Réseau

- Fiche TP - PacketTracer - Révisions 1
- Fiche TP - PacketTracer - Révisions 2

Fiche TP - PacketTracer - Révisions 1

I. Introduction

Cette fiche de TP vise à mettre en pratique les notions de bases du réseau sur cisco packet tracer.

Ce TP récapitulera les notions vues en première année, telles que :

- La création d'un premier réseau.
- La création des VLAN, access et Trunk.
- Le routage statique
- Le NAT / PAT
- Le DHCP
- La configuration des connexions à distance et la sécuritation des accès
- Les ACL

L'ensemble des systèmes et protocoles de redondance seront vu dans un second temps (routage dynamique, rstp, agrégation de ports, topologie meshée)

> **Prérequis** : Pour commencer ce TP, il faut télécharger et installer Cisco Packet Tracer et disposer d'un compte netacad.

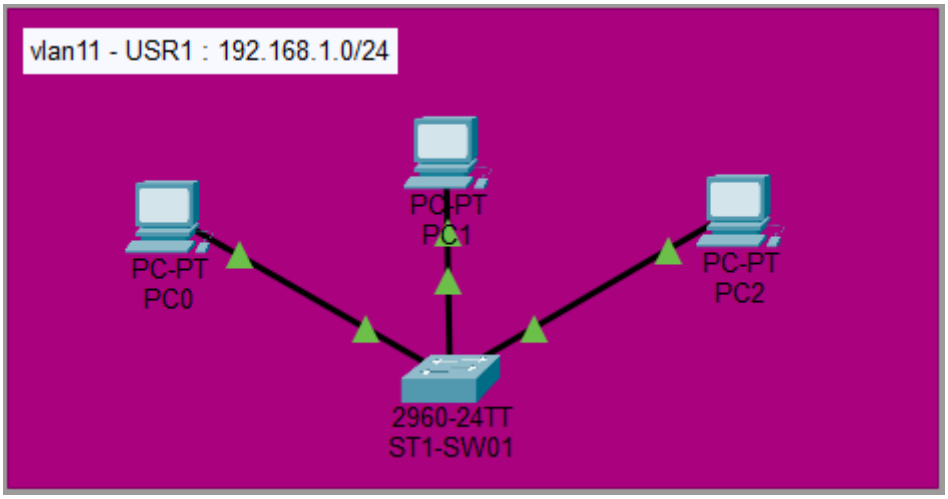
> **Conseil** : Au besoin, une version complétée du TP est disponible ci-joint.

II. Réseau simple

2.1 Paramétrage de base

Le premier objectif est de créer un réseau simple avec 2 ou 3 Postes reliés par un switch et paramétrer basiquement le switch

Premier réseau : VLAN 11 - 192.168.1.0/24



Paramétrer 3 PC en ip fixe, puis relier un switch et effectuer le paramétrage de base de celui-ci :

