



Université Ain Temouchent  
Faculté des sciences et technologies  
Département Génie Electrique  
2021



# *Recueil en Routage IP (Travaux Pratiques)*

*Auteur :SOUIKI Sihem*

*Maître de Conférences à l'Université d'Ain Temouchent  
Faculté des Sciences et Technologies  
Département Génie Electrique*

## Table des matières

<b>Table des matières .....</b>	<b>I</b>
<b>Introduction générale .....</b>	<b>1</b>
<b>TP1 : Configuration de base d'un commutateur (plateforme CISCO) .....</b>	<b>3</b>
I. Objectifs pédagogiques.....	3
II. Partie théorique .....	3
II.1. Notions fondamentales.....	3
II.1.1 Sources de configuration .....	3
II.1.2 Modes de configuration.....	4
II.2. Outil de simulation : Cisco Packet tracer .....	4
III. Partie pratique .....	4
III.1 Schéma de topologie et adressage .....	4
III.2 Suppression d'une configuration existante sur un commutateur .....	5
III.3 Vérification de la configuration par défaut du commutateur .....	6
III.4 Création d'une configuration de base de commutateur .....	8
<b>TP N° 02 Création et configuration d'un réseau segmenté en VLAN .....</b>	<b>12</b>
I. Objectifs pédagogiques.....	12
II. Partie théorique .....	12
II.1 Définition d'un VLAN.....	12
II.2 Types de VLAN .....	13
III. Partie pratique .....	13
III.1 Mise en place de la topologie et adressage .....	13
III.2 Configuration de VLANs (Niveau 1) sur un seul Switch .....	14
III.2.1 Définir les VLANs.....	14
III.2.2 Associer les ports à leurs VLANs.....	15
III.2.3 Permuter deux postes .....	16
III.3 Configuration de VLANs (Niveau 1) sur deux Switchs .....	16
III.3.1 Préparation de la maquette .....	16
III.3.2 Affecter un nom au Switch2.....	17
III.3.3 Configuration de VLANs sur le Switch2 .....	17
III.3.4 Associer les ports à leurs VLANs.....	17

III.3.5 Configuration des ports Trunk entre les deux Switchs .....	18
<b>TP N°03 : Configuration de routage inter-VLAN.....</b>	<b>19</b>
I. Objectifs pédagogiques.....	19
II. Partie théorique .....	19
II.1 Router On A Stick .....	19
II.2 Multilayer Switch (Layer 3).....	20
III. Partie pratique .....	20
III.1 Configuration du routage inter-VLAN avec un routeur Router On A Stick .....	20
III.1.1 Création des vlans.....	21
III.1.2 Association des VLANs créés avec les ports du commutateur .....	21
III.1.3 Mise en mode trunk de l'interface reliant le switch au routeur .....	21
III.1.4 Mise en place du routage inter-VLANs .....	21
III.1.5 Création des sous-interfaces .....	21
III.2 Configuration du routage iner-VLAN avec des switch L3 .....	22
III.2.1 Création des vlans.....	22
III.2.2 Association des VLANs créés avec les ports du commutateur .....	23
III.2.3 Création des interfaces VLAN .....	23
III.2.4 Activation du routage au niveau du switch (L3).....	24
<b>TP4 : Création d'un réseau avec des liens redondant.....</b>	<b>26</b>
I. Objectifs pédagogiques.....	26
II. Partie théorique .....	26
II.1 Problématique.....	26
II.1.1 Tempête de Broadcast .....	26
II.1.2 Duplication de trame et instabilité de table CAM.....	27
II.2 Fonctionnement du spanning tree .....	27
III. Partie pratique .....	28
III.1 Scénario utilisé .....	28
III.2 Comment activer Spanning Tree? .....	28
III.3 Choix du meilleur chemin/ désactivation des chemins redondants .....	30
III.4 Les Timers STP .....	32
III.5 Rapid-PVST .....	33
<b>TP5 : Configuration du protocole Etherchannel entre commutateurs Simulation sous packet-tracer .....</b>	<b>37</b>
I. Objectifs pédagogiques.....	37
II. Partie théorique .....	37

II.1 Définition .....	37
II.2 Négociation de l'agrégation .....	37
a) PAgP .....	37
b) LACP .....	37
III. Partie pratique .....	38
III.1 Configuration d'un EtherChannel avec Cisco PAgP .....	38
III.2 Configuration d'un EtherChannel LACP 802.3ad .....	41
III.3 Configuration d'un lien EtherChannel redondant .....	42
<b>TP6 : Mise en œuvre d'un routage statique .....</b>	<b>45</b>
I. Objectifs pédagogiques .....	45
II. Partie théorique .....	45
III. Partie pratique .....	45
III.1 Configuration du routage statique .....	45
III.2 Routage statique et métrique .....	48
III.2.1 Définition de la métrique : .....	48
III.2.2 Configuration des nouvelles interfaces .....	49
III.2.3 Configuration des routes statiques et tables de routage .....	51
<b>TP7 : Mise en œuvre d'un routage dynamique RIPv2, EIGRP et OSPF .....</b>	<b>54</b>
I. Objectifs pédagogiques .....	54
II. Partie théorique .....	54
II.1 Protocole RIP .....	54
II.2 Protocole EIGRP .....	55
III. Partie pratique .....	56
III.1 Configuration du protocole RIP .....	56
III.1.1 Configuration des interfaces des routeurs .....	57
III.1.2 Configuration du protocole RIPv2 .....	58
III.1.3 Désactivation du RIP2 .....	59
III.2 Configuration du protocole EIGRP 1 .....	59
III.3 Configuration du protocole OSPF .....	63
<b>Conclusion générale .....</b>	<b>65</b>

## Liste d'acronymes

**BID:** Bridge ID

**BPDU:** Bridge Protocol Data Units

**CIDR:** Classless Inter-Domain Routing

**CLI:** Command Line Interface

**EIGRP:** Enhanced Interior Gateway Routing Protocol

**LACP:** Link Agregation Control Protocol)

**MAC:** Media Access Control

**NVRAM:** Non-volatile random access memory

**OSPF:** Open Shortest Path First

**PAgP:** Port Agregation Protocol

**PC:** Personal computer

**PING:** Packet Internet or Inter-Network Groper

**Rapid-PVST:** Rapid per VLAN Spanning Tree

**RIP:** Routing Information Protocol

**RIPv2:** Routing Information Protocol version 2

**RTP:** Reliable Transport Protocol

**SNMP:** Simple Network Management Protocol

**STP:** Spanning tree protocol

**TFTP:** Trivial File Transfer Protocol

**VLAN:** Virtual LAN

**VLSM:** Variable-Length Subnet Masking

**VTY:** virtual teletype

## **Introduction générale**

La structure de l'Internet peut être comparée à une grande coalition de sous réseaux autonomes. Chacun de ces réseaux fonctionne avec ses propres politiques, prix, services et clients.

Un sous réseau est en fait un réseau local, ou LAN (Local Area Network). C'est un groupe de périphériques associés qui partagent des liaisons de communication filaires ou sans fil, liées à la transmission et l'échange d'information entre différentes entités.

Il existe plusieurs manières d'acheminer cette information à leur destination, qui sont implémentées par divers standards. Et on peut classer ces différentes méthodes en plusieurs catégories suivant leur organisation ou architecture, les distances, les vitesses de transmission et la nature des informations transmises.

Ce travail a été réalisé dans le cadre des Travaux Pratiques du Routage IP pour des étudiants en 1<sup>ère</sup> année Master académique en Réseaux et Télécommunications (R&T), à l'université d'Ain Temouchent Belhadj Bouchaib, qui désirent approfondir leurs compétences pratiques ou avoir au moins des connaissances de base sur la configuration des équipements réseau tels que : les commutateurs ou routeurs.

L'objectif est de permettre à l'étudiant de se familiariser rapidement avec les équipements réseau, il s'agit aussi de faire comprendre aux étudiants leur fonctionnement, d'analyser le comportement des différents types de routage utilisés tels que le routage statique ou bien dynamique.

Le présent document constitue un support de travaux pratiques pour ceux qui veulent apprendre les notions de base sur la commutation et le routage IP en utilisant l'outil de simulation Cisco Packet Tracer. Il est organisé en sept chapitres.

**TP1** : Configuration de base d'un commutateur (plateforme CISCO).

**TP2** : Création et configuration d'un réseau segmenté en VLAN.

**TP3** : Configuration de routage inter-VLAN.

**TP4** : Création d'un réseau avec des liens redondants.

**TP5** : Configuration du protocole Etherchannel entre commutateurs.

**TP6** : Mise en œuvre d'un routage statique.

**TP7** : Mise en œuvre d'un routage dynamique RIPv2, EIGRP et OSPF.

A la fin de ce recueil de TPs, l'étudiant sera capable de simuler, résoudre différents problèmes de configuration des équipements réseaux Cisco, ce qui va lui procurer une simplicité d'analyse de fonctionnement des différents systèmes.

## **Introduction générale**

Je suis ouverte à toute suggestion de correction ou de modification de la part des lecteurs intéressés par la matière présentée, j'espère qu'ils y trouvent un support utile et un outil de travail intéressant, comme j'apprécie fortement leurs réactions, critiques et conseils. Toute erreur ou ambiguïté relevée peut être communiquée à l'adresse suivante : **[souikisihem@gmail.com](mailto:souikisihem@gmail.com)**

## TP1 : Configuration de base d'un commutateur (plateforme CISCO)

### I. Objectifs pédagogiques

Dans ce TP, nous allons explorer le rôle principal d'un commutateur CISCO, ainsi que les différentes commandes de base pour leur configuration.

- Comprendre la fonction de base d'un commutateur.
- Supprimer une configuration existante sur un commutateur.
- Vérifier la configuration par défaut du commutateur.
- Créer une configuration de base de commutateur.

### II. Partie théorique

#### II.1. Notions fondamentales

##### II.1.1 Sources de configuration :

Les commutateurs CISCO peuvent être configurés, simultanément et/ou indépendamment, à partir de plusieurs sources. On peut classer ces différentes sources en deux catégories : les sources locales et les sources distantes [1].

##### a) Sources locales :

Le port "Console": Il s'agit d'un port série qui sera relié par un câble série (en général de quelques décimètres), soit à un Terminal Asynchrone, soit à un micro-ordinateur utilisant un émulateur de Terminal Asynchrone comme Hyper Terminal de Microsoft.

La configuration par défaut est 9600 bits/s, 8 bits/caractère, 1 bit de départ, 1 bit d'arrêt, pas de bit de parité, pas de contrôle de flux. Le port console est indispensable si le commutateur n'a pas de protocole IP configuré.

##### b) Sources distantes

Dès que le protocole IP est configuré sur le commutateur, il est possible de le configurer à distance à partir d'une station de réseau local. La communication utilise alors l'une des interfaces de réseau du commutateur.

- Les terminaux virtuels (VTY) : au moyen d'un émulateur de Terminal Asynchrone comme un client Telnet par exemple.
- Les serveurs TFTP : qui permettront de télécharger un fichier de configuration sur le commutateur.
- Les stations d'administration de réseau : au moyen d'une station SNMP (ex : CiscoWorks ou HP Open View).



## TP1 : Configuration de base d'un commutateur (plateforme CISCO)

### II.1.2 Modes de configuration

Les commutateurs CISCO peuvent utiliser plusieurs modes différents parmi lesquels [1] :

- a) **Mode utilisateur:** Ce mode ne permet qu'un examen limité de la configuration du commutateur. L'invite est "Switch>".
- b) **Mode privilégié:** Le mode privilégié est obtenu en tapant la commande "enable" à partir du mode utilisateur. Il permet l'examen total et la configuration du commutateur, ainsi que l'accès à des mécanismes de tests et de dépannage. L'invite est "Switch#". Pour quitter le mode privilégié, taper "exit", "end" ou "CTRL+Z".
- c) **Mode de configuration globale:** Il est obtenu en tapant la commande "configure" à partir du mode privilégié. L'invite est "Switch (config)#". Ce mode donne accès à des commandes qui concernent l'ensemble du commutateur comme par exemple la commande "**hostname**" qui affecte un nom au commutateur. Ce nom sera repris par la plupart des invites des différents modes.
  - Mode de configuration d'interface : ...
  - Mode de configuration de protocole: ...

### II.2. Outil de simulation : Cisco Packet tracer

C'est un outil de simulation de matériel réseau (routeurs, commutateurs, concentrateur, etc.), créé par Cisco systèmes [2]. Le but de Packet Tracer est de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur réalise son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible de les configurer (adresses IP, les services disponibles, ...etc.).

## III. Partie pratique

### III.1 Schéma de topologie et adressage

#### a) Schéma de topologie

A l'aide de l'outil « CISCO Packet Tracer », schématiser le réseau de la figure I.1 composé d'un commutateur (Switch), et de deux ordinateurs.

## TP1 : Configuration de base d'un commutateur (plateforme CISCO)

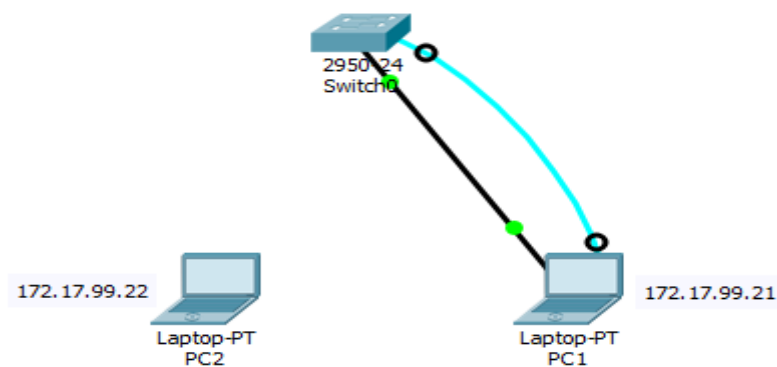


Figure I.1 Schéma de topologie

Choisissez un Switch de type 2950-24 et des PCs Laptop-PT (PC-PT)

### b)Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
PC1	Carte réseau	172.17.99.21	255.255.255.0	172.17.99.1
PC2	Carte réseau	172.17.99.22	255.255.255.0	172.17.99.1
Switch0	VLAN99	172.17.99.11	255.255.255.0	192.17.99.1

Tableau I.1 La table d'adressage

## III.2 Suppression d'une configuration existante sur un commutateur

- **Étape 1 : Passage en mode d'exécution privilégié**

Cliquez sur Switch0 puis sélectionnez l'onglet **CLI** (Ou en utilisant un câble de console pour configurer le commutateur Cisco par l'intermédiaire du port de console. Il s'agit de créer une connexion console avec le commutateur à partir de PC1 à l'aide de l'émulation de terminal).

Utilisez la commande **enable** pour passer en mode d'exécution privilégié.

```
Switch>enable
```

```
Switch#
```

- **Étape 2 : Suppression du fichier d'informations de la base de données VLAN**

Dans le répertoire Flash, les informations de la base de données VLAN sont sauvegardées séparément des fichiers de configuration dans **vlan.dat**.

Pour effacer le fichier VLAN, exécutez la commande **delete flash:vlan.dat**

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Entrée]
Delete flash:vlan.dat? [confirm] [Entrée]
```

- **Étape 3 : Suppression du fichier de configuration initiale du commutateur de la mémoire vive non volatile (NVRAM)**

## TP1 : Configuration de base d'un commutateur (plateforme CISCO)

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm] [Entrée]
[OK]
Erase of nvram: complete
```

- **Étape 4 : Vérification de la suppression des informations du réseau local virtuel**

Vérifiez que la configuration VLAN a été supprimée à l'aide de la commande **show vlan**

```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 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
10 VLAN10	active	
30 VLAN30	active	
1002 fddi-default	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

- **Étape 5 : Rechargement du commutateur**

À l'invite du mode d'exécution privilégié, entrez la commande **reload** pour commencer le processus.

```
Switch#reload
Proceed with reload? [confirm] [Entrée]
%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
<résultat omis>
Press RETURN to get started! [Entrée]
Switch>
```

### III.3 Vérification de la configuration par défaut du commutateur

- **Étape 1 : passage en mode privilégié**

Vous pouvez accéder à toutes les commandes du commutateur en mode privilégié. Toutefois, comme un grand nombre des commandes du mode privilégié permettent de configurer des paramètres d'exploitation, l'accès privilégié doit être protégé par un mot de passe pour empêcher toute utilisation non autorisée. Parmi les commandes du mode privilégié, on retrouve celles du mode d'exécution utilisateur, ainsi que la commande **configure** qui donne accès aux autres modes de configuration.

```
Switch>enable
Switch#
```

## TP1 : Configuration de base d'un commutateur (plateforme CISCO)

Notez que l'invite a changé dans la configuration pour représenter le mode d'exécution privilégié.

- **Étape 2 : Examen de la configuration en cours d'exécution du commutateur**

**a.** Examinez la configuration en cours d'exécution en exécutant la commande **show running-config**.

1. Combien d'interfaces Fast Ethernet le commutateur possède-t-il ?
2. Combien d'interfaces Gigabit Ethernet le commutateur possède-t-il ?
3. Quelle est la plage de valeurs affichée pour les lignes vty ?

**b.** Examinez le contenu actuel de la mémoire vive non volatile (NVRAM) en exécutant la commande

**show startup-config**.

1. Pourquoi le commutateur donne-t-il cette réponse ?

**c.** Examinez les caractéristiques de l'interface virtuelle VLAN1 en exécutant la commande **show interface vlan1**.

1. Une adresse IP est-elle définie sur le commutateur ?
2. Quelle est l'adresse MAC de cette interface de commutateur virtuelle ?
3. Cette interface fonctionne-t-elle ?

**d.** À présent, affichez les propriétés IP de l'interface à l'aide de la commande **show ip interface vlan1**.

1. Quel résultat voyez-vous ?

- **Étape 3 : Affichage des informations du logiciel Cisco IOS**

**a.** Affichez les informations du logiciel Cisco IOS à l'aide de la commande **show version**.

1. Quelle version de Cisco IOS le commutateur exécute-t-il ?
2. Quel est le nom de fichier de l'image système ?
3. Quelle est l'adresse MAC de base de ce commutateur ?

- **Étape 4 : Examen des interfaces Fast Ethernet**

**a.** Examinez les propriétés par défaut de l'interface Fast Ethernet utilisée par PC1 à l'aide de la commande **show interface fastethernet 0/18**.

