-router 192.168.60.1
COEUR1(dhcp-config)#option 150 ip 192.168.60.1
```

### 5-8-1-2 Configuration du service de téléphonie « Call Manager Express »

Pour configurer le CME, il faut exécuter les commandes suivantes :

```
1-Router(config)#telephony-service
2-Router(config-telephony)#max-dn 5
3-Router(config-telephony)#max-ephones 5
4-Router(config-telephony)#ip source-address 192.168.60.1 port 2000
5-Router(config-telephony)#auto assign 1 to 5
```

1-Commande telephony-service afin de passer en mode de configuration du téléphone

2-Commande « max-dn 5 » afin de déterminer le nombre maximal d'extensions prise en charge par la plateforme.

3-« max-ephones 5 »pour déterminer le nombre maximal de téléphones IP prise en charge par la plateforme.

4- ip source-address 192.168.60.1 port 2000 : pour identifier L'adresse IP du routeur et le port utilisé (par défaut 2000) où les téléphones seront enregistrés et l'adresse source où s'exécutent les services DHCP et CallMaangerExpress.

5- auto assign 1 to 5 : enregistrer automatiquement les téléphones, dans ce cas, c'est du téléphone 1 à 5.

### 5-8-1-3 Configurer les téléphones IP

Pour pouvoir passer ou recevoir des appels, il faut inscrire les téléphones IP qu'on utilise sur le système service CallManager Express. Chaque téléphone physique doit être configuré comme un ephone dans le routeur Cisco CallManager Express afin de permettre une prise en charge dans le réseau.

Nous avons configuré 5 téléphones IP max, nous allons donc configurer 5 numéros max pour les lignes, les commandes ephone-dn pour créer l'extension et number pour donner un numéro :

```
Router(config)#ephone-dn 1
Router(config-ephone-dn)##LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up

Router(config-ephone-dn)#number 10
Router(config-ephone-dn)#exit
Router(config)#ephone-dn 2
Router(config-ephone-dn)##LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up

Router(config-ephone-dn)#number 20
Router(config-ephone-dn)#ephone-dn 3
Router(config-ephone-dn)##LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state to up

Router(config-ephone-dn)#number 30
Router(config-ephone-dn)#ephone-dn 4
Router(config-ephone-dn)##LINK-3-UPDOWN: Interface ephone_dsp DN 4.1, changed state to up

Router(config-ephone-dn)#number 40
Router(config-ephone-dn)#ephone-dn5
      ^
% Invalid input detected at '^' marker.

Router(config-ephone-dn)#ephone-dn 5
Router(config-ephone-dn)##LINK-3-UPDOWN: Interface ephone_dsp DN 5.1, changed state to up

Router(config-ephone-dn)#number 50
Router(config-ephone-dn)#exit
```

#### 5-8-1-4 Configuration du vlan Voice sur les switches

Il faut ensuite configurer les switches afin de séparer les données et les communications, la commande switchport voice indique donc ici qu'on souhaite faire passer de la VOIP et brancher un pc derrière ce téléphone voip :


```
SW-Access4(config)#interface fa0/10
SW-Access4(config-if)#switchport mode access
SW-Access4(config-if)#switchport voice vlan 40
SW-Access4(config-if)#switchport access vlan 20
```

#### 5-8-2 Vérifications et tests de fonctionnement

Je vais d'abord vérifier des attributions IP et des numéros. Il ne faut pas oublier d'allumer les téléphones voip, en connectant la prise :



On observe ci-dessous qu'une adresse IP a été distribuée en dessous de « IP Address » et qu'un numéro de téléphone a été associé à côté de Line Number.



IP Phone

Port	Link	IP Address	MAC Address
Vlan1	Down	<not set>	0030.F2C1.BA28
Switch	Up	<not set>	0040.0BB7.5D01
PC	Down	<not set>	0040.0BB7.5D02
Vlan40	Up	192.168.40.2/24	0030.F2C1.BA28

Gateway: 192.168.60.1  
Line Number: 10

Physical Location: Intercity, Home City, Corporate Office

#### Tests du bon fonctionnement :

Le but est de s'assurer que le tout fonctionne correctement. Pour ce test, j'effectue un appel depuis le téléphone avec le numéro 10 vers le téléphone 20. Dans l'onglet « GUI », on tape le numero du téléphone IP 20.

Il est bien stipulé « Ring Out » ce qui indique que le second téléphone est bien contacté et qu'il sonne. Maintenant allons sur l'interface IP Phone 20 pour recevoir l'appel en décrochant de la même manière.



Figure 9 : Phone numéro 10 appelle numéro 20

La lumière rouge du téléphone clignote et l'écran nous indique un appel provenant de 10. On décroche, et on voit apparaître « Connected » sur l'écran du téléphone. Le service de téléphonie est donc fonctionnel puisque les appels sont envoyés et reçus avec succès.



Fig10 : Appel réussi sur le Phone numéro 20

### **Problèmes rencontrés :**

Ici j'ai rencontré des problèmes au niveau de la voip : en effet lorsque le switch coeur1 tombe en panne, le relais est assuré par le coeur2 mais la voip malheureusement ne s'avère pas être fonctionnelle.

## **5-9 Tests finaux**

Pour réaliser ces tests, j'ai effectué des tests de ping pour la connectivité et vérifier que les équipements obtiennent bien une adresse IP et sont donc bien identifiés sur le réseau. J'ai également vérifié que le protocole HSRP était fonctionnel

J'ai procédé comme précisé ci dessous :

- Simuler une panne du cœur 1 en désactivant tous ces ports : le switch CŒUR 2 prend bien le relais, les attributions et les tests de connectivité sont concluants, hormis la téléphonie le tout fonctionne.
- Activer tous les ports du cœur 1 : résultats concluants, il reprend bien sa place
- Désactiver des ports sur les switchs cœurs : Par unité fa0/1, réactiver fa0/1 puis désactiver fa0/2 ainsi de suite : résultats concluants. En désactivant plusieurs ports à la fois : résultats non concluants, ceci s'explique par le fait qu'il n'y a plus de lien qui mènerait vers par exemples les switchs du labo 1.
- Désactiver les ports sur les différents switchs distribution interconnectés aux switchs access, en opérant par switch et par labo : résultats concluants.



## 6 Analyse conclusion

---

L'architecture répond en partie aux besoins, il s'est avéré judicieux de placer le routage sur le switch cœur ainsi que le protocole DHCP, même si il y a eu des conflits au niveau de ce protocole. Le routeur permettant un accès au WAN ou MAN est sans doute le point faible de l'architecture proposé : il pourrait être plus sain de mettre en place 2 routeurs box avec chacun un accès à des FAI différents et sur des sites différents.

Il y aurait ici une amélioration à apporter au niveau de la VOIP, car d'une part je n'ai pas réussi à spécifier un port secondaire pour exécuter le service call manager en cas de panne du cœur 1. D'autre part, la mise en place de la QOS n'a pas été réalisée, elle aurait permis de fournir un service optimale conforme à des exigences techniques.

Il aurait été également plus logique d'essayer d'établir des ACL afin de permettre ou non l'accès à certains équipements constituant le réseau. Il est vrai que je n'ai pas mis en place une stratégie haute de sécurité, cela peut se faire par la mise en place d'un firewall.

Pour finir, il faudrait sûrement ajouter de la redondance et mieux appréhender le protocole STP pour optimiser le travail accompli, en effet à certains niveaux des problèmes aux niveau des chemins sont sûrements apparus.