Paramétrage ST1-SW01

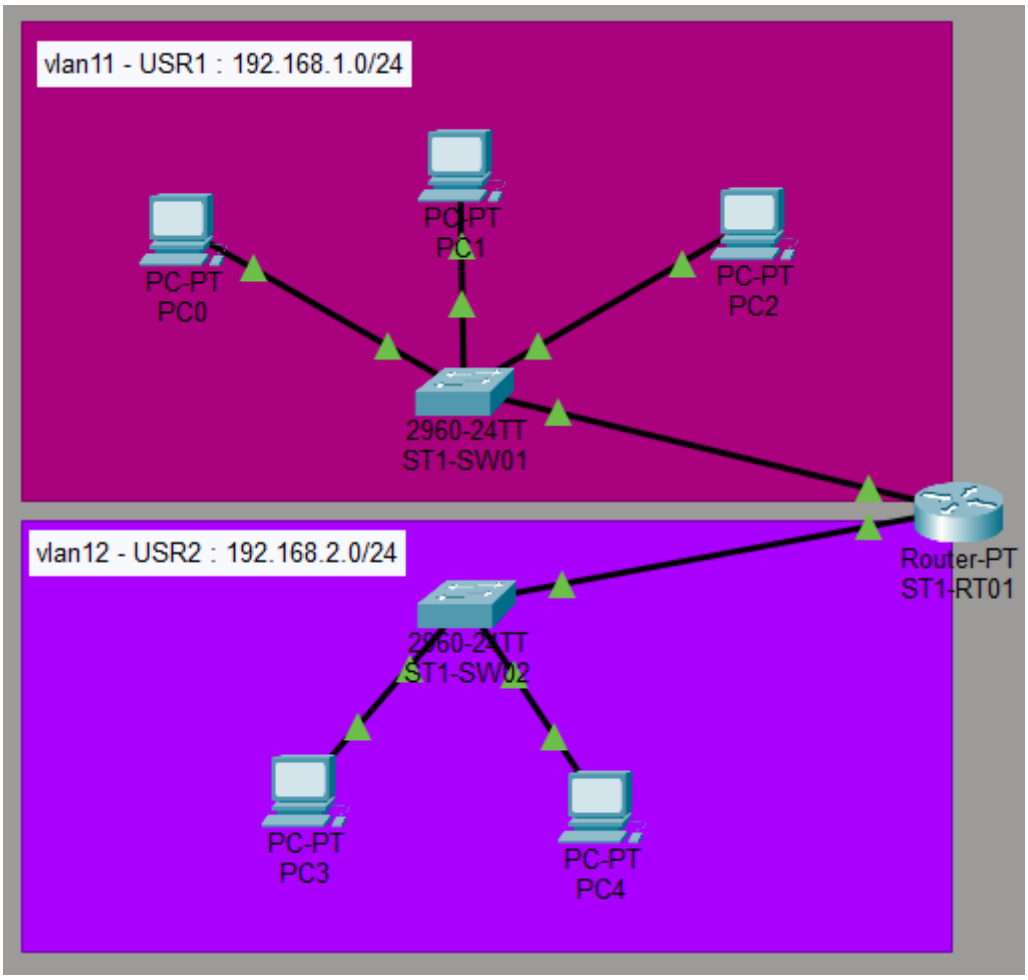
```
# Passer en mode privilège
enable

# Passer en mode configuration ( fonctionne aussi avec 'conf t')
configure terminal

# Paramétrer le hostname, le domaine, la timezone et l'heure.
hostname ST1-SW01
ip domain-name lab.local
```

```
clock timezone CET 1

# Sortir du mode configuration
exit
clock set hh:mm:ss mois jour année


# Sauvegarder la configuration
copy running-config startup-config
```

2.2 Ajout de routeur

L'objectif suivant est d'ajouter un second réseau et de les router afin que ceux-ci communiquent.

Second réseau : VLAN 12 - 192.168.2.0/24



Paramétrer un second switch comme pour le premier.

Ajouter un routeur avec le modèle '***PT-Router***'.

Puis paramétrer le routeur.

Paramétrage ST1-RT01

```
# Passer en mode privilèges
enable
# Passer en mode configuration ( fonctionne aussi avec 'conf t')
configure terminal

# Paramétrer le hostname, le domaine, la timezone et l'heure.
hostname ST1-RT01
ip domain-name lab.local
clock timezone CET 1
```

```
exit
clock set hh:mm:ss mois jour année

conf t

#Configurer les interface réseaux et adresses IP
interface GigabitEthernet 1/0
ip address 192.168.1.254 255.255.255.0
no shutdown
exit

interface GigabitEthernet 2/0
ip address 192.168.2.254 255.255.255.0
no shutdown
exit

# Sortir du mode configuration
exit

# Sauvegarder la configuration
copy running-config startup-config
```

Les postes des deux réseaux sont désormais capable de se joindre.