```
Switch#show interface fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.5c36.4412 (bia 0060.5c36.4412)
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  <résultat omis>
```

1. Quel est l'état de l'interface (activée ou désactivée) ?
2. Quel événement pourrait activer une interface ?
3. Quelle est l'adresse MAC de l'interface ?
4. Quels sont les paramètres de vitesse et de mode bidirectionnel de l'interface ?

## TP1 : Configuration de base d'un commutateur (plateforme CISCO)

- **Étape 5 : Examen des informations du réseau local virtuel**

a. Examinez les paramètres du réseau local virtuel par défaut pour le commutateur à l'aide de la commande **show vlan**.

1. Quel est le nom du VLAN 1 ?
2. Quels ports se trouvent dans ce VLAN ?
3. Le VLAN 1 est-il actif ?
4. Quel est le type de VLAN par défaut ?

- **Étape 6 : Examen de la mémoire Flash**

a. Deux commandes permettent d'examiner la mémoire Flash, **dir flash:** ou **show flash**. Exécutez l'une de ces commandes pour examiner le contenu du répertoire Flash.

1. Quels sont les fichiers ou répertoires trouvés ?

- **Étape 7 : Examen et enregistrement du fichier de configuration initiale**

À l'étape 2, vous avez appris que le fichier de configuration initiale n'existait pas. Apportez une modification à la configuration du commutateur et enregistrez-la. Tapez les commandes suivantes :

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S1
S1(config)#exit
S1#
```

Pour enregistrer le contenu du fichier de configuration en cours dans la mémoire vive non volatile, exécutez la commande **copy running-config startup-config**.

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

À présent, affichez le contenu de la mémoire vive non volatile (NVRAM). La configuration en cours a été enregistrée sur la mémoire vive non volatile (NVRAM).

### III.4 Création d'une configuration de base de commutateur

- **Étape 1 : Attribution d'un nom au commutateur**

Passez en mode de configuration globale. Le mode de configuration permet de gérer le commutateur. Tapez les commandes de configuration (une par ligne). Remarquez que l'invite de ligne de commande change pour refléter le nom de commutateur et l'invite actuels. Voici une liste des commandes utilisées.

```
Switch#configure terminal
Switch(config)#hostname S1
S1(config)#exit
```

## TP1 : Configuration de base d'un commutateur (plateforme CISCO)

- **Étape 2 : Définition des mots de passe d'accès**

Passez en mode config-line pour la console. Attribuez au mot de passe de connexion la valeur TelecomAT. Configurez également les lignes vty 0 à 15 en utilisant le mot de passe TelecomAT.

```
S1#configure terminal
S1(config)#line console 0
S1(config-line)#password TelecomAT
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password TelecomAT
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

- **Étape 3 : Définition des mots de passe du mode de commande**

Définissez TPRT comme mot de passe secret actif.

```
S1(config)#enable secret TPRT
```

- **Étape 4 : Configuration de l'adresse de la couche 3 du commutateur**

Définissez l'adresse IP du commutateur sur 172.17.99.11 avec 255.255.255.0 comme masque de sous-réseau sur l'interface virtuelle interne VLAN 99. (Le VLAN 99 est réservé à des fins de gestion et ne dispose pas d'interface physique).

Vous devez créer le réseau local virtuel sur le commutateur avant d'affecter l'adresse.

```
S1(config)#vlan 99
S1(config-vlan)#exit
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

- **Étape 5 : Affectation des ports sur le réseau local virtuel du commutateur**

Affectez Fastethernet 0/1, 0/8 et 0/18 aux ports sur VLAN 99.

```
S1(config)#interface fa0/1
S1(config-if)#switchport access vlan 99
S1(config-if)#interface fa0/8
S1(config-if)#switchport access vlan 99
S1(config-if)#interface fa0/18
S1(config-if)#switchport access vlan 99
S1(config-if)#exit
```

- **Étape 6 : Définition de la passerelle par défaut du commutateur**

## TP1 : Configuration de base d'un commutateur (plateforme CISCO)

S1 étant un commutateur de couche 2, il prend des décisions de transfert en fonction de l'entête de la couche 2. Si plusieurs réseaux sont connectés à un commutateur, vous devez préciser la façon dont le commutateur transfère les trames de l'inter-réseau, car le chemin doit être déterminé sur la couche 3. Il faut pour cela spécifier une adresse de passerelle par défaut qui pointe vers un routeur ou commutateur de couche 3. Bien que cet exercice n'inclue pas de passerelle IP externe, considérez que vous connecterez le réseau local à un routeur pour un accès externe. En supposant que l'interface du réseau local soit 172.17.99.1 sur le routeur, la passerelle par défaut pour le commutateur est définie comme suit :

```
S1(config)#ip default-gateway 172.17.99.1
S1(config)#exit
```

- **Étape 7 : Configuration de l'adresse IP et de la passerelle par défaut pour PC1**

Connectez le PC1 sur l'interface Fast Ethernet 0/18 et définissez l'adresse IP de PC1 sur 172.17.99.21, avec 255.255.255.0 pour masque de sous-réseau. Configurez une passerelle par défaut de 172.17.99.11. Cliquez sur PC1, sur son onglet Desktop, puis sur IP configuration pour entrer les paramètres d'adressage.

- **Étape 8 : Vérification de la connectivité**

Pour vérifier que l'hôte et le commutateur sont correctement configurés, envoyez une requête **ping** au commutateur à partir de PC1. Si la requête ping échoue, rectifiez la configuration de l'hôte et du commutateur. Sachez que les requêtes ping doivent être relancées parfois deux fois avant d'aboutir.

- **Étape 9 : Configuration des paramètres de vitesse du port et du mode bidirectionnel pour une interface FastEthernet**

Configurez les paramètres de vitesse et du mode bidirectionnel sur Fast Ethernet 0/18. Utilisez la commande **end** pour retourner au mode d'exécution privilégié une fois que vous avez terminé.

```
S1#configure terminal
S1(config)#interface fastethernet 0/18
S1(config-if)#speed 100
S1(config-if)#duplex full
S1(config-if)#end
```

La détection automatique est définie par défaut sur l'interface Ethernet du commutateur. Ainsi, les paramètres optimaux sont négociés automatiquement. Vous ne devez configurer manuellement le mode bidirectionnel et la vitesse que si un port doit fonctionner à une vitesse et un mode bidirectionnel définis.

Notez comment la liaison entre PC1 et le commutateur S1 a été désactivée. Supprimez les commandes speed 100 et full duplex. Vérifiez à présent les paramètres sur l'interface Fast Ethernet à l'aide de la commande **show interface fa0/18**.

## TP1 : Configuration de base d'un commutateur (plateforme CISCO)

### S1#show interface fastethernet 0/18

```
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is lance, address is 0060.5c36.4412 (bia 0060.5c36.4412)
  MTU 1500 bytes, BW100000 Kbit, DLY 1000 usec,
    reliability 255/255,txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  <Résultat omis>
```

- **Étape 10 : Enregistrement de la configuration**

Vous avez terminé la configuration de base du commutateur. Sauvegardez le fichier de configuration en cours dans la mémoire vive non volatile (NVRAM) pour vous assurer que les modifications ne soient pas perdues en cas de redémarrage du système ou d'une coupure de courant.

### S1#copy running-config startup-config

```
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```



## TP N° 02 Création et configuration d'un réseau segmenté en VLAN

### I. Objectifs pédagogiques

Le but de ce TP est de présenter la technologie VLAN, le concept de "Trunk" VLAN selon Cisco Systems et l'implémentation de la technologie en général.

- Créer une configuration de VLANs niveau 1
- Configuration d'un port en mode « Access »
- Configuration d'un port en mode « Trunk »

### II. Partie théorique

#### II.1 Définition d'un VLAN

Une topologie sans VLAN est représentée dans la figure 01. Dans ce scénario, chaque Switch peut connecter plusieurs machines dans un même sous réseau. Si l'on souhaite utiliser plusieurs sous réseaux, il nous faut alors plusieurs Switchs.

De plus, les machines d'un même sous réseau seront forcément regroupées de manière physique. Imaginons que le sous réseau 192.168.1.0 /24 soit à l'étage 1, et le sous réseau 192.168.2.0 /24 à l'étage 2 de notre entreprise, comment faire si nous souhaitons placer à l'étage 2 des utilisateurs du sous réseau 192.168.1.0 /24 ? L'ajout d'un câble jusqu'au Switch du niveau 1 est obligatoire, afin de placer un nouveau Switch au niveau 2.

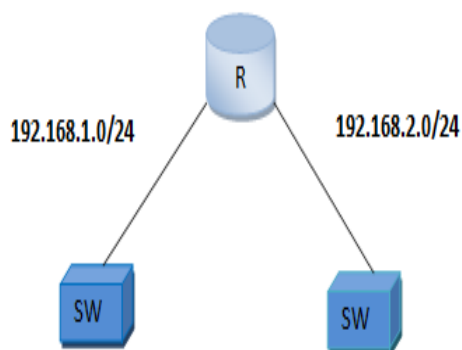


Figure II.1 : Topologie sans VLAN

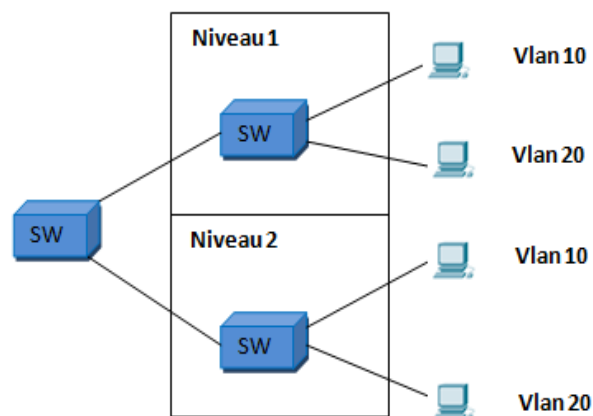


Figure II.2 : Topologie avec VLAN

L'idéal serait de pouvoir connecter les utilisateurs à n'importe quel Switch, en les gardant dans leurs sous réseaux respectifs.

Dans notre réseau, **un VLAN va correspondre à un sous réseau.**

## TP N° 02 Création et configuration d'un réseau segmenté en VLAN

Par exemple : 192.168.1.0 /24 sera le **VLAN 10**, 192.168.2.0 /24 sera le **VLAN 20** (le numéro du VLAN est choisi par l'administrateur réseau).

Le principe est simple : on configure les ports des Switch, afin qu'ils appartiennent à un certain VLAN. Ensuite, on peut connecter les utilisateurs sur n'importe quel Switch, du moment que le port associé est configuré dans le bon VLAN.

Comme il est mentionné dans la figure II.2 (le Switch principal sera un Switch de niveau 3), l'utilisateur pourra toujours se trouver dans le sous réseau voulu avec les différents Switch utilisés.

Avec des VLAN, les hôtes d'un même sous réseau ne sont plus rassemblées de manière physique (connectées au même Switch), mais de manière **logique** [3].

### II.2 Types de VLAN

Nous pouvons dénombrer trois types de VLAN [3, 4, 5], même si en général, nous n'utiliserons que le premier.

- **VLAN de niveau 1**, ou encore appelé VLAN par port. Il s'agit ici de configurer les ports du switch pour les placer dans le bon VLAN.
- **VLAN de niveau 2**, se base sur les adresses MAC. En fonction de l'adresse MAC source des frames reçues, le switch va placer ces dernières dans un certain VLAN. Un serveur va contenir la liste de correspondance VLAN / adresse MAC.
- **VLAN de niveau 3**, se base sur l'IP source des paquets reçus.

Les VLAN de niveau 2 et 3 permettent bien évidemment de gagner en souplesse et en mobilité. Néanmoins, ces deux types sont rarement utilisés.

## III. Partie pratique

### III.1 Mise en place de la topologie et adressage :

#### a) Schéma de topologie et adressage :

- A l'aide de l'outil « Packet Tracer », schématiser le réseau de la figure II.3 composé d'un commutateur (Switch), et quatre ordinateurs. Choisissez un Switch de type 2950-24 et des PCs génériques (PC-PT).
- Configurez les adresses IP et masques correspondants aux postes PC1 à PC4.

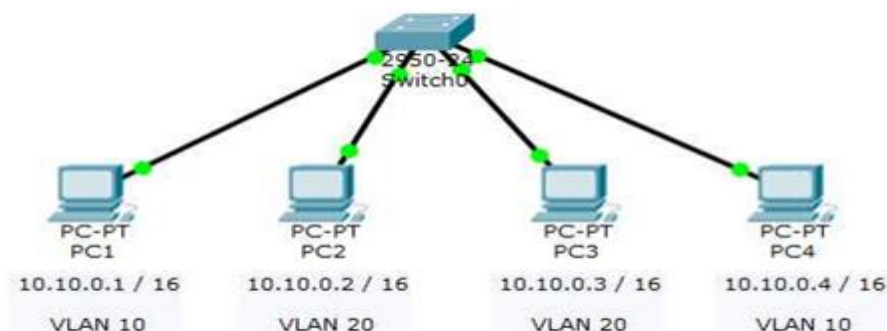


Figure II.3 Topologie de VLANs (Niveau 1) sur un seul Switch

## TP N° 02 Création et configuration d'un réseau segmenté en VLAN

### b) Table d'adressage :

Périphérique	Adresse IP	Périphérique	AdresseIP	Masque de sous-réseau
PC1	10.10.0.1	PC2	10.10.0.2	255.255.0.0
PC4	10.10.0.4	PC3	10.10.0.3	255.255.0.0

Tableau II.1 La table d'adressage PCs (1, 2, 3, 4).

### c) Affecter un nom au Switch

Nous allons donner un nom au Switch, entrez les commandes suivantes :

```
Switch#configure terminal  
Switch(config)#hostname SW1  
SW1(config)#end
```

En absence d'une configuration spécifique, le Switch considère que tous les ports font partie d'un même VLAN « par défaut », dont le numéro de VLAN (ou VLAN Id) est 1. Dans ce contexte, toutes les machines communiquent « comme s'il n'y avait pas de VLAN ». Mais un VLAN peut également être repéré par un nom comme nous allons le voir. Avec un unique VLAN « par défaut » équivalent à « pas de VLAN ».

## III.2 Configuration de VLANs (Niveau 1) sur un seul Switch

On souhaite que le trafic entre PC1 et PC4 soit totalement isolé du trafic entre PC2 et PC3, c'est à dire qu'aucun échange ni observation ne puisse avoir lieu entre ces deux réseaux locaux virtuels. Pour cela, on va créer deux VLANs distincts : le 1<sup>er</sup> VLAN pour PC1, PC4 et le 2<sup>ème</sup> VLAN pour PC2, PC3.

On va définir ici des VLANs par port (VLAN physique ou VLAN de niveau 1) c'est à dire qu'on ne s'intéresse ici (au niveau du « filtrage » du Switch) ni aux adresses MAC des postes qui vont communiquer, ni à leurs adresses IP. Ainsi que vous avez dû le constater lors de la première partie du TP, en l'absence de configuration particulière, le Switch considère que tous les ports font partie du même VLAN par défaut et donc que toutes les machines communiquent comme s'il n'y avait pas de VLAN. Il faut donc configurer le Switch pour qu'il puisse reconnaître nos VLANs.

### III.2.1 Définir les VLANs

Il faut à présent définir le numéro de VLAN à affecter à la zone PVID (Port VLAN ID). Par défaut, tous les ports du Switch appartiennent à un Default\_VLAN qui a la valeur 1 comme numéro de VLAN. Il faut donc donner des VLAN ID différents aux deux VLANs. Par exemple, 10 pour le 1<sup>er</sup> VLAN et 20 pour le 2<sup>ème</sup> VLAN.

Vous allez donc créer les VLAN (10) « vlan10 » et le VLAN (20) « vlan20 ». Pour cela, entrez les commandes suivantes :

```
SW1>enable  
SW1#config t  
SW1(config)#vlan 10 (on affecte le numéro au vlan)
```

## TP N° 02 Création et configuration d'un réseau segmenté en VLAN

```
SW1(config-vlan)#name vlan10 (on affecte le nom au vlan)
SW1(config-vlan)#vlan 20
SW1(config-vlan)#name vlan20
SW1(config-vlan)#exit
Sw1#show vlan
```

Vous devez maintenant voir les 3 VLAN (1, 10 et 20 ainsi que leurs noms). Remarquez que les ports ne sont pour l'instant affectés qu'au seul VLAN 1 par défaut.

### III.2.2 Associer les ports à leurs VLANs

Il nous faut associer à présent les ports 1, 4 au VLAN 10 (vlan10) reliant les postes PC1 et PC4 et les ports 2, 3 au VLAN 20 (vlan20) reliant les postes PC2 et PC3.

- a) Entrez les commandes suivantes :

```
SW1#configure terminal
SW1(config)#interface fa 0/1
SW1(config-if)#switchport access vlan 10
SW1(config-if)# no shutdown (active le port qui passe de l'état down à up)
SW1(config)#end
```

- b) Entrez les commandes suivantes :

```
SW1#configure terminal
SW1(config)#interface fa 0/4
SW1(config-if)#switchport access vlan 10
SW1(config-if)# no shutdown
SW1(config)#end
SW1#show vlan
```

- c) Associez les ports fast Ethernet 0/2 et 0/3 au VLAN20 reliant les postes PC2 et PC3.

```
SW1(config)#interface fa 0/2
SW1(config-if)#switchport access vlan 20
SW1(config-if)# no shutdown
SW1(config)#interface fa 0/3
SW1(config-if)#switchport access vlan 20
SW1(config-if)# no shutdown
SW1(config)#end
```

- d) Vérifiez que les ports sont bien affectés aux bons VLANs.

```
SW1#show vlan
```

- e) Faites des ping entre PC (entre PC d'un même VLAN, vers des PC de l'autre VLAN et vers une machine inconnue, etc.). Observez bien les réponses obtenues.
- f) Vérifiez en particulier que les trames générées par le ping d'une machine sur un VLAN n'atteignent pas les machines de l'autre VLAN.

## TP N° 02 Création et configuration d'un réseau segmenté en VLAN

### III.2.3 Permuter deux postes

Nous avons associé, actuellement, les postes PC1 et PC4 aux ports 1 et 4 définis comme appartenant au VLAN 10 (vlan10) et les postes PC2 et PC3 aux ports 2 et 3 définis comme appartenant au VLAN 20 (vlan20). Mais, en principe, un commutateur travaille au niveau 2 (adresses MAC) et il constitue à cet effet une table des adresses MAC associées à chaque port. Cette table peut d'ailleurs être visualisée au moyen de la commande **show mac-address-table**.

- a) Exécutez donc la commande :

SW1#show mac-address-table

- b) Permutez maintenant, sur le Switch, les connecteurs 1 et 2 correspondant aux postes PC1 et PC2 et attendez que les diodes clignotantes passent de l'orange au vert (le Switch est en train d'apprendre les adresses MAC).
- c) Faites sur PC1 une série de ping en direction des autres postes ! Même chose sur PC2...

Que constatez-vous ?

On observe bien à présent que le PC2 a changé de VLAN et que c'est donc bien la position « Physique » du connecteur qui va indiquer à quel VLAN est connectée la machine, quelle que soit son adresse MAC ! On a donc bien un VLAN par port ou de niveau 1 (et non pas par adresse MAC qui serait un VLAN de niveau 2).

### III.3 Configuration de VLANs (Niveau 1) sur deux Switchs

Lorsque les VLANs sont répartis sur plusieurs commutateurs (2 dans notre cas), un lien particulier est mis en place entre les commutateurs. Ce lien configuré en mode **Trunk**, transmet la trame en ajoutant 4 octets indiquant le vlan d'appartenance. La configuration de l'interface se fait à partir du mode de configuration globale.

#### III.3.1 Préparation de la maquette

1. Réalisez le montage suivant (en ajoutant un autre Switch et trois PCs ordinaires).
2. Configurez les adresses IP et masques correspondants aux postes PC5, PC6 et PC7.
3. Connectez les deux Switchs en utilisant un câble croisé.

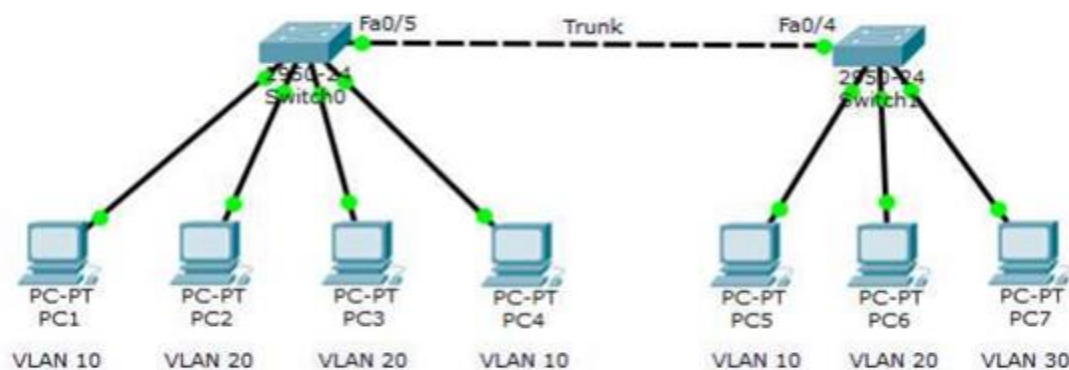


Figure II.4 Topologie de VLANs (Niveau 1) sur deux Switchs

## TP N° 02 Création et configuration d'un réseau segmenté en VLAN

- Table d'adressage :

Périphérique	Adresse IP	Masque de sous-réseau
PC5	10.10.0.5	255.255.0.0
PC6	10.10.0.6	255.255.0.0
PC7	10.10.0.7	255.255.0.0

Tableau II.2 La table d'adressage PCs (5,6, 7)

### III.3.2 Affecter un nom au Switch2

Entrez les commandes suivantes :

```
Switch#configure terminal
Switch(config)#hostname SW2
SW2(config)#end
```

### III.3.3 Configuration de VLANs sur le Switch2

On va créer trois VLANs distincts : le VLAN 10 pour le PC5, le VLAN 20 pour le PC6 et enfin VLAN 30 pour le PC7.

Entrez les commandes suivantes :

```
SW2>enable
SW2#config t
SW2(config)#vlan 10
SW2(config-vlan)#name vlan10
SW2(config-vlan)#vlan 20
SW2(config-vlan)#name vlan20
SW2(config-vlan)#vlan 30
SW2(config-vlan)#name vlan30
SW2(config-vlan)#exit
```

### III.3.4 Associer les ports à leurs VLANs

Il nous faut associer le port 0/1 au VLAN 10 (vlan10) reliant le poste PC5, le port 0/2 au VLAN 20 (vlan20) reliant le poste PC6 et le port 0/3 au VLAN 30 (vlan30) reliant le poste PC7.

1. Entrez les commandes suivantes :

```
SW2#config t
SW2(config)#int fa 0/1
SW2(config-if)#switchport access vlan 10
SW2(config-if)# no shutdown
SW2(config)#int fa 0/2
SW2(config-if)#switchport access vlan 20
SW2(config-if)# no shutdown
SW2(config)#int fa 0/3
SW2(config-if)#switchport access vlan 30
SW2(config-if)# no shutdown
SW2(config)#end
```

2. Vérifiez que les ports sont bien affectés aux bons VLANs.

```
SW2#show vlan
```

## TP N° 02 Création et configuration d'un réseau segmenté en VLAN

3. Faites des ping entre PC (entre PC d'un même VLAN, vers des PC de l'autre VLAN et vers une machine inconnue...). Observez bien les réponses obtenues.

### *III.3.5 Configuration des ports Trunk entre les deux Switchs*

Nous allons maintenant créer nos ports Trunk sur les interfaces Fa0/5 et Fa0/4 de nos deux Switchs. Le port Trunk va permettre, au travers des trames 802.1q de faire transiter des trames tagguées (ou étiquetées) selon un VLAN ou un autre afin que tous les VLAN autorisés puissent passer au travers d'un même lien. Plus clairement, c'est un port qui peut faire passer plusieurs VLAN vers un autre élément actif. Cela permet, dans notre cas, de faire communiquer les VLANS 10, 20 et 30 entres des éléments connectés à deux Switchs différents.

1. Entrez les commandes suivantes pour Switch1 « SW1 »:

```
SW1#config t  
SW1(config)#int fa 0/5  
SW1(config-if)#switchport mode trunk  
SW1(config-if)# exit
```

2. Entrez les commandes suivantes pour Switch2 « SW2 »:

```
SW2#config t  
SW2(config)#int fa 0/4  
SW2(config-if)#switchport mode trunk  
SW2(config-if)# exit
```

3. Maintenant, faites des ping entre PC (entre PC d'un même VLAN et des VLANs différents). Observez bien les réponses obtenues.

## TP N°03 : Configuration de routage inter-VLAN

### I. Objectifs pédagogiques

Nous avons abordé dans le TP précédent la notion de création et configuration des VLAN au sein des réseaux, mais nous avons très peu parlé du routage entre les VLAN. Deux solutions s'offrent à nous, utiliser un routeur, ou utiliser un Switch de niveau 3. Nous parlerons rapidement de la configuration d'un routeur, avant de voir plus en détail les Switchs de niveau 3.

- Configuration d'un routeur et d'un Switch niveau 3 (L3 SW)
- Configuration du routage inter-VLANs

### II. Partie théorique

Il existe différentes méthodes possibles pour effectuer un routage inter-VLANs, les méthodes présentées sont : Router on A Stick, Multilayer Switch [3,6].

#### II.1 Router On A Stick

« Router On A Stick » c'est la solution la plus courante pour configurer le routage entre VLAN, en utilisant un routeur. L'exemple suivant montre par la Figure III.1 une architecture composée par 2 VLAN différents. Pour communiquer d'un VLAN à un autre, il est obligatoire de passer par un routeur. Dans la configuration dite Router On A Stick, il faut créer un trunk entre le switch et le routeur. Tous les messages allant d'un VLAN à un autre, passeront par ce trunk. Cela a un avantage et un inconvénient.

Avantage : un seul port est nécessaire sur le switch et le routeur. Même si le routeur permet de connecter 20 VLAN entre eux.

Inconvénient : cela crée un goulot d'étranglement. Tout le trafic inter-VLAN allant d'un port à un autre du switch, devra remonter jusqu'au routeur par ce lien.

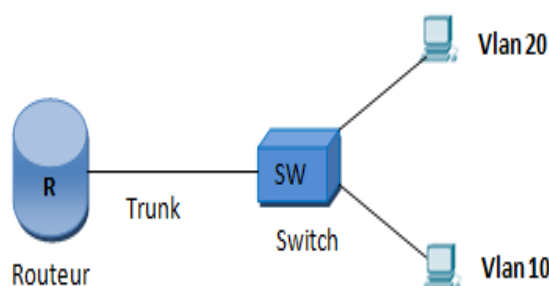


Figure III.1 Routage inter-vlan : Router on a stick



## TP N°03 : Configuration de routage inter-VLAN

### II.2 Multilayer Switch (Layer 3)

Tout d'abord, qu'est-ce qu'un switch de niveau 3 ?

Il s'agit simplement d'un switch qui peut réaliser la fonction du routage. Tandis que de nombreuses opérations propres aux routeurs ne sont pas effectuées sur les switches L3.

Dans la Figure III.2, le switch L3 pourra acheminer les données sans aucun problème allant simultanément de PC1 à PC2 et de PC3 à PC4, alors que dans une topologie Routeur On A Stick, le lien Routeur – Switch aurait potentiellement été saturé.

La latence s'en trouve alors réduite. De plus, le coût par port est relativement faible par rapport à un routeur. Par contre, le prix d'un switch L3 est tout de même bien plus élevé que celui d'un switch L2.

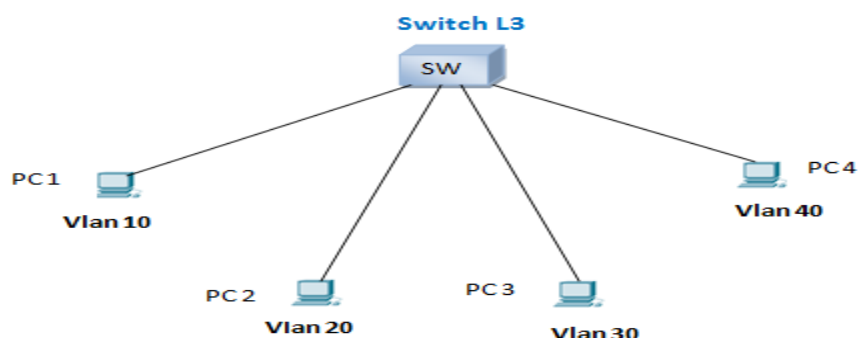


Figure III.2 Routage inter vlan en utilisant un switch (Layer 3)

## III. Partie pratique

### III.1 Configuration du routage inter-VLAN avec un routeur Router On A Stick

Cette section montre la façon de procéder pour faire communiquer trois hôtes de VLANs différents. Pour cela, nous allons mettre en place le routage inter-VLAN.

Procédure :

1. Création des VLANs.
2. Association des VLANs aux ports du commutateur.
3. Configuration de l'interface reliant le commutateur au routeur/
4. Mise en place du routage inter-VLANs.

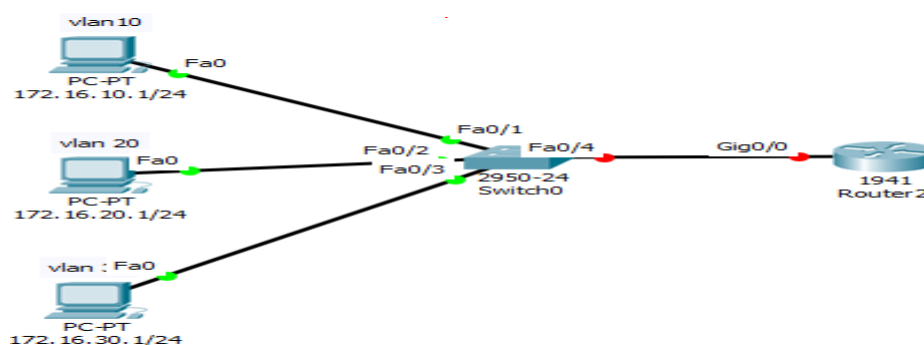


Figure III.3 Simulation du routage inter-vlan : Router on a stick

## TP N°03 : Configuration de routage inter-VLAN

### III.1.1 Création des vlans

```
switch# conf t
switch(conf)# vlan 10
switch(conf)# name Vlan10
switch(conf)# vlan 20
switch(conf)# name Vlan20
switch(conf)# vlan 30
switch(conf)# name Vlan30
```

Vérifiez si les vlan ont été bien créés.

```
switch(conf)#exit
switch#show vlan
```

### III.1.2 Association des VLANs créés avec les ports du commutateur :

```
switch(conf)# int fa 0/1
switch(conf-int)# switchport access vlan 10
switch(conf-int)# no shutdown
switch(conf-int)#exit
switch(conf)#int fa 0/2
switch(conf-int)#switchport access vlan 20
switch(conf-int)#no shutdown
switch(conf-int)#exit
switch(conf)#int fa 0/3
switch(conf-int)#switchport access vlan 30
switch(conf-int)#no shutdown
switch(conf-int)#exit
```

### III.1.3 Mise en mode trunk de l'interface reliant le switch au routeur:

```
switch(conf)#int fa 0/4
switch(conf-int)#switchport mode trunk
switch(conf-int)#exit
```

### III.1.4 Mise en place du routage inter-VLANs :

```
Routeur#conf t
Routeur(conf)#int Gig 0/0
Routeur(conf-int)#ip address 192.168.1.254 255.255.255.0
Routeur(conf-int)#no sh
Routeur(conf-int)#exit
```

### III.1.5 Création des sous-interfaces

```
Routeur(conf)#int fa 0/0.1
Routeur(conf-subint)#encapsulation dot1Q 10
Routeur(conf-subint)#ip address 172.16.10.254 255.255.255.0
Routeur(conf-subint)#no sh
Routeur(conf-subint)#exit
Routeur(conf)#int fa 0/0.2
```

### TP N°03 : Configuration de routage inter-VLAN

```
Routeur(conf-subint)#encapsulation dot1Q 20
Routeur(conf-subint)#ip address 172.16.20.254 255.255.255.0
Routeur(conf-subint)#no sh
Routeur(conf-subint)#exit
Routeur(conf)#int fa 0/0.3
Routeur(conf-subint)#encapsulation dot1Q 30
Routeur(conf-subint)#ip address 172.16.30.254 255.255.255.0
Routeur(conf-subint)#no sh
Routeur(conf-subint)#exit
```

N'oubliez surtout pas de configurer sur chaque poste une passerelle qui sera pour cette partie :  
192.168.1.254

Notre routage inter-vlan est maintenant fonctionnel.

### III.2 Configuration du routage inter-VLAN avec des switch L3

- **PC1 : IP :172.16.10.2 Masque :255.255.0.0**
- **PC2 :IP :172.16.20.2 Masque :255.255.0.0**
- **PC2 :IP :172.16.30.2 Masque :255.255.0.0**

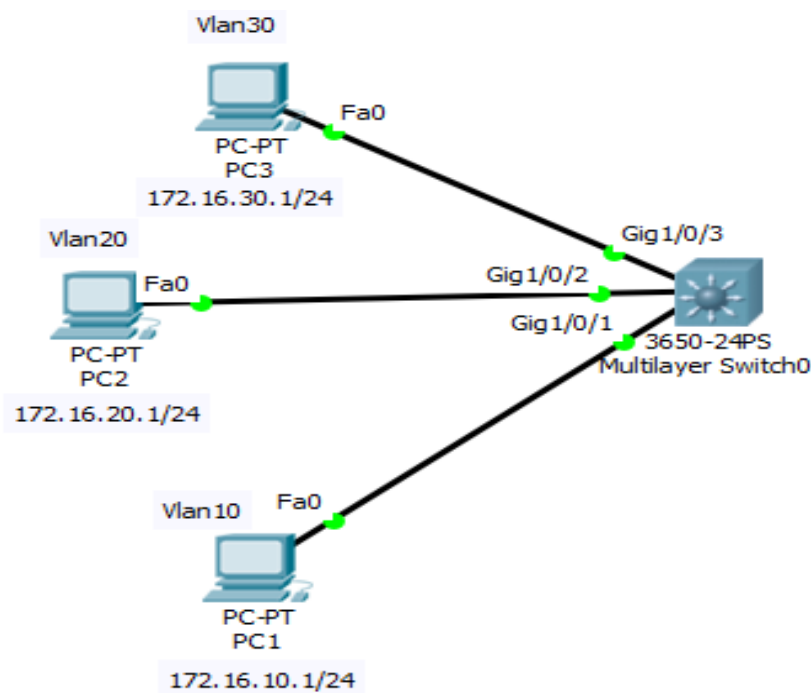


Figure III.4 Simulation du routage inter vlan en utilisant un switch (Layer 3)

#### III.2.1 Création des vlans

```
switch# conf t
switch(conf)# vlan 10
switch(conf-vlan)# name Vlan10
switch(conf-vlan)#exit
```

## TP N°03 : Configuration de routage inter-VLAN

```
switch(conf)# vlan 20  
switch(conf-vlan)# name Vlan20  
switch(conf-vlan)#exit
```

```
switch(conf)# vlan 30  
switch(conf-vlan)# name Vlan30  
switch(conf-vlan)#exit
```

- Vérifiez si les vlan ont été bien créés.