III. Réseau avancé

3.1 Ajout de vlan + trunk

Nous allons ensuite créer un second site, avec un réseau administrateur et un réseau serveur.

Mais nous n'allons y mettre qu'un seul routeur avec 2 interface et un seul switch pour économiser sur le matériel.

RAPPEL : Définition du VLAN

Un ***VLAN*** **(Virtual Local Area Network)** est un ***domaine de broadcast logique*** créé au sein d'un réseau local, permettant de segmenter un même switch physique en plusieurs réseaux virtuels indépendants. Cette segmentation se fait à la ***couche 2*** du modèle OSI (couche Liaison de données).

Cela permet notamment d'améliorer la sécurité en séparant les réseaux et d'en optimiser le fonctionnement en réduisant les domaines de collision.

Lorsque des VLANs doivent traverser un lien entre switches (trunk), on utilise le ***VLAN tagging*** , défini par la norme ***IEEE 802.1Q***.

Le switch ajoute dans la trame Ethernet un champ de 4 octets contenant :

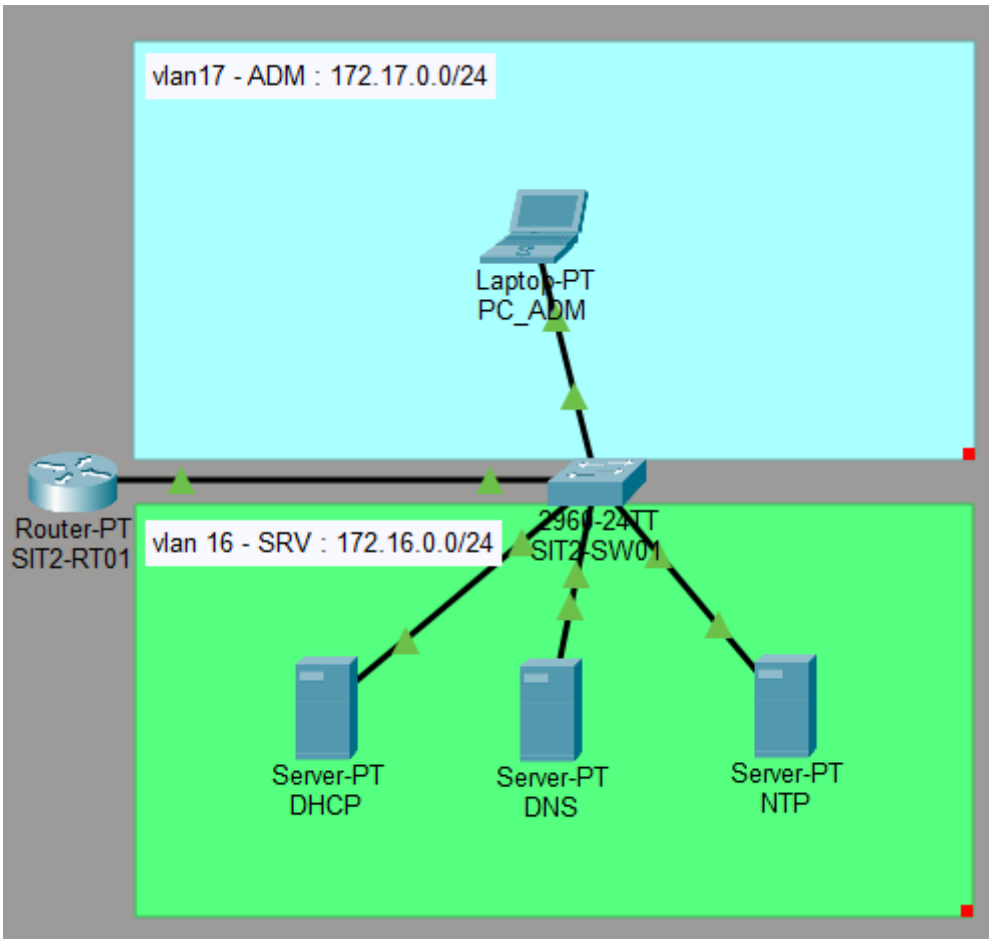
- **Tag Protocol Identifier (TPID)** : identifie qu'il s'agit d'une trame VLAN
- **Tag Control Information (TCI)**, qui inclut :