```
switch(conf)#exit  
switch#show vlan
```

### *III.2.2 Association des VLANs créés avec les ports du commutateur :*

```
switch(conf)# int gig 1/0/1  
switch(conf-int)# switchport access vlan 10  
switch(conf-int)# no shutdown  
switch(conf-int)#exit  
switch(conf)#int gig 1/0/2  
switch(conf-int)#switchport access vlan 20  
switch(conf-int)#no shutdown  
switch(conf-int)#exit  
switch(conf)#int gig 1/0/3  
switch(conf-int)#switchport access vlan 30  
switch(conf-int)#no shutdown  
switch(conf-int)#exit
```

### *III.2.3 Création des interfaces VLAN*

- **vlan 10**

```
switch(conf)# interface vlan 10  
switch(conf-if)# ip address 172.16.10.1 255.255.255.0  
switch(conf-if)#no shutdown  
switch(conf-if)#exit
```

- **vlan 20**

```
switch(conf)# interface vlan 20  
switch(conf-if)# ip address 172.16.20.1 255.255.255.0  
switch(conf-if)#no shutdown  
switch(conf-if)#exit
```

- **vlan 30**

### TP N°03 : Configuration de routage inter-VLAN

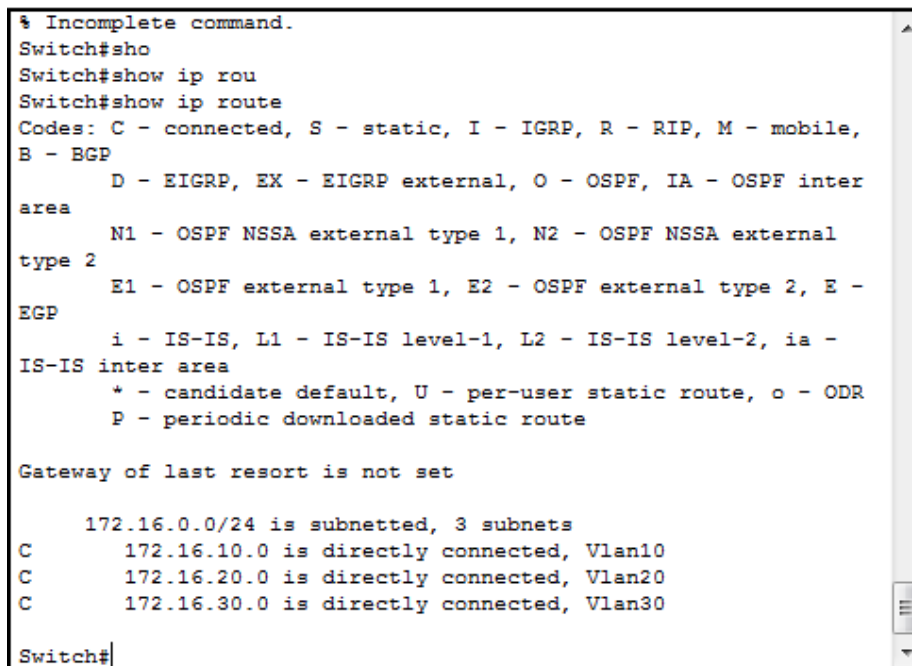
```
switch(conf)# interface vlan 30
switch(conf-if)# ip address 172.16.30.1 255.255.255.0
switch(conf-if)#no shutdown
switch(conf-if)#exit
switch(conf-if)#end
```

#### III.2.4 Activation du routage au niveau du switch (L3)

```
switch#
switch#conf t
switch(conf)# ip routing
switch(conf)# end
```

- Vérifiez la table de routage :

```
switch#exit
switch#show ip route
```



```
% Incomplete command.
Switch#sho
Switch#show ip rou
Switch#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

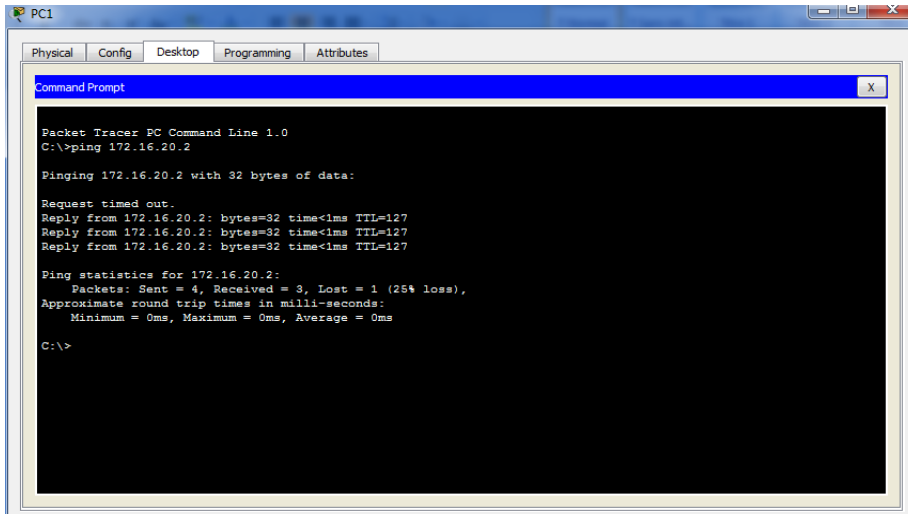
Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 3 subnets
C       172.16.10.0 is directly connected, Vlan10
C       172.16.20.0 is directly connected, Vlan20
C       172.16.30.0 is directly connected, Vlan30

Switch#
```

Voici le résultat du Test de connectivité entre les différents PCs :

### TP N°03 : Configuration de routage inter-VLAN



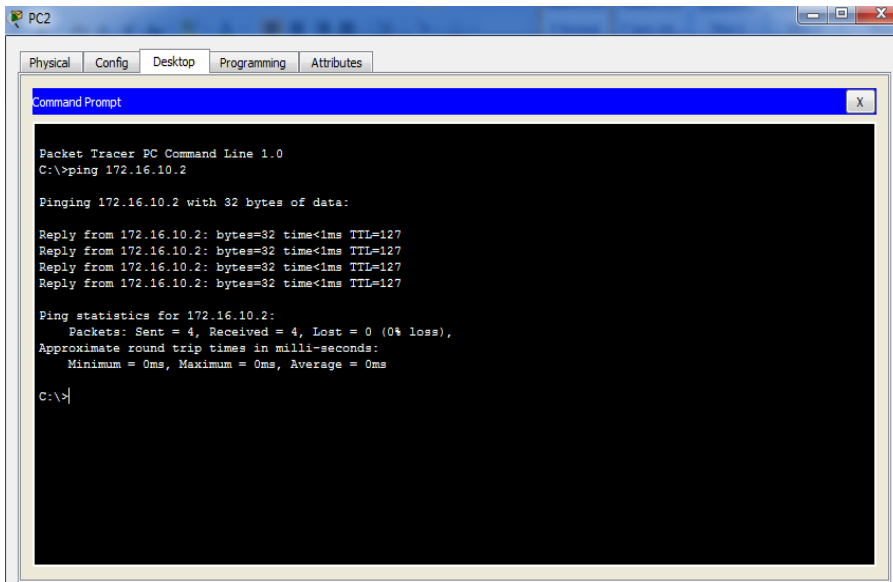
```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.20.2

Pinging 172.16.20.2 with 32 bytes of data:

Request timed out.
Reply from 172.16.20.2: bytes=32 time<1ms TTL=127
Reply from 172.16.20.2: bytes=32 time<1ms TTL=127
Reply from 172.16.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



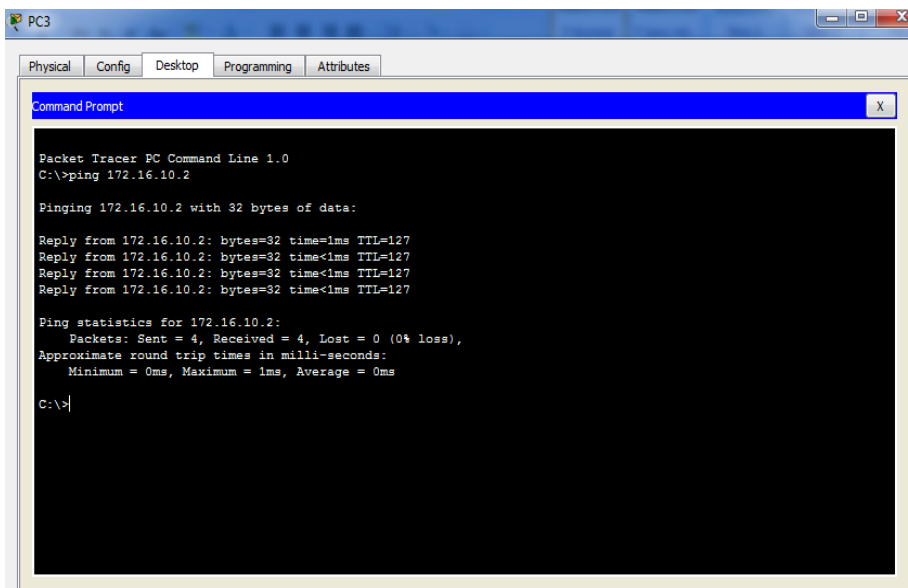
```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.2

Pinging 172.16.10.2 with 32 bytes of data:

Reply from 172.16.10.2: bytes=32 time<1ms TTL=127
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.2

Pinging 172.16.10.2 with 32 bytes of data:

Reply from 172.16.10.2: bytes=32 time<1ms TTL=127
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127
Reply from 172.16.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

## TP4 : Création d'un réseau avec des liens redondant

### I. Objectifs pédagogiques

Ce TP fournit des notions basiques sur la création d'une topologie de réseau redondante optimale en étudiant le fonctionnement du protocole STP (spanning tree protocol).

- Désactivation des liens redondants en utilisant le protocole STP.
- Déterminer le lien désactivé, puis influence sur l'élection du Root Bridge.
- Configuration du protocole Rapid spanning tree protocol (Rapid-STP).

### II. Partie théorique

Le protocole STP (Spanning Tree Protocol) est un protocole de la couche liaison de données, standardisé par la norme IEEE 802.1D, basé sur l'utilisation des ponts et des commutateurs. Il permet d'écartier les boucles dans un réseau en profitant toujours des topologies redondantes [7].

#### II.1 Problématique

En raison de minimiser l'effet d'une panne dans le réseau, généralement nous cherchons toujours à redonder les liens et les équipements, mais ceci peut provoquer un autre problème qui est les boucles dans le réseau.

Les sources des boucles dans un réseau peuvent résulter soit d'une erreur, ou d'une topologie redondante.

En absence du protocole STP, plusieurs problèmes peuvent survenir on peut citer [4,7]:

##### II.1.1 Tempête de diffusion

On appelle tempête de diffusion la tournée en rond des messages de diffusion [3,8].

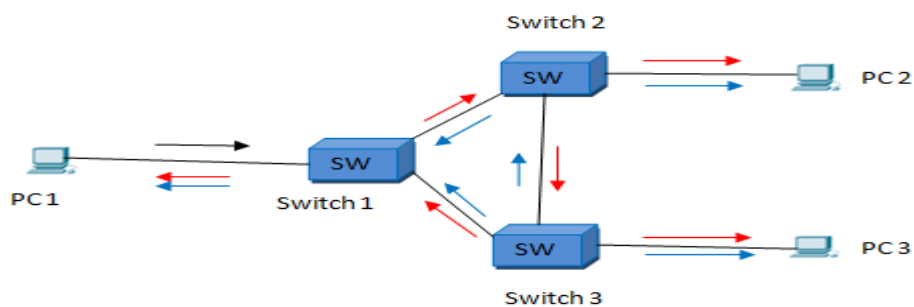


Figure IV.1 Tempête de diffusion

#### TP4 : Création d'un réseau avec des liens redondant

Comme il est mentionné dans l'exemple de la Figure IV.1, si le PC 1 envoie un message en diffusion, ce message va alors arriver jusqu'à S1. Comme c'est un message de diffusion, S1 va l'envoyer sur tous ses ports. Le message va alors partir vers S2 et S3. Considérons le message qui part vers S2. Quand le message arrivera sur S2, il sera alors transmis vers PC 2 et S3. Reçue par S3, le message va alors aller vers PC 3 et S1. Quand S1 va recevoir le Broadcast, il va l'envoyer à PC 1 et S2 [7].

Le message tournera de cette façon (sans arrêt), et cela va continuer d'une manière infinie. En conséquence, les liens vont finir par être saturés (en raison des Broadcast qui s'ajoutent). Les switches tombent en panne, donc aucune circulation de trafic dans le réseau.

##### II.1.2 Duplication de trame et instabilité de table CAM

- Dans la topologie redondante présentée par la Figure IV.2, Les PCs sont connectés aux deux commutateurs (switchs). Quand par exemple PC 2 émet une trame à PC 1, celle-ci sera envoyée à S1 et S2. Ces derniers vont ensuite transmettre la trame à PC1. PC 1 aura donc reçu la trame à deux reprises. Donc, ceci posera le problème des trames dupliquées [7].

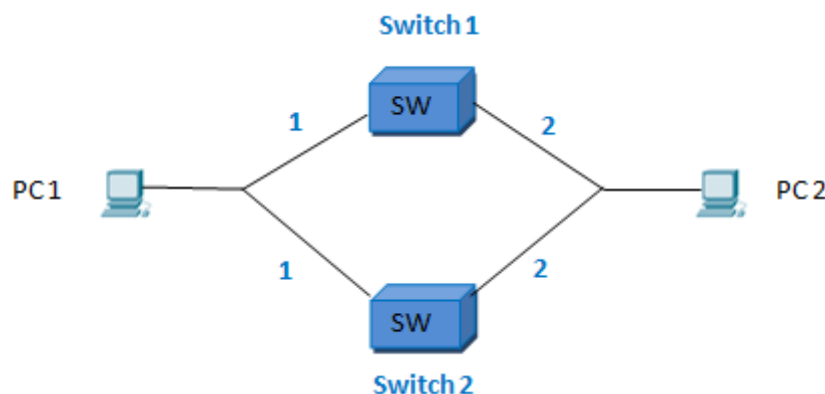


Figure IV.2 Topologie redondante.

## II.2 Fonctionnement du spanning tree

Spanning-Tree calcule une topologie sans boucle en 4 étapes [3,5 ,9]:

1. Choix d'un commutateur Root, un seul par topologie, qui sera le commutateur racine de la topologie, tous ses ports communiquent le trafic (ports Designated). Le commutateur qui possède l'identifiant "Bridge ID" (BID) le plus faible sera élu par la suite comme commutateur racine.
2. Un seul port Root sera désigné sur les autres commutateurs non-racine, qui porte la liaison dont le coût vers le commutateur Root est le minimal. C'est le seul à transférer du trafic.
3. Pour chaque segment physique reliant deux commutateurs, un port « Designated » est choisie quand c'est nécessaire. C'est le port qui a le coût vers le commutateur racine le plus petit qui est sélectionné, il est le seul à transférer le trafic.



## TP4 : Création d'un réseau avec des liens redondant

4. Les ports qui sont désigné comme « Root » et « Designated » transfèrent du trafic (état “Forwarding”) et les autres ports désactivent la liaison (état “Blocking”).

### III. Partie pratique

Dans cette partie nous allons mettre en place les notions théoriques précédemment évoquées, en comprenant le fonctionnement du protocole Spanning Tree dans un réseau,.

#### III.1 Scénario utilisé

Voici la topologie que nous utiliserons :

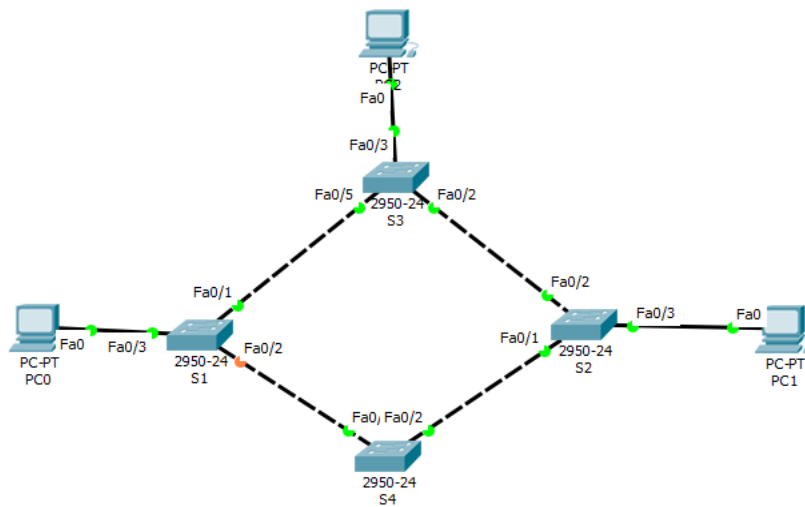


Figure IV.3 Schéma du réseau [9]

#### III.2 Comment activer Spanning Tree?

Vous vous demandez comment le protocole Spanning Tree est activé, alors le protocole STP est déjà activé. En utilisant la commande « **show running config** », nous pouvons déterminer la version utilisée.

## TP4 : Création d'un réseau avec des liens redondant

```
S2#sh ru
S2#sh running-config
Building configuration...