- **VLAN ID (12 bits)** → identifie le VLAN (0–4095, dont 1–4094 utilisables)
- **Priority Code Point (PCP)** → priorité (QoS)
- **DEI** → indication de congestion

Ce tag permet aux équipements réseau de savoir à quel VLAN appartient la trame lorsqu'elle circule sur un lien partagé.

Réseau 1 : VLAN17 - 172.17.0.0/24

Réseau 2 : VLAN 16 - 172.16.0.0/24



Paramétrage SIT2-SW01

```
# Entrer en mode privilège
enable

# Entre en mode configuration
conf t

# Créer les VLAN
vlan 16
name server
exit

vlan 17
name admin
exit
```

```
# Attribuer les port dans les vlan
interface FastEthernet 0/1
switchport mode access
switchport access vlan 17
exit

interface range FastEthernet 0/2 - 4
switchport mode access
switchport access vlan 16
exit

# Créer le trunk
interface GigabitEthernet 0/1
switchport mode trunk
switchport trunk allowed vlan 16,17
switchport trunk native vlan 1
exit

# Sortir du mode configuration
exit

# Sauvegarder la conf
copy running-config startup-config
```

paramétrage SIT2-RT01

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t

# Activer l'interface
interface GigabitEthernet 1/0
no shut
exit

# Créer les sous-interfaces VLAN virtuelles et les binder sur l'interface physique
```

```
interface GigabitEthernet 1/0.1
encapsulation dot1Q 16
ip address 172.16.0.254 255.255.255.0
no shut
exit

interface GigabitEthernet 1/0.2
encapsulation dot1Q 17
ip address 172.17.0.254 255.255.255.0
no shut
exit

# sortir du mode configuration
exit

# Sauvegarder la conf
copy running-config stratup-config
```

3.2 Interconnexion et tables de routage

Nous allons maintenant créer un réseau d'interconnexion et écrire les tables de routage.

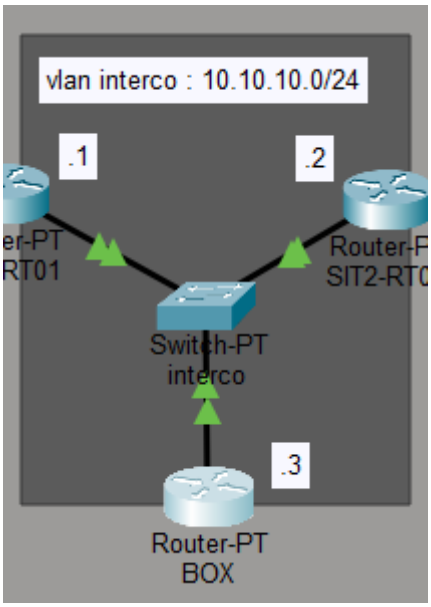
Ajouter un 'PT switch' qui servira de liaison interco. Pas besoin de configuration, il ne servira que pour les liaisons physiques.

Il faut ajouter un routeur qui fera office de 'box internet' sur ce réseau.

Réseau interco : VLAN 100 - 10.10.10.0/24

On part sur les adresses suivantes :

- SIT1-RT1 : 10.10.10.1
- SIT2-RT1 : 10.10.10.2
- BOX : 10.10.10.3



Paramétrage ST1-RT01 (à gauche)

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t

# Paramétrage interface interco
interface GigabitEthernet 0/0
ip address 10.10.10.1 255.255.255.0
no shut
exit

# Remplir la table de routage
ip route 172.16.0.0 255.255.255.0 10.10.10.2
ip route 172.17.0.0 255.255.255.0 10.10.10.2
ip route 0.0.0.0 0.0.0.0 10.10.10.3
exit

# Sauvegarder la conf
copy running-config startup-config
```