Current configuration : 1010 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
--More--
```

La version activée actuellement est la PVST, la version classique du STP. L'élection du Root Bridge est fondé sur deux critères sont les suivants :

- Priorité la plus basse.
- Adresse MAC la plus basse.

En utilisant la topologie de Figure IV.3, la commande « Show Spanning Tree » permet de voir l'état Spanning Tree :

```
S2>en
S2#sh sp
S2#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0009.7CC8.BA92
             This bridge is the root
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0009.7CC8.BA92
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
             Aging Time 20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/1        Desg FWD 19        128.1    P2p
Fa0/2        Desg FWD 19        128.2    P2p
Fa0/3        Desg FWD 19        128.3    P2p

S2#
```

## TP4 : Création d'un réseau avec des liens redondant

Les informations présentées sont celles du VLAN 1. Nous remarquons trois parties principales.

- La partie « Root ID ».
- La partie « Bridge ID ».
- La partie « Interface »

Observons maintenant le résultat de la même commande sur S1 :

```
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    32769
           Address    0009.7CC8.BA92
           Cost      38
           Port      1(FastEthernet0/1)
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
           Bridge ID Priority    32769 (priority 32768 sys-id-ext 1)
           Address    0060.7072.C7BB
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
           Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Root FWD 19        128.1    P2p
Fa0/2          Altn BLK 19        128.2    P2p
Fa0/3          Desg FWD 19        128.3    P2p

S1#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to down
```

La partie Root ID fait bien référence à S2. Nous pouvons voir que le port Fa 0/1 a le rôle Root.

### III.3 Choix du meilleur chemin/ désactivation des chemins redondants

Le tableau IV.1 présente différents cout STP pour multiples bandes passantes, dans notre scénario tous les liens sont en 100 Mb/s. Le coût est effectivement de 19 :

Bande Passante du lien	Cout STP
4 Mbps	250
10 Mbps	100
16 Mbps	62
100 Mbps	19
1 Gbps	4
10 Gbps	2
100 Gbps	1
1 Tbps	1
10 Tbps	1

Tableau IV.1 Cout STP de différentes bandes passantes.

#### TP4 : Création d'un réseau avec des liens redondant

- Pourquoi S1 a-t-il choisit le lien vers S4 comme étant le meilleur chemin ?

S1 a 2 liaisons égaux à disposition. Précédemment, nous avons dit qu'en cas d'égalité, c'est le voisin avec le plus faible BID qui sera selectionné.

- Comparons S3 et S4 :

```
S3#sh sp
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    32769
              Address    0009.7CC8.BA92
              Cost      19
              Port      2 (FastEthernet0/2)
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
  Bridge ID    Priority    32769 (priority 32768 sys-id-ext 1)
              Address    000A.41C3.2D90
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
              Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/3          Desg FWD 19        128.3    P2p
Fa0/5          Desg FWD 19        128.5    P2p
Fa0/2          Root FWD 19        128.2    P2p

S3#
```

```
%SYS-5-CONFIG_I: Configured from console by console

S4#sh sp
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    32769
              Address    0009.7CC8.BA92
              Cost      19
              Port      2 (FastEthernet0/2)
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
  Bridge ID    Priority    32769 (priority 32768 sys-id-ext 1)
              Address    00D0.5828.29A1
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
              Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Desg FWD 19        128.1    P2p
Fa0/2          Root FWD 19        128.2    P2p

S4#
```

Les deux switches possède une priorité identique. Par contre, S4 a une adresse MAC plus élevée. S3 a donc un BID plus faible. Ce qui montre pourquoi S1 a désactivé le port Fa 0/2.

### III.4 Les Timers STP

Pour comprendre les Timers STP, on va désactiver le port Fa 0/2 de S2, pour que S1 réactive son port Fa 0/2. Pour cela, nous commençons par désactiver le port.

```
S2(config)#interface fastEthernet 0/2
```

```
S2(config-if)#shutdown
```

Par la suite, on passe sur S1, et nous affichons l'état Spanning Tree :

```
S1#sh spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address     0009.7CC8.BA92
            Cost       38
            Port       1(FastEthernet0/1)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address     0060.7072.C7BB
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
            Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Root FWD 19        128.1   P2p
Fa0/2          Altn BLK 19        128.2   P2p
Fa0/3          Desg FWD 19        128.3   P2p

S1#
```

Nous observons que le port garde le mode Blocking pendant 20 secondes dont nous avons parlé. Ensuite, le port passe en mode Listening pendant 15 secondes (il écoute les BPDU).

```
S1#sh spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address     0009.7CC8.BA92
            Cost       38
            Port       2(FastEthernet0/2)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address     0060.7072.C7BB
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
            Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Desg FWD 19        128.1   P2p
Fa0/2          Root LSN 19        128.2   P2p
Fa0/3          Desg FWD 19        128.3   P2p

S1#
```

## TP4 : Création d'un réseau avec des liens redondant

Après, il passe en mode Learning (pendant 15 secondes) :

```
S1#sh spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address     0009.7CC8.BA92
            Cost       38
            Port       2 (FastEthernet0/2)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address     0060.7072.C7BB
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec

            Aging Time 20

Interface          Role Sts Cost          Prio.Nbr Type
-----
Fa0/1              Desg FWD 19           128.1   P2p
Fa0/2              Root LRN 19          128.2   P2p
Fa0/3              Desg FWD 19           128.3   P2p

S1#
```

Enfin, le port passe en mode Forwarding :

```
S1#sh spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
            Address     0009.7CC8.BA92
            Cost       38
            Port       2 (FastEthernet0/2)
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address     0060.7072.C7BB
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec

            Aging Time 20

Interface          Role Sts Cost          Prio.Nbr Type
-----
Fa0/1              Desg FWD 19           128.1   P2p
Fa0/2              Root FWD 19          128.2   P2p
Fa0/3              Desg FWD 19           128.3   P2p

S1#
```

### III.5 Rapid-PVST

Dans le but de rendre le processus Spanning Tree plus rapide, nous allons mettre en place le protocole Rapid PVST. Voici comment modifier le mode Spanning Tree :

#### TP4 : Création d'un réseau avec des liens redondant

```
Press RETURN to get started.

S1>en
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#sp
S1(config)#spanning-tree mo
S1(config)#spanning-tree mode ?
    pvst      Per-Vlan spanning tree mode
    rapid-pvst Per-Vlan rapid spanning tree mode
S1(config)#spanning-tree mode
```

En utilisant la commande **spanning-tree mode** ?

On aura le choix entre différentes modes. On sélectionnant Rapid-PVST, Car Il a le meme principe de fonctionnement comme PVST, mais il est plus rapide.

S1(config)# **spanning-tree mode rapid-pvst**

```
S1#show ru
S1#show running-config
Building configuration...

Current configuration : 1016 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
--More--
```

En répétant la manipulation sur tous les switches. Le résultat est relativement similaire à ce que nous avons en PVST :

#### TP4 : Création d'un réseau avec des liens redondant

```
S1#sh sp
S1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID      Priority    32769
              Address    0009.7CC8.BA92
              Cost      38
              Port      1(FastEthernet0/1)
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
  Bridge ID    Priority    32769 (priority 32768 sys-id-ext 1)
              Address    0060.7072.C7BB
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
              Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Root FWD 19        128.1    P2p
Fa0/2          Altn BLK 19        128.2    P2p
Fa0/3          Desg FWD 19        128.3    P2p

S1#
```

Maintenant, nous désactivons le port Fa 0/2 de S2, de manière à forcer le port FA 0/2 de S1 à passer en mode Forwarding, identiquement à la manipulation précédente.

Voici l'état actuel de S1 :

```
S1#sh sp
S1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID      Priority    32769
              Address    0009.7CC8.BA92
              Cost      38
              Port      1(FastEthernet0/1)
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
  Bridge ID    Priority    32769 (priority 32768 sys-id-ext 1)
              Address    0060.7072.C7BB
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
              Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Root FWD 19        128.1    P2p
Fa0/2          Altn BLK 19        128.2    P2p
Fa0/3          Desg FWD 19        128.3    P2p

S1#
```

Procédons à la coupure :

```
S2(config)#interface fastEthernet 0/2
```

```
S2(config-if)#shutdown
```



#### TP4 : Création d'un réseau avec des liens redondant

Passons rapidement sur S1, et observons l'état Spanning Tree :

```
S1#show sp
S1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address    0009.7CC8.BA92
             Cost      38
             Port      2 (FastEthernet0/2)
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address    0060.7072.C7BB
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15
sec
             Aging Time 20

Interface          Role Sts Cost      Prio.Nbr Type
-----
Fa0/1              Desg FWD 19       128.1   P2p
Fa0/2              Root FWD 19       128.2   P2p
Fa0/3              Desg FWD 19       128.3   P2p

S1#
```

Le changement a été déjà fait !, ce changement est très rapide, qu'il est très difficile de le percevoir.

## TP5 : Configuration du protocole Etherchannel entre commutateurs (Simulation sous packet-tracer)

### I. Objectifs pédagogiques

L'objectif de ce TP est d'étudier le principe de fonctionnement du protocole etherchannel, la technique d'agrégation qui permet d'utiliser des liens redondants entre multiples nœuds du réseau en configurons les deux protocoles **PAgP et LACP**.

- Configuration d'un EtherChannel avec **Cisco PAgP, LACP (802.3ad)**.
- Configuration d'un lien EtherChannel redondant.

### II. Partie théorique

#### II.1 Définition

Ether Channel est une technologie utilisé dans les réseaux permettant de concevoir une seule liaison logique en assemblant plusieurs liens physiques Ethernet similaire [10].

Le but est d'améliorer la vitesse et la tolérance aux pannes dans le réseau, ainsi elle permet de diminuer le nombre de liens utilisés.

Un lien EtherChannel peut rassembler de 2 à 8 liens actifs de 100 Mbit/s, 1 Gbit/s et 10 Gbit/s, et de 1 à 8 liens inactifs en réserve qui s'activent quand les liens actifs sont en panne [11].

#### II.2 Négociation de l'agrégation

L'agrégation des liens est conçue avec deux techniques [10]:

- Statique: l'agrégation est forcée, en utilisant la négociation de Trunk. Soit le Trunk est créé d'une manière manuelle, ou bien est négocié par les Switchs.
- Dynamique: dans ce cas l'agrégation utilise un protocole de négociation, il existe deux protocoles :
  - a) **PAgP**(Port Agregation Protocol) est un protocole crée par Cisco, le principe de base de ce protocole est basé sur ce qu'on appelle le mode. Ce dernier peut avoir deux valeurs : auto, desirable.
    - mode auto : la négociation ne commence pas par le système, mais elle va etre initiée par le système distant.
    - mode désirable : la négociation est initié par le système lui-même en utilisant le protocole PAgP.
  - b) **LACP** (Link Agregation Control Protocol) est un protocole représenté par la norme 802.3ad, son fonctionnement est basé sur deux modes : passive et active. la différence entre les deux modes est focalisée sur l'initiative de démarrer la négociation (mode active) ou attendre seulement la négociation du système distant (mode passive).

### III. Partie pratique :

#### III.1 Configuration d'un EtherChannel avec Cisco PAgP

##### 1. Etape 01 : Mise en place de la topologie

- a. Réalisez le montage du schéma suivant, en choisissant trois commutateurs de type 2960-24TT, des câbles droits.

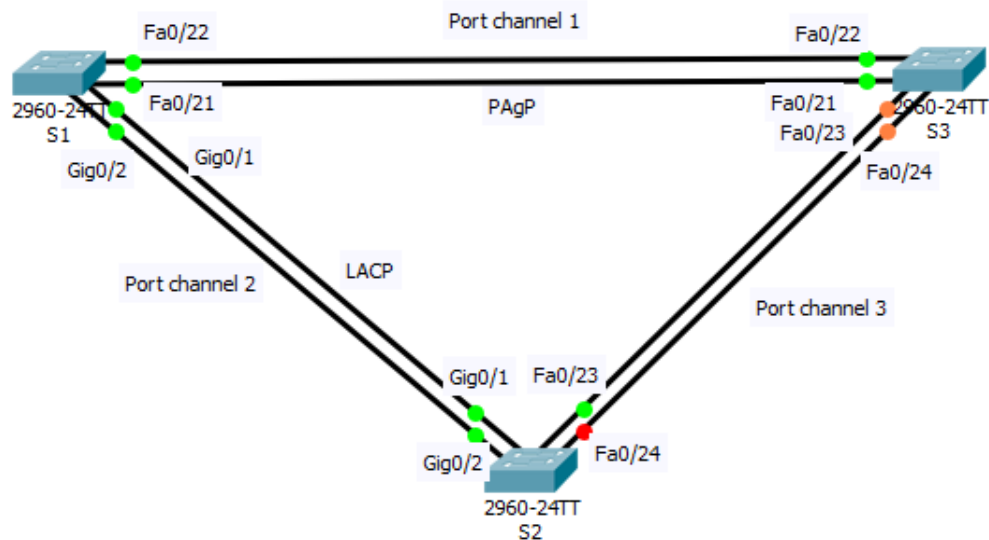


Figure V.1 Schéma du réseau

- b. Affectez un nom d'hôte à chaque commutateur, convenablement au schéma de topologie.

```
Switch(config)# hostname S1
Switch(config)# hostname S2
Switch(config)# hostname S3
```

- c. Configurez tous les ports requis en mode Trunk, en fonction des connexions entre les périphériques.

**Remarque :** Le mode défini par défaut sur un commutateur 2960 est le mode automatique dynamique, les liaisons doivent être configurées en mode Trunk, sinon les ports restent des ports d'accès.

```
S1(config)# interface range g0/1 - 2
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# interface range f0/21 - 22
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# end
```

```
S2(config)# interface range g0/1 - 2
S2(config-if-range)# switchport mode trunk
```

## TP5 : Configuration du protocole Etherchannel entre commutateurs Simulation sous packet-tracer

```
S2(config-if-range)# interface range f0/23 - 24
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# end
```

```
S3(config)# interface range f0/21 - 24
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# end
```

### 2. Etape 02 : Configuration du protocole Cisco PAgP

Au cours de la configuration des EtherChannels, la désactivation des ports physiques regroupés sur les deux périphériques est très recommandée avant de les configurer. Sinon, l'utilitaire de protection de configuration incorrecte EtherChannel peut mettre ces ports en état « err-disabled ». Les ports et les canaux de port peuvent être réactivés après la configuration d'EtherChannel [12].

#### 2.1. Configurez Port Channel 1

- Le premier EtherChannel conçu pour cette étape relie les ports F0/22 et F0/21 entre S1 et S3. Avec la commande **show interfaces trunk** vous pouvez vérifier qu'il y a une liaison de **trunking** active pour ces deux liaisons.

```
S1#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/21    on        802.1q         trunking    1
Fa0/22    on        802.1q         trunking    1
Gig0/1    on        802.1q         trunking    1
Gig0/2    on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/21    1-1005
Fa0/22    1-1005
Gig0/1    1-1005
Gig0/2    1-1005

Port      Vlans allowed and active in management domain
Fa0/21    1
Fa0/22    1
Gig0/1    1
Gig0/2    1

Port      Vlans in spanning tree forwarding state and not
pruned
Fa0/21    1
Fa0/22    1
Gig0/1    1
--More--
```

- Au niveau des deux commutateurs, insérez les ports F0/21 et F0/22 au Port Channel 1 grâce à la commande **channel-group 1 mode desirable**.  
L'option mode desirable : permet au commutateur de négocier de manière active la formation d'une liaison PAgP.

```
S1(config)# interface range f0/21 - 22
S1(config-if-range)# shutdown
S1(config-if-range)# channel-group 1 mode desirable
S1(config-if-range)# no shutdown
```

```
S3(config)# interface range f0/21 - 22
S3(config-if-range)# shutdown
S3(config-if-range)# channel-group 1 mode desirable
S3(config-if-range)# no shutdown
```

## TP5 : Configuration du protocole Etherchannel entre commutateurs Simulation sous packet-tracer

- c. Configurez l'interface logique d'une manière qu'elle devienne un trunk en exécutant tout d'abord la commande **interface port-channel number**, ensuite la commande **switchport mode trunk**. Ajoutez cette configuration aux deux commutateurs.

```
S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk
```

```
S3(config)# interface port-channel 1
S3(config-if)# switchport mode trunk
```

### 2.2.Vérifiez l'état de Port Channel 1.

- a. Afin de vérifier qu'EtherChannel fonctionne sur les deux commutateurs, exécutez la commande suivante : **show etherchannel summary**.

Cette commande affiche (le type d'EtherChannel, les ports utilisés, les états des ports).

```
%SYS-5-CONFIG_I: Configured from console by console

S1#sh
S1#show ether
S1#show etherchannel su
S1#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----
+-----+-----+-----
1      Po1(SU)         PAgP       Fa0/21(P) Fa0/22(P)
S1#
```

```
%SYS-5-CONFIG_I: Configured from console by console

S3#sh
S3#show ethe
S3#show etherchannel su
S3#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----
+-----+-----+-----
1      Po1(SU)         PAgP       Fa0/21(P) Fa0/22(P)
S3#
```

- b. Dans le cas où EtherChannel ne répond pas, désactivez les interfaces physiques au sein des deux extrémités de l'EtherChannel, puis réactivez-les. En utilisant la commande **shutdown** sur ces interfaces, suivie d'une commande **no shutdown**.

Les commandes **show interfaces trunk** et **show spanning-tree** affichent également le Port Channel comme une seule liaison logique.

```
S1#show int
S1#show interfaces tr
S1#show interfaces trunk
Port          Mode          Encapsulation  Status        Native vlan
Po1           on            802.1q         trunking      1
Gig0/1       on            802.1q         trunking      1
Gig0/2       on            802.1q         trunking      1

Port          Vlans allowed on trunk
Po1           1-1005
Gig0/1       1-1005
Gig0/2       1-1005

Port          Vlans allowed and active in management domain
Po1           1
Gig0/1       1
Gig0/2       1

Port          Vlans in spanning tree forwarding state and not
pruned
Po1           1
Gig0/1       1
Gig0/2       1

S1#
```

```
S1#sh
S1#show sp
S1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address    0001.6309.DB61
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15
sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address    0001.6309.DB61
             Hello Time 2 sec Max Age 20 sec Forward Delay 15
sec

             Aging Time 20

Interface          Role Sts Cost          Prio.Nbr Type
-----
Gi0/1              Desg FWD 4             128.25 P2p
Gi0/2              Desg FWD 4             128.26 P2p
Po1                 Desg FWD 9             128.27 Shr

S1#
```

### III.2 Configuration d'un EtherChannel LACP 802.3ad

#### 1. Configurez Port Channel 2.

- a. La norme 802.3ad, a été publiée par IEEE en 2000 (la version standard ouverte d'EtherChannel). En utilisant les commandes précédentes, configurez la liaison entre S1 et S2 sur les ports G0/1 et G0/2 en tant qu'EtherChannel LACP.

## TP5 : Configuration du protocole Etherchannel entre commutateurs Simulation sous packet-tracer

Le numéro de Port Channel utilisé doit être différent de 1 sur S1, car vous avez déjà utilisé cette valeur durant l'étape précédente.

La configuration d'un Port Channel en tant que LACP nécessite l'utilisation de la commande **channel-group numbermode active** de mode de configuration d'interface. Le mode actif reflète que le commutateur essaie de négocier cette liaison en tant que LACP, inversement à PAgP.

```
S1(config)# interface range g0/1 - 2
S1(config-if-range)# shutdown
S1(config-if-range)# channel-group 2 mode active
S1(config-if-range)# no shutdown
S1(config-if-range)# interface port-channel 2
S1(config-if)# switchport mode trunk
```

```
S2(config)# interface range g0/1 - 2
S2(config-if-range)# shutdown
S2(config-if-range)# channel-group 2 mode active
S2(config-if-range)# no shutdown
S2(config-if-range)# interface port-channel 2
S2(config-if)# switchport mode trunk
```

### 2. Vérification de l'état de Port Channel 2.

- Pour vérifier l'état de Port Channel 2 utilisez les commandes show lors de l'Étape 2 de la Partie 1. Par la suite vous pouvez identifier le protocole utilisé par chaque port.

```
S1#sh
S1#show eth
S1#show etherchanne
S1#show etherchannel su
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----
+-----+-----+-----
1      Po1 (SU)        PAgP       Fa0/21 (P) Fa0/22 (P)
2      Po2 (SU)        LACP       Gig0/1 (P) Gig0/2 (P)
S1#
```

## III.3 Configuration d'un lien EtherChannel redondant

### 1. Configurez Port Channel 3.

Plusieurs moyens sont possibles pour exécuter la commande **channel-group number mode** :

```
S2(config-if-range)#exit
S2(config)#inter
S2(config)#interface po
S2(config)#interface port-channel 2
S2(config-if)#sw
S2(config-if)#switchport mo
S2(config-if)#switchport mode tr
S2(config-if)#switchport mode trunk
S2(config-if)#exi
S2(config-if)#exit
S2(config)#int
S2(config)#interface ra
S2(config)#interface range f
S2(config)#interface range fastEthernet 0/23-24
S2(config-if-range)#ch
S2(config-if-range)#cha
S2(config-if-range)#channel-g
S2(config-if-range)#channel-group 3 mode ?
  active      Enable LACP unconditionally
  auto        Enable PAgP only if a PAgP device is detected
  desirable   Enable PAgP unconditionally
  on          Enable Etherchannel only
  passive     Enable LACP only if a LACP device is detected
S2(config-if-range)#
```

- a) Ajoutez les ports F0/23 et F0/24 au Port Channel 3 sur le commutateur S2, en utilisant la commande **channel-group 3 mode passive**. L'option **passive** signifie que le commutateur utilise le protocole LACP uniquement si un autre périphérique LACP est détecté. Configurez le Port Channel 3 de manière statique en tant qu'interface de trunking.

```
S2(config)# interface range f0/23 - 24
S2(config-if-range)# shutdown
S2(config-if-range)# channel-group 3 mode passive
S2(config-if-range)# no shutdown
S2(config-if-range)# interface port-channel 3
S2(config-if)# switchport mode trunk
```

- b) Ajoutez les ports F0/23 et F0/24 au Port Channel 3 sur le commutateur S3, en utilisant la commande **channel-group 3 mode active**. L'option **active** signifie que le commutateur utilise le protocole LACP d'une façon inconditionnelle. Configurez le Port Channel 3 de manière statique en tant qu'interface de trunking.

```
S3(config)# interface range f0/23 - 24
S3(config-if-range)# shutdown
S3(config-if-range)# channel-group 3 mode active
S3(config-if-range)# no shutdown
S3(config-if-range)# interface port-channel 3
S3(config-if)# switchport mode trunk
```



## 2. Vérifiez l'état de Port Channel 3.

- a) Pour vérifier l'état du Port Channel 3, utilisez les commandes **show etherchannel summary**, identifiez le protocole utilisé par chaque port.

```
S2#sh
S2#show eth
S2#show etherchannel su
S2#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
+-----+-----+-----+-----
2      Po2(SU)         LACP       Gig0/1(P) Gig0/2(P)
3      Po3(SU)         LACP       Fa0/23(P) Fa0/24(P)
S2#
```

- b) Le Port Channel 2 n'est pas opérationnel, en raison que le protocole STP a bloqué certains ports. Malheureusement, ces ports étaient des ports Gigabit. Pour restaurer ces ports, soit vous configurez S1 en tant que pont racine principal pour le VLAN 1 ou bien vous définissez la priorité à 24576.

Remarque : La priorité du commutateur est configurée sur la valeur prédéfinie de 24576 ou sur le multiple le plus élevé de 4096, moins la plus basse valeur de priorité de pont détectée sur le réseau.

S1(config)# **spanning-tree vlan 1 root primary**

Ou:

S1(config)# **spanning-tree vlan 1 priority 24576**

## TP6 : Mise en œuvre d'un routage statique

### I. Objectifs pédagogiques :

Ce TP a pour objectif de configurer des stations de travail et des routeurs afin de communiquer ensemble deux réseaux distants et d'apprendre à configurer des routes statiques sur un routeur Cisco.

- Configuration des interfaces des routeurs.
- Configuration du routage statique.
- Routage statique et métrique.
- Routes statiques et tables de routage.

### II. Partie théorique

Les routes statiques sont ajoutées manuellement à une table de routage via une configuration directe. À l'aide d'un routage statique, un routeur peut découvrir une route vers un réseau distant qui n'est pas directement connecté à l'une de ses interfaces. Notez que, cependant, les routes statiques ne sont pas largement utilisées aujourd'hui, car vous devez configurer chaque route statique manuellement sur chaque routeur du réseau [3,13].

Les routes statiques sont configurées en mode de configuration globale à l'aide de la commande :

**ip route[adresse réseau] [masque] [passerelle]**

Le paramètre [passerelle] est l'adresse IP du routeur du prochain saut qui recevra les paquets et les transmettra au réseau distant. Le routeur avec l'adresse IP du prochain saut doit se trouver sur un réseau directement connecté [14].

### III. Partie pratique

#### III.1 Configuration du routage statique :

##### a) Schéma de topologie

Schématiser le réseau de la figure ci-dessous composé de 2 routeurs, Cisco 2621XM avec deux postes clients PC1 et PC2.

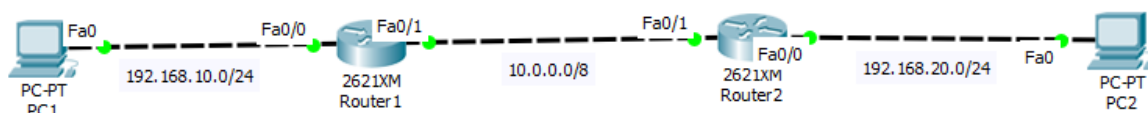


Figure VI.1 : Schéma de topologie

## TP6 : Mise en œuvre d'un routage statique

### b) Table d'adressage :

Commençons par configurer nos deux postes clients avec la configuration suivante, puis nous configurons les deux routeurs.

PCs	Adresse IP	Masque de sous réseau	Passerelle par défaut
PC1	192.168.10.2	255.255.255.0	192.168.10.1
PC2	192.168.20.2	255.255.255.0	192.168.20.1

Tableau VI.1 La table d'adressage PCs

Routeurs	Interfaces	Adresse IP	Masque de sous réseau
R1	Fa 0/0	192.168.10.1	255.255.255.0
	Fa 0/1	10.0.0.1	255.0.0.0
R2	Fa 0/0	192.168.20.1	255.255.255.0
	Fa 0/1	10.0.0.254	255.0.0.0

Tableau VI.2 La table d'adressage des Routeurs.

### Configuration du routeur Router1 :

```
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#interface fastEthernet 0/0
Router1(config-if)#ip address 192.168.10.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config)#interface fastEthernet 0/1
Router1(config-if)#ip address 10.0.0.1 255.0.0.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#ip routing
```

### Configuration du routeur Router2 :

```
Router#configure terminal
Router(config)#hostname Router2
Router2(config)#interface fastEthernet 0/0
Router2(config-if)#ip address 192.168.20.1 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#interface fastEthernet 0/1
Router2(config-if)#ip address 10.0.0.254 255.0.0.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#ip routing
```

- Après cette étape, toutes les interfaces doivent passer à l'état UP. Assurez-vous qu'elles le sont avant de passer à la section suivante.
- Testez les connexions entre les équipements suivants et qu'est ce que vous observez ?
  - PC1 et le R1 ?

## TP6 : Mise en œuvre d'un routage statique

- R1 et R2 ?
- R2 et PC2 ?
- PC1 et PC2 ?

Si on fait ces tests, nous pouvons observer que :

Le ping entre PC1 et le R1 fonctionne, le ping entre R1 et R2 fonctionne, le ping entre R2 et PC2 fonctionne. Mais nous pouvons voir aussi que le ping entre PC1 et PC2 ne fonctionne pas. Que se passe-t-il réellement dans les tuyaux : PC1 remarque que PC2 n'est pas dans le même réseau que lui. Il envoie donc le ping à sa passerelle (routeur R1), le routeur R1 ne connaît pas le réseau de PC2, donc, il abandonne le paquet. Si nous effectuons un ping entre PC1 et R2, cela ne fonctionne pas non plus. Que se passe-t-il réellement dans les tuyaux : PC1 remarque que PC2 n'est pas dans le même réseau que lui. Il envoie donc le ping à sa passerelle (routeur R1), R1 connaît l'adresse de R2 donc il envoie le ping. Lorsque R2 reçoit le ping, il souhaiterait répondre mais ne connaissant pas le chemin qui mène à PC1, il abandonne le paquet.

Comment résoudre ces problèmes ? Pour résoudre ces problèmes, il faut simplement rajouter des routes statiques de routage sur R1 et R2.

### Configuration du routage statique

Le principe du routage statique est le suivant : Pour chaque routeur, identifier tous les réseaux qui ne sont pas voisins (en d'autres termes, qui ne sont pas directement raccordés) à celui-ci. Ensuite, il faut définir une route (à l'aide d'une passerelle) pour atteindre chacun de ces réseaux.

La commande est la suivante en mode configuration :

**ip route [adresse réseau] [masque] [passerelle]**

(En général, la passerelle est l'adresse IP de l'interface directement opposée au routeur concerné dans le sens de ces réseaux en question).

- Appliquons ce principe sur notre schéma de la figure VI.1:
- Pour le Routeur1  
Les réseaux qui ne sont pas directement raccordés au Routeur1 sont : 192.168.20.0/24.  
La passerelle pour atteindre le réseau 192.168.20.0/24 est : 10.0.0.254.
- Pour le Routeur2  
Les réseaux qui ne sont pas directement raccordés au Routeur1 sont : 192.168.10.0/24.  
La passerelle pour atteindre le réseau 192.168.10.0/24 est : 10.0.0.1

Tapez donc les commandes suivantes dans chaque routeur pour configurer le routage statique.

#### Routeur1

```
Router(config)#ip route 192.168.20.0 255.255.255.0 10.0.0.254
```

## TP6 : Mise en œuvre d'un routage statique

```
Router(config)#do wr
Router(config)#end
```

### Routeur2

```
Router(config)#ip route 192.168.10.0 255.255.255.0 10.0.0.1
Router(config)#do wr
Router(config)#end
```

Votre routage est effectif, vous pouvez tester cette configuration avec quelques commandes Cisco. Depuis le PC1, faites un PING pour tenter de joindre le PC2 et vice versa :

### Remarque:

- Pour la première tentative (du PING), c'est possible que ça ne marche pas car le réseau a besoin d'un peu de temps pour acheminer les paquets d'un bout à l'autre. Retentez plusieurs fois pour que ça marche.
- Pour afficher la table de routage d'un routeur, tapez la commande suivante en mode privilégié : **show ip route**
- Chaque ligne détermine une route.
  - La lettre **C** est placée devant tous les réseaux qui sont directement connectés au routeur en question.
  - La lettre **S** (pour Statique) désigne une route configurée statiquement. La lettre sera suivie du réseau ainsi que la passerelle pour atteindre celui-ci.
  - Pour avoir aussi une idée de la route (trajet) empruntée par les paquets ainsi que le nombre de sauts, utilisez la commande **traceroute** (équipements Cisco) ou **tracert** (sous Windows).

```
R2>en
R2#sho
R2#show ip r
R2#show ip rou
R2#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   10.0.0.0/8 is directly connected, FastEthernet0/1
S   192.168.10.0/24 [1/0] via 10.0.0.1
C   192.168.20.0/24 is directly connected, FastEthernet0/0
R2#
```

```
! Unknown command or computer name, or unable to find computer
address
R1>en
R1#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   10.0.0.0/8 is directly connected, FastEthernet0/1
C   192.168.10.0/24 is directly connected, FastEthernet0/0
S   192.168.20.0/24 [1/0] via 10.0.0.254
R1#
```

## III.2 Routage statique et métrique

### III.2.1 Définition de la métrique :

La métrique est une valeur associée à chaque route dans la table de routage. Elle sert à sélectionner la route à utiliser lorsqu'il en existe plusieurs vers le même réseau de

## TP6 : Mise en œuvre d'un routage statique

destination. Dans le cas de l'utilisation d'un protocole de routage, le calcul de la métrique se fait de manière automatique. En effet, chaque protocole a son algorithme. Par exemple, pour RIP, la valeur correspond au nombre de saut vers le réseau de destination. Pour OSPF, elle dépend de la bande passante des liaisons [13].

Lorsque l'on crée une route statique, on peut associer une métrique arbitraire à celle-ci. Par défaut, sa valeur est de 1, mais nous pouvons la modifier si nous souhaitons par exemple faire en sorte que la route soit un lien de secours ou donner des priorités à plusieurs liens pointant vers la même destination mais possédant des débits différents [13].

Afin d'étudier cette notion de la métrique, nous allons étendre le schéma de notre réseau comme le montre la Figure suivante :

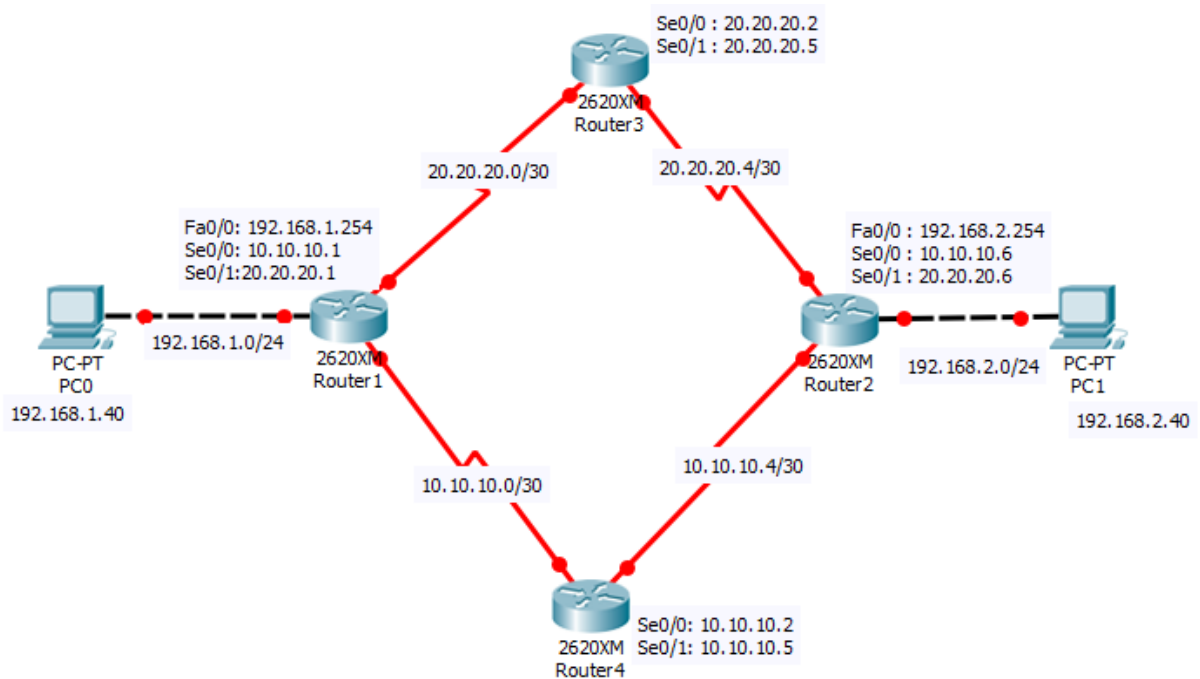


Figure VI.2 : Schéma du réseau (routage statique avec métriques).

- Ajouter deux routeur de type (2620XM), sur chaque Routeur, vous devez installer les deux modules série (module Série WIC-1T) afin de faire la liaison entre eux.
- Nous allons commencer par configurer les nouvelles interfaces de nos routeurs, puis nous allons faire toutes nos routes, cette opération est identique à la précédente (configuration de routage statique).

### III.2.2 Configuration des nouvelles interfaces :

- **Configuration du Routeur1**

```
Router#conf t
```

```
Router(config)#interface Serial0/0
```

```
Router(config-if)#ip address 10.10.10.1 255.255.255.252
```

```
Router(config-if)#no shutdown
```

## TP6 : Mise en œuvre d'un routage statique

```
Router(config-if)#end
```

```
Router#conf t
Router(config)#interface Serial0/1
Router(config-if)#ip address 20.20.20.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#end
```

- **Configuration du Routeur2**

```
Router#conf t
Router(config)#interface Serial0/0
Router(config-if)#ip address 10.10.10.6 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#end
```

```
Router#conf t
Router(config)#interface Serial0/1
Router(config-if)#ip address 20.20.20.6 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#end
```

- **Configuration du Routeur3**

```
Router>enable
Router#conf t
Router(config)#int Se0/0
Router(config-if)#ip address 20.20.20.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

```
Router#conf t
Router(config)#int Se0/1
Router(config-if)#ip address 20.20.20.5 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#end
```

- **Configuration du Routeur4**

```
Router>enable
Router#conf t
Router(config)#int Se0/0
Router(config-if)#ip address 10.10.10.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

## TP6 : Mise en œuvre d'un routage statique

```
Router>enable
Router#conf t
Router(config)#int Se0/1
Router(config-if)#ip address 10.10.10.5 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

### III.2.3 Configuration des routes statiques et tables de routage:

- Pour chaque routeur nous allons ajouter deux routes :
  - Sur le Routeur1, nous allons créer deux routes vers le réseau 192.168.2.0 avec deux métriques différentes.
  - Sur le Routeur2, nous allons créer deux routes vers le réseau 192.168.1.0 avec deux métriques différentes.
  - Sur le Routeur3 et Routeur4, nous allons créer une route pour le réseau 192.168.1.0 et une autre route pour le réseau 192.168.2.0.
- Avant tout ça, nous devons effacer toutes les anciennes routes sur les routeurs (Routeur1 et Routeur2), en utilisant la commande suivante en mode configuration :

**no ip route [adresse réseau] [masque] [passerelle]**

- Tapez donc les commandes suivantes dans chaque routeur pour ajouter les routes
  - Routeur1

```
Router(config)#ip route 192.168.2.0 255.255.255.0 20.20.20.2 20
Router(config)#ip route 192.168.2.0 255.255.255.0 10.10.10.2 10
Router(config)#do wr
```

Les valeurs 10 et 20, à la fin des deux commandes, représentent les métriques de chaque route. Nous obtenons la table de routage suivante :

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
...