Paramétrage ST2-RT02 (à droite)

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t

# Paramétrage interface interco
interface GigabitEthernet 0/0
ip address 10.10.10.2 255.255.255.0
no shut
exit

# Remplir la table de routage
ip route 192.168.1.0 255.255.255.0 10.10.10.1
ip route 192.168.2.0 255.255.255.0 10.10.10.1
ip route 0.0.0.0 0.0.0.0 10.10.10.3
exit

# Sauvegarder la conf
copy running-config startup-config
```

Paramétrage "box"

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t

# Paramétrage interface interco
interface GigabitEthernet 0/0
ip address 10.10.10.3 255.255.255.0
no shut
exit
```

```
interface GigabitEthernet 0/1
ip address 8.8.8.1 255.255.255.0
no shut
exit

# Remplir la table de routage
ip route 192.168.1.0 255.255.255.0 10.10.10.1
ip route 192.168.2.0 255.255.255.0 10.10.10.1
ip route 172.16.0.0 255.255.255.0 10.10.10.2
ip route 172.17.0.0 255.255.255.0 10.10.10.2
exit

# Sauvegarder la conf
copy running-config startup-config
```

IV. Liaison "internet"

4.1 NAT / PAT

Pour émuler une connexion internet, nous allons ajouter un serveur à l'extérieur sur la patte du routeur 'box'.

Réseau "internet" : 8.8.8.0/24

serveur "google" : 8.8.8.8

RAPPEL : Définition du NAT / PAT

Le ***NAT*** **(Network Address Translation)** est un mécanisme permettant de ***traduire des adresses IP privées en adresses IP publiques*** (et inversement) lors du passage d'un routeur. Il agit principalement à la ***couche 3*** du modèle OSI (couche Réseau).

Cela permet d'économiser les adresses IP publiques, masquer la topologie interne du réseau (masquerading) et faciliter la modification ultérieure des plans d'adressages internes.

Il y a 3 types de NAT :

- NAT statique : 1 ip privée = 1 ip publique (NAT 1:1)
- NAT dynamique : un pool d'adresses publiques est attribué dynamiquement
- ***PAT*** **(Port Address Translation)** : plusieurs ip privées = 1 ip publique sur des ports de sortie différents (sockets)

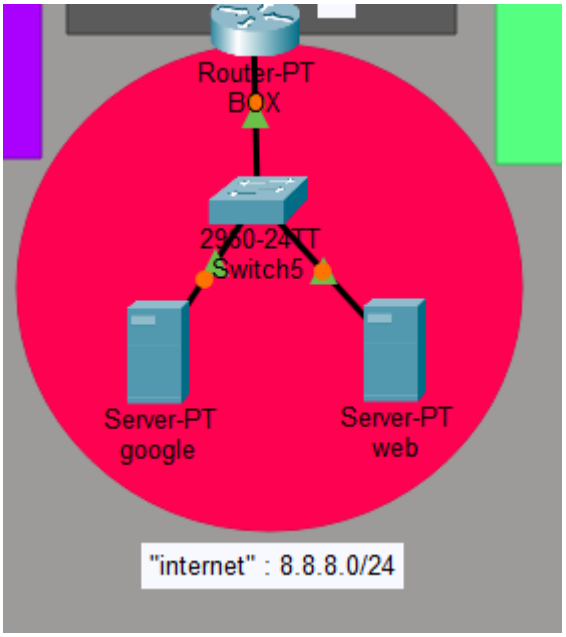
Le ***PAT***, parfois appelé **NAT surcharge (overload)**, est une extension du NAT permettant à plusieurs hôtes privés de partager une seule adresse IP publique.

Le routeur translate non seulement l'ip privée en IP publique, mais également le port source.

Ainsi chaque flux sortant est identifié par in socket (couple ip/port) qui permet de maintenir une table de correspondance interne.

Le PAT à 3 avantages :

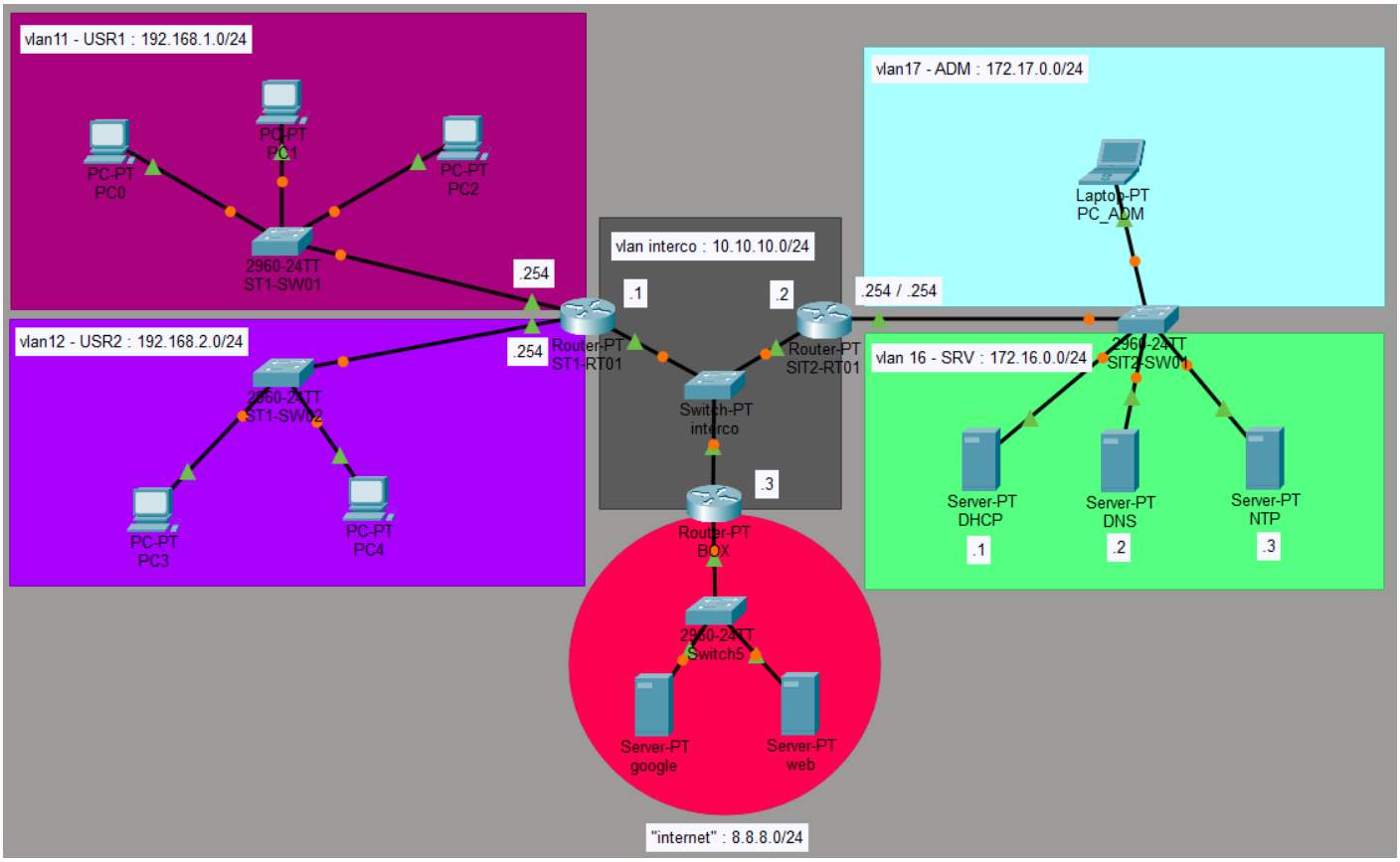
- Economie d'adresses publiques encore plus importante
- Fonctionne peut importe le nombre d'hôtes sortants
- Transparent pour les utilisateurs