Gateway of last resort is not set

    10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Serial0/0
    20.0.0.0/30 is subnetted, 1 subnets
C       20.20.20.0 is directly connected, Serial0/1
C       192.168.1.0/24 is directly connected, FastEthernet0/0
S       192.168.2.0/24 [10/0] via 10.10.10.2
```

Si nous regardons la table de routage du Routeur1, nous pouvons voir que seule la route statique avec la plus faible métrique vers 192.168.2.0 a été ajoutée.

- Routeur2

```
Router(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.5 20
Router(config)#ip route 192.168.1.0 255.255.255.0 20.20.20.5 10
```



## TP6 : Mise en œuvre d'un routage statique

```
Router(config)#do wr
```

Si nous regardons la table de routage du Routeur1, nous pouvons voir que seule la route statique avec la plus faible métrique vers 192.168.1.0 a été ajoutée.

- Routeur3  
Router(config)#ip route 192.168.1.0 255.255.255.0 20.20.20.1 10  
Router(config)#ip route 192.168.2.0 255.255.255.0 20.20.20.6 20  
Router(config)#do wr
- Routeur4  
Router(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.1 20  
Router(config)#ip route 192.168.2.0 255.255.255.0 10.10.10.6 10  
Router(config)#do wr

Si nous testons la connectivité entre PC1 et PC2, nous remarquons que :

- PC1 envoie le ping, qui passe par le Routeur1, puis par le Routeur4 et ensuite par le Routeur2 pour enfin atteindre PC2.
- PC2 répond au ping qu'il a reçu, le ping passe par le Routeur2, puis par le Routeur3 et ensuite par le Routeur1 pour enfin atteindre le PC1.

Le réseau fonctionne correctement, nous obtenons bien une route dans les deux sens. Si une panne survient sur notre réseau, alors le lien entre le Routeur1 et le Routeur4 ne fonctionne plus.

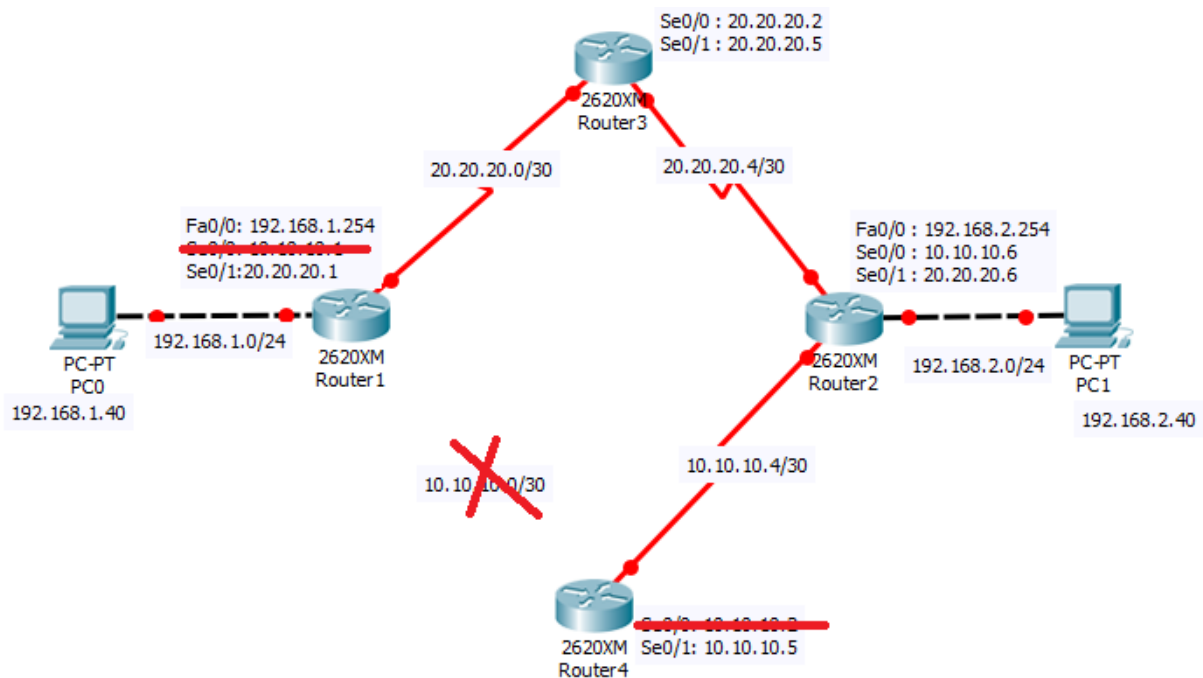


Figure VI.3 : Schéma du réseau (avec une panne).

## TP6 : Mise en œuvre d'un routage statique

Voyons comment se passent le ping maintenant. Le Routeur1 modifie sa table de routage, nous obtenons maintenant :

```
Gateway of last resort is not set
```

```
Gateway of last resort is not set
  20.0.0.0/30 is subnetted, 1 subnets
C       20.20.20.0 is directly connected, Serial0/1
C       192.168.1.0/24 is directly connected, FastEthernet0/0
S       192.168.2.0/24 [20/0] via 20.20.20.2
```

La ligne : "S 192.168.2.0/24 [10/0] via 10.10.10.2" a été remplacé par la ligne : "S 192.168.2.0/24 [20/0] via 20.20.20.2" car le lien entre Routeur1 et Routeur4 n'existe plus.

- Le PC1 envoie donc le ping, qui passe par le Routeur1, puis par le Routeur3 et ensuite par le Routeur2 pour enfin atteindre le PC2.
- PC2 répond à ce ping, qui va faire le chemin inverse Routeur2 > Routeur3 > Routeur1 > PC1

Sachez que sur un routeur, l'interface se trouvant dans le réseau local possède en général, soit la première adresse du réseau soit la dernière.

Sachez aussi que le routage est une chose simple, mais il faut être très méticuleux et faire attention à ne pas faire de fautes de frappe, surtout dans les adresses IP.

Sachez ensuite que la valeur de la métrique peut être manipulée pour forcer les paquets à passer par un lien plutôt que par un autre.

Pour finir sachez que la route par défaut (0.0.0.0 0.0.0.0...) est utilisée pour envoyer tous les paquets dont la route est inconnue soit par une interface du routeur ou soit en indiquant une passerelle adjacente [13]. Très utilisé pour router les paquets vers internet.

## TP7 : Mise en œuvre d'un routage dynamique RIPv2, EIGRP et OSPF

### I. Objectifs pédagogiques

Lors du TP précédent, vous avez exploré le principe et la configuration du routage statique, si la topologie d'un réseau offre la possibilité de plusieurs routes pour atteindre une même destination. Si le réseau est vaste et complexe, sujet à des changements fréquents de configuration, le routage dynamique est alors un bon moyen d'entretenir les tables de routages et de manière automatique.

Il existe de nombreux protocoles de routage dynamique, les plus couramment employés sont RIP (Routing Information Protocol) qui est simple à comprendre et à utiliser, ou encore OSPF (Open Shortest Path First) ou EIGRP (Enhanced Interior Gateway Routing Protocol).

- L'objectif principal du TP est de comprendre le fonctionnement des trois protocoles et d'apprendre à les configurer.

### II. Partie théorique

#### II.1 Protocole RIP

RIP (Routing Information Protocol) est l'un des plus anciens protocoles de routage à vecteur de distance. Il est généralement utilisé sur des petits réseaux car il est très simple à configurer et à entretenir. Il existe deux versions du protocole: la version 1 et 2. Les deux versions utilisent le nombre de sauts comme métrique et ont la distance administrative de 120. La version 2 de RIP est capable d'annoncer les masques de sous-réseau et utilise la multidiffusion pour envoyer des mises à jour de routage, tandis que la version 1 ne le fait pas. La version 2 est rétro compatible avec la version 1.

RIPv2 envoie toute la table de routage toutes les 30 secondes, ce qui peut consommer beaucoup de bande passante. RIPv2 utilise aussi l'adresse de multidiffusion 224.0.0.9 pour envoyer des mises à jour de routage, et prend en charge l'authentification et les mises à jour déclenchées (mises à jour envoyées en cas de modification du réseau) [13,14].

Pour un exemple du fonctionnement de RIP, considérez la figure VII.1 :

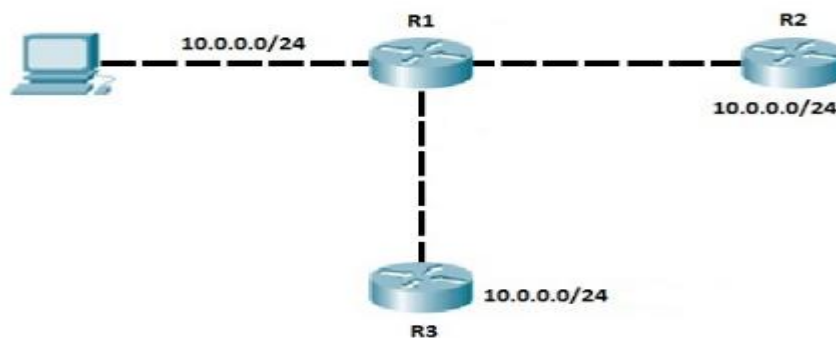


Figure VII.1 Schéma de topologie

Le routeur R1 se connecte directement au sous-réseau 10.0.0.0/24, après que le protocole RIP a été configuré sur R1 pour annoncer l'itinéraire vers ce sous-réseau. R1 envoie des mises à jour de routage à R2 et R3. Les mises à jour de routage répertorient le sous-réseau, le masque de sous-réseau et la métrique pour cette route. Chaque routeur R2 et R3 reçoit cette mise à jour et ajoute la route à leurs tables de routage respectives. Les deux routeurs répertorient la métrique de 1 car le réseau n'est qu'à un seul saut.

Le nombre maximal de sauts pour une route RIP est de 15. Toute route avec un nombre de sauts plus élevé est considérée comme inaccessible.

## II.2 Protocole EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) est un protocole de routage à vecteur de distance avancé. Ce protocole est une évolution d'un ancien protocole Cisco appelé IGRP, qui est maintenant considéré comme obsolète. EIGRP prend en charge le routage sans classe et VLSM, la récapitulation des itinéraires, les mises à jour incrémentielles, l'équilibrage de charge et de nombreuses autres fonctionnalités utiles. Il s'agit d'un protocole propriétaire de Cisco [13].

Les routeurs exécutant EIGRP doivent devenir voisins avant d'échanger des informations de routage. Pour découvrir dynamiquement les voisins, les routeurs EIGRP utilisent l'adresse de multidiffusion 224.0.0.10. Chaque routeur EIGRP stocke les informations de routage et de topologie dans trois tables [13 ,14]:

- Table de voisinage : Elle stocke des informations sur les voisins EIGRP.
- Table de topologie : Elle stocke les informations de routage apprises des routeurs voisins.
- Table de routage : Elle stocke les meilleurs itinéraires.

La distance administrative de l'EIGRP est de 90, ce qui est inférieur à la fois à la distance administrative du RIP et à la distance administrative de l'OSPF, de sorte que les routes EIGRP seront préférées à ces routes. EIGRP utilise le protocole RTP (Reliable Transport Protocol) pour l'envoi de messages.

EIGRP calcule sa métrique en utilisant la bande passante, le délai, la fiabilité et la charge. Par défaut, seuls la bande passante et le délai sont utilisés lors du calcul de la métrique, tandis que la fiabilité et la charge sont définies par zéro.

L'EIGRP utilise le concept de systèmes autonomes. Un système autonome est un ensemble de routeurs compatibles EIGRP qui devraient devenir des voisins EIGRP. Chaque routeur à l'intérieur d'un système autonome doit avoir le même numéro de système autonome configuré, sinon les routeurs ne deviendront pas voisins.

### **II.3 Protocole OSPF**

OSPF (Open Shortest Path First) est un protocole de routage d'état de liaison. OSPF fonctionnera sur la plupart des routeurs qui ne doivent pas nécessairement être des routeurs Cisco. Voici les fonctionnalités les plus importantes d'OSPF [6,13]:

- un protocole de routage sans classe.
- prend en charge VLSM, CIDR, récapitulation manuelle des itinéraires, équilibrage de charge à coût égal.
- les mises à jour incrémentielles sont prises en charge.
- utilise un seul paramètre comme métrique - le coût de l'interface.
- la distance administrative des routes OSPF est, par défaut, 110.
- utilise les adresses de multidiffusion 224.0.0.5 et 224.0.0.6 pour le routage des mises à jour.

Les routeurs exécutant OSPF doivent établir des relations de voisinage avant d'échanger des routes. Étant donné qu'OSPF est un protocole de routage à état de liaison, les voisins n'échangent pas de tables de routage. Au lieu de cela, ils échangent des informations sur la topologie du réseau. Chaque routeur OSPF exécute l'algorithme SPF pour calculer les meilleurs itinéraires et les ajoute à la table de routage. Étant donné que chaque routeur connaît la topologie entière d'un réseau, la probabilité qu'une boucle de routage se produise est minime.

Chaque routeur OSPF stocke les informations de routage et de topologie dans trois tables:

- Table des voisins : stocke des informations sur les voisins OSPF.
- Table topologique : stocke la structure topologique d'un réseau.
- Table de routage : stocke les meilleurs itinéraires.

## **III. Partie pratique**

### **III.1 Configuration du protocole RIP**

La configuration de RIPv2 est un processus assez simple. Seules trois étapes sont nécessaires:

1. Activation de RIP à l'aide de la commande de configuration globale du **router rip**
2. Demander au routeur d'utiliser RIPv2 en tapant la commande version 2.
3. Dire à RIP quels réseaux annoncer en utilisant une ou plusieurs commandes réseau.

## TP7 : Mise en œuvre d'un routage dynamique RIPv2, EIGRP et OSPF

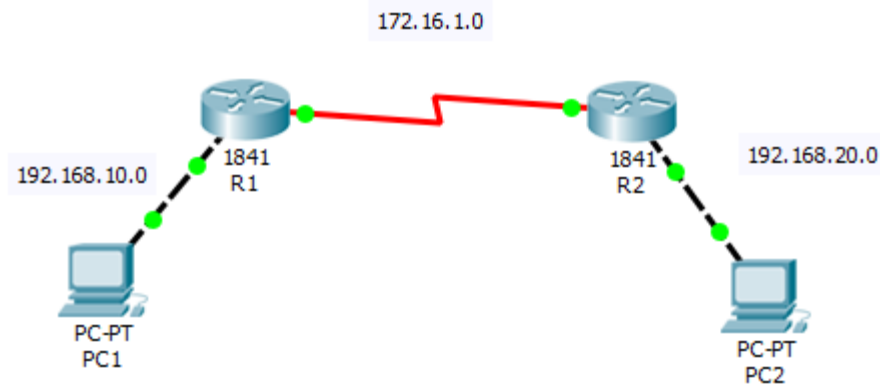


Figure VII.2 Schéma du réseau

Mettez également deux (2) PC pour le teste à la fin de la configuration.

**PC1 : IP : 192.168.10.2 Masque : 255.255.255.0 Gatewaye : 192.168.10.1**

**PC2 : IP : 192.168.20.2 Masque : 255.255.255.0 Gatewaye : 192.168.20.1**

### III.1.1 Configuration des interfaces des routeurs

#### ➤ Routeur R1 :

```
Router>enable
Router#conf t
Router(config)#hostname R1
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config)#int se0/1/0
R1(config-if)#ip add 172.16.1.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#end
```

#### ➤ Routeur R2

```
Router>enable
Router#conf t
Router(config)#hostname R2
R2(config)#int Fa0/0
R2(config-if)#ip add 192.168.20.1 255.255.255.0
R2(config-if)#no shut

R2(config)#int se0/0/0
R2(config-if)#ip add 172.16.1.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#end
```

```
R1(config)#int se0/1/0
R1(config-if)#clock rate 64000
```

Après cette étape, toutes les interfaces doivent passer à l'état UP. Assurez-vous qu'elles le sont avant de passer à la section suivante.

### III.1.2 Configuration du protocole RIPv2

#### ➤ Routeur R1

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.10.0
R1(config-router)#network 172.16.1.0
R1(config-router)#end
R2#write
```

#### ➤ Routeur R2

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.20.0
R2(config-router)#network 172.16.1.0
R2(config-router)#end
R2#write
```

```
R1#show ip r
R1#show ip ro
R1#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

      172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/1/0
C       192.168.10.0/24 is directly connected, FastEthernet0/0
R       192.168.20.0/24 [120/1] via 172.16.1.2, 00:00:08,
Serial0/1/0
R1#
```

## TP7 : Mise en œuvre d'un routage dynamique RIPv2, EIGRP et OSPF

```
R2>en
R2#sh ip ro
R2#sh 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

      172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/0/0
R       192.168.10.0/24 [120/1] via 172.16.1.1, 00:00:05,
Serial0/0/0
C       192.168.20.0/24 is directly connected, FastEthernet0/0

R2#
```

### III.1.3 Désactivation du RIP2

```
Press RETURN to get started.

R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no rou
R1(config)#no router ri
R1(config)#no router rip 2
R1(config)#end
```

## III.2 Configuration du protocole EIGRP 1

Pour configurer cette partie, en utilise le même schéma de la Figure VII.2

### ➤ Routeur R1

```
R1(config)#router eigrp 1
```

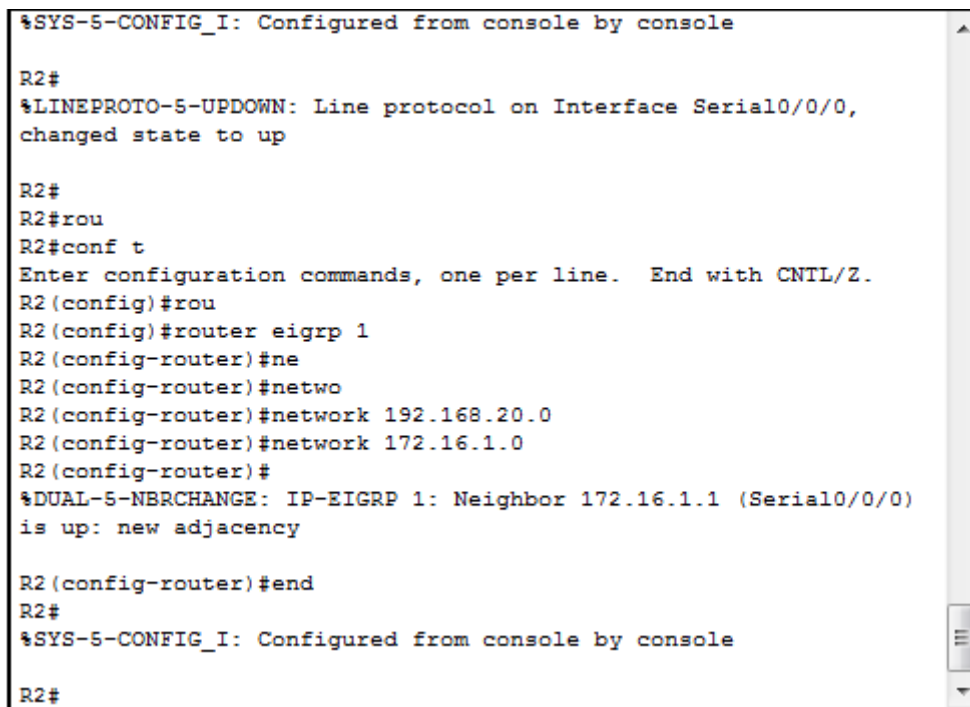


## TP7 : Mise en œuvre d'un routage dynamique RIPv2, EIGRP et OSPF

```
R1(config-router)#network 192.168.10.0
R1(config-router)#network 172.16.1.0
R1(config-router)#end
R2#write
```

### ➤ Routeur R2

```
R2(config)#router eigrp1
R2(config-router)#network 192.168.20.0
R2(config-router)#network 172.16.1.0
R2(config-router)#end
R2#write
```



```
%SYS-5-CONFIG_I: Configured from console by console

R2#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

R2#
R2#rou
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#rou
R2(config)#router eigrp 1
R2(config-router)#ne
R2(config-router)#netwo
R2(config-router)#network 192.168.20.0
R2(config-router)#network 172.16.1.0
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.1.1 (Serial0/0/0)
is up: new adjacency

R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
```

Vérifiez maintenant la configuration EIGRP. Commençons par vérifier la relation de voisinage EIGRP des routeurs. Sur le routeur 1, on utilise la commande suivante :

```
R1#show ip eigrp neighbors
```

## TP7 : Mise en œuvre d'un routage dynamique RIPv2, EIGRP et OSPF

```
%SYS-5-CONFIG_I: Configured from console by console

R1#ri
R1#wri
R1#write
Building configuration...
[OK]
R1#
R1#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.1.2 (Serial0/0/0)
is up: new adjacency

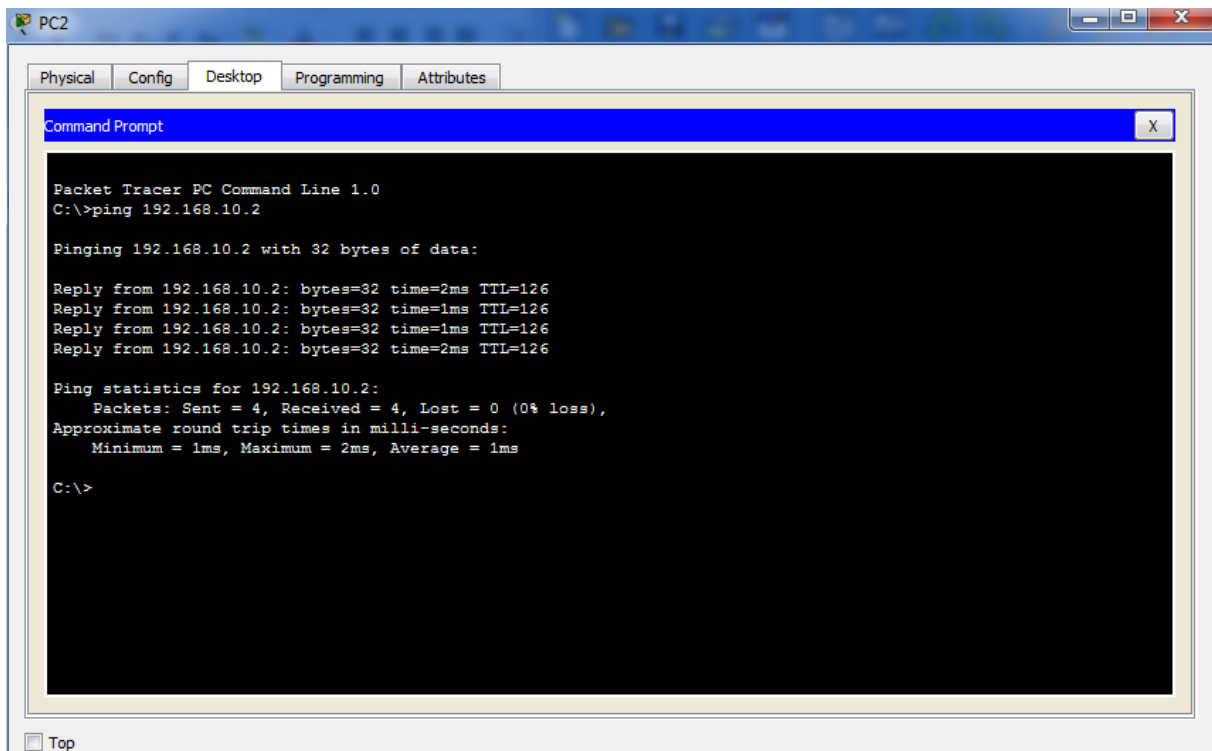
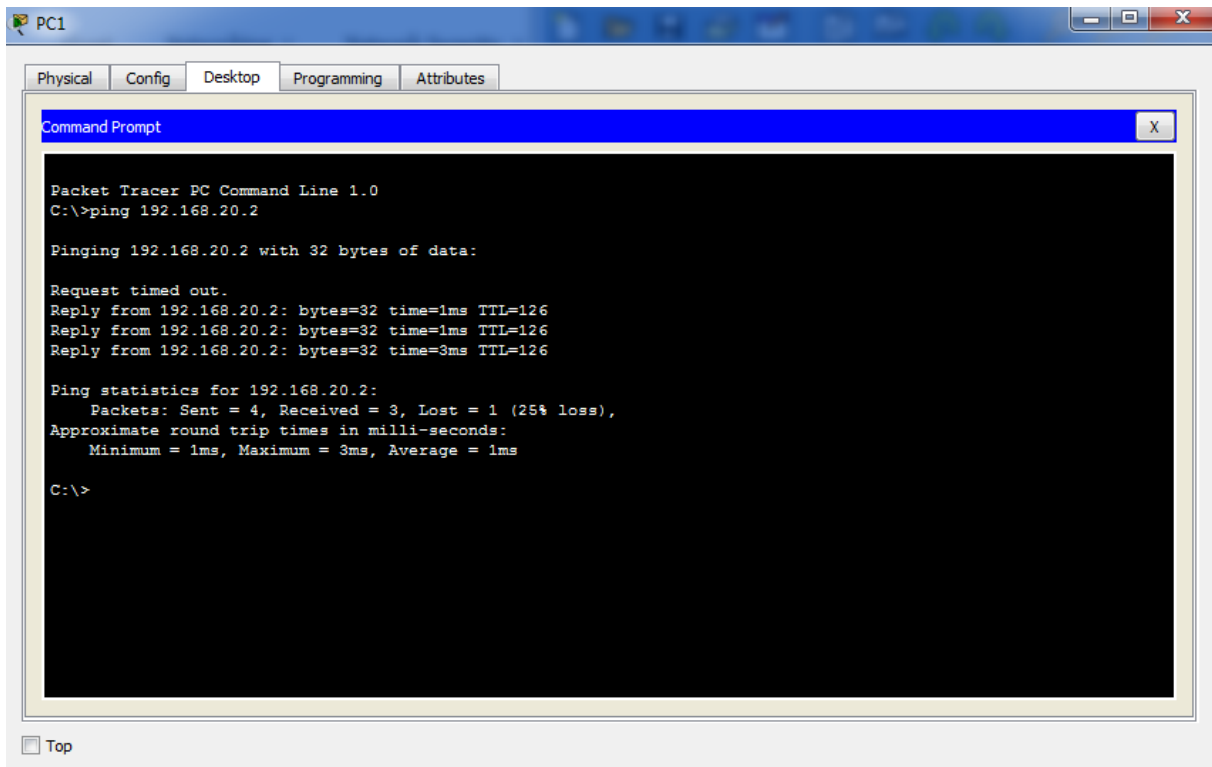
R1#sh
R1#show ip eig
R1#show ip eigrp nei
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address          Interface      Hold Uptime    SRTT   RTO   Q
Seq
                               (sec)         (ms)          Cnt
Num
0   172.16.1.2        Se0/0/0       10  00:06:28  40   1000  0
3
R1#
```

Dans cette image, vous pouvez voir que R1 a un seul voisin avec l'adresse IP de 172.16.1.2. Deuxièmement, nous vérifierons si R1 a reçu un itinéraire pour atteindre le réseau 192.168.10.0/24. Nous pouvons utiliser la commande *show ip route eigrp*

```
R1>en
R1#sho
R1#show ip
R1#show ip rou
R1#show ip route eig
R1#show ip route eigrp
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D    172.16.0.0/16 is a summary, 00:35:54, Null0
D   192.168.20.0/24 [90/2172416] via 172.16.1.2, 00:34:11,
Serial0/0/0
R1#
```

Enfin, envoyons une requête ping à PC2 à partir de PC1. Ping devrait réussir car R1 a appris la route vers 192.168.10.0/24 via EIGRP comme indiqué par la lettre D. Essayez également d'envoyer une requête ping à PC1 à partir de PC2. Ping devrait fonctionner.

## TP7 : Mise en œuvre d'un routage dynamique RIPv2, EIGRP et OSPF



## Désactivation du EIGRP

```
R1#show ip
R1#show ip rou
R1#show ip route eig
R1#show ip route eigrp
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:35:54, Null0
D       192.168.20.0/24 [90/2172416] via 172.16.1.2, 00:34:11,
Serial0/0/0

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no rou
R1(config)#no router eigrp 1
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#sh
R1#show ip rou
R1#show ip route eig
R1#show ip route eigrp

R1#
R1#
```

### III.3 Configuration du protocole OSPF

La configuration est assez simple et ne nécessite que deux étapes majeures:

1. Activez OSPF sur un routeur à l'aide du routeur ospf PROCESS\_ID en mode de configuration globale.
2. Définissez sur quelles interfaces OSPF s'exécutera et quels réseaux seront annoncés à l'aide de la commande **network IP\_ADDRESS WILCARD\_MASK AREA** en mode de configuration OSPF.

Notez que l'ID de processus OSPF n'a pas besoin d'être le même sur tous les routeurs pour que les routeurs établissent une relation de voisinage, mais le paramètre de zone doit être le même sur tous les routeurs voisins pour que les routeurs deviennent voisins.

#### ➤ Routeur R1

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.0 255.255.255.0 area 0
R1(config-router)#network 172.16.1.0 255.255.255.252 area 0
R1(config-router)#end
R2#write
```

#### ➤ Routeur R2

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.20.0 255.255.255.0 area 0
R2(config-router)#network 172.16.1.0 255.255.255.252 area 0
```

## TP7 : Mise en œuvre d'un routage dynamique RIPv2, EIGRP et OSPF

```
R2(config-router)#end
R2#write
```

Comme vous pouvez le voir sur cette image, il suffit d'activer OSPF sur les routeurs qui annoncent, ensuite les réseaux directement connectés à chacun d'eux.

Vérifier la configuration OSPF. Tout d'abord, vérifions que les routeurs ont établi une relation de voisinage en tapant la commande **show ip ospf Neighbour** sur R1:

```
R1(config)#rou
R1(config)#router osp
R1(config)#router ospf 1
R1(config-router)#net
R1(config-router)#network 192.168.10.0 255.255.255.0 are
R1(config-router)#network 192.168.10.0 255.255.255.0 area 0
R1(config-router)#network 172.16.1.0 255.255.255.252 area 0
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
01:31:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.20.1 on
Serial0/0/0 from LOADING to FULL, Loading Done

R1#sh
R1#show ip ospf nei
R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
Interface
192.168.20.1     0    FULL/ -         00:00:36    172.16.1.2
Serial0/0/0
R1#
```

Ensuite, pour vérifier que R1 a appris la route vers le réseau 192.168.20.0, nous utiliserons la commande **show ip route ospf** sur R1:

```
R1#show ip route ospf
O    192.168.20.0 [110/65] via 172.16.1.2, 00:04:16, Serial0/0/0

R1#
```

Notez que la lettre O indique les routes OSPF.

Enfin, vérifiez la connectivité. Envoyez une requête ping à PC2 depuis PC1. Le ping devrait réussir.

```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time=1ms TTL=126
Reply from 192.168.20.2: bytes=32 time=1ms TTL=126
Reply from 192.168.20.2: bytes=32 time=2ms TTL=126
Reply from 192.168.20.2: bytes=32 time=6ms TTL=126

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 6ms, Average = 2ms

C:\>
```

## **Conclusion générale**

### **Conclusion générale**

Le présent document est rédigé dans le but d'élucider les principes de configuration de la commutation et du routage IP. En général, ce travail est scindé en deux parties :

Pour la première partie « La Commutation dans les LANs », l'objectif est de permettre aux étudiants de comprendre les principes de base de la commutation dans un réseau local et le fonctionnement des principaux protocoles de la couche 2 du modèle OSI. L'accent est mis principalement sur le réseau avec des liens redondant (Spanning Tree), les réseaux VLAN et le routage Inter-VLAN ainsi que le protocole Etherchannel entre commutateurs.

La deuxième partie « Le Routage IP : Statique et Dynamique », aborde les avantages et inconvénients de la mise en place d'un routage statique ou dynamique ainsi leurs différences conceptuelle, dans cette partie on a étudié aussi le principe de fonctionnement de multiple protocoles de routage IP tels que : RIP, OSPF et EIGRP.

## Références

### Références

- [1] Cisco Systems, Inc., “Configuration Fundamentals Configuration Guide, Cisco IOS Release15S”, 2014,  
<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15s/fundamentals-15-s-book.pdf>
- [2] A JESIN, “Packet Tracer Network Simulator: Simulate an unlimited number of devices on a network using Packet Tracer “, Packt Publishing Limited, Janvier 2014, ISBN: 978-1-78217-042-6.
- [3] Laurent SCHALKWIJK, André VAUCAMPS, “CISCO - Routage et Commutation : 2<sup>ème</sup> module de préparation à la certification CCNA 200-120“, Éditions ENI, Octobre2015, ISBN: 978-2-7460-9785-8.
- [4] Claude SERVIN, “Réseaux et télécoms - Cours avec 129 exercices corrigés“, Dunod Sciences sup, 2<sup>ème</sup> édition, Août 2006, ISBN: 978-2-10-049148-3.
- [5] Laurent SCHALKWIJK, Romain LEGRAND, “Les réseaux avec Cisco : Connaissances approfondies sur les réseaux“, Éditions ENI, 3<sup>e</sup> édition, Janvier 2015, ISBN: 978-2-409-01051-4.
- [6] Aurélien ROUX, “Cisco: entraînez-vous à configurer routeurs et commutateurs“, Éditions ENI, Seconde édition, Janvier 2009, ISBN: 978-2-746-04687-0.
- [7] Valentin Weber, CCNP switches, spanning-tree, 2013,  
<https://www.networklab.fr/spanning-tree-theorie/>
- [8] Cisco Systems, Inc., “Présentation et configuration du protocole Spanning Tree (STP) sur les commutateurs Catalyst “, Cours Cisco - Réussir son CCNA, Mis à jour:17 Août 2006, ID du document:5234.  
[https://www.cisco.com/c/fr\\_ca/support/docs/lan-switching/spanning-tree-protocol/5234-5.pdf](https://www.cisco.com/c/fr_ca/support/docs/lan-switching/spanning-tree-protocol/5234-5.pdf)
- [9] François Emmanuel Goffinet, CCNA partie 12, redondance de liens, spanning tree et rapid spanning tree, 2021,  
<https://cisco.goffinet.org/ccna/redondance-de-liens/spanning-tree-rapid-stp-pvst-cisco/>
- [10] Haugeard LAURENT, “Agrégation de liens Ethernet - Etherchannel sur switch Cisco“, Documentation version 1.0 créé le 19 avril 2005,  
<http://index-of.es/Varios/Reseau/Etherchannel.pdf>
- [11] François emmanuel Goffinet, ccna partie 12 redondance de liens, Cisco Etherchannel : configuration, vérification et dépannage, 2021,  
<https://cisco.goffinet.org/ccna/redondance-de-liens/cisco-etherchannel-configuration-verification-depannage/>
- [12] Cisco Systems, Inc., Packet Tracer : configuration d’EtherChannel ,2014,

## Références

<http://cisco.ofppt.info/ccna3/course/files/3.2.1.3%20Packet%20Tracer%20-%20Configuring%20EtherChannel%20Instructions.pdf>

[13] André VAUCAMPS, “CISCO - Protocoles et concepts de routage -Configuration avancée des routeurs“, Éditions ENI, Août 2010, ISBN : 978-2-7460-0581-6.

[14] Innokenty RUDENKO, “Configuration IP des routeurs Cisco“, Éditions Eyrolles, Paris, Décembre 2000, ISBN: 2-212-09238-5.

<https://www.eyrolles.com/Informatique/Livre/configuration-ip-des-routeurs-cisco-9782212092387/>