routeur "box" paramétrage NAT

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t

# Définir les interfaces internes et externes

interface GigabitEthernet 0/0
ip nat inside
exit

interface GigabitEthernet 1/0
ip nat outside
exit

# Créer le pool d'adresses (ici une seule car PAT et pas NAT)
ip nat pool OUTips 8.8.8.1 8.8.8.1 netmask 255.255.255.0

# Créer les ACL
access-list 10 permit 172.16.0.0 0.0.0.255
access-list 10 permit 172.17.0.0 0.0.0.255
access-list 10 permit 192.168.1.0 0.0.0.255
access-list 10 permit 192.168.2.0 0.0.0.255

# Appliquer le PAT (ajout de overload pour passer en PAT et pas en NAT)
ip nat inside source list 10 pool OUTips overload

# Sortir de la conf
exit

# Sauvegarder la conf
copy running-config startup-config
```

Le réseau est désormais pleinement fonctionnel.



V. DHCP interne

5.1 Réseaux utilisateurs (sur le routeur)

Sur cette étape, le but est d'utiliser le routeur comme serveur DHCP pour les deux réseaux utilisateurs.

Routeur SIT1-RT01

```
# Entrer en mode privilèle
enable

# Entrer en mode configuration
conf t
```

```
# Définir les pools dhcp
ip dhcp pool CLI1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.254
dns-server 172.16.0.2
domain-name lab.local
exit

ip dhcp pool CLI2
network 192.168.2.0 255.255.255.0
default-router 192.168.2.254
dns-server 172.16.0.2
domain-name lab.local
exit

# Définir les plages d'exclusions
ip dhcp excluded-address 192.168.1.21 192.168.1.254
ip dhcp excluded-address 192.168.2.21 192.168.2.254

# Sortir du mode config
exit

# sauvegarder la conf
copy running-config startup-config
```

5.2 Réseau admin (via relai)

Sur cette étape, le but est de paramétrer le relai DHCP sur le routeur SIT1-RT1 pour que le routeur relaye les demandes au DHCP tier.

On part du principe que le serveur DHCP est installé dans le réseau ***172.16.0.0/24*** et à l'adresse ***172.16.0.1***.

Routeur SIT2-RT01

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t

# Activer le relai DHCP
interface GigabitEthernet 1/0.2
ip helper-address 172.16.0.1
exit

# Sortir du mode config
exit

# sauvegarder les modifs
copy running-config startup-config
```

VI. Activation du SSH + Sécurisation

6.1 Activation SSH

Nous allons activer le SSH sur les équipements afin de pouvoir en centraliser l'administration.

> **Prérequis** : les paramètres suivant doivent avoir été initialisés : hostname, domaine, adresse IP.

> **Info** : Voici une liste des privilèges.

Par défaut, il existe trois niveaux de commande sur le routeur :

- privilege level 0 : inclut les commandes disable, **enable**, **exit**, **help** et **logout**
- privilege level 1 : inclut toutes les commandes de niveau *utilisateur* à l'invite `router>`.
- privilege level 15 : inclut toutes les commandes *enable*-level à l'invite `router>`

Les manipulations doivent être effectuées sur toutes les équipements à manager.

Activation SSH

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t

# créer l'utilisateur SSH
username admin privilege 15 password <motdepasse>

# Générer les clé
crypto key generate rsa general-keys modulus 512

# Configurer la ligne SSH
line vty 0 15
login local
transport input ssh
ip ssh version 2
end

# Ecrire la configuration de la ligne
write

# Chiffrer les mots de passe
service password-encryption

# Sortir du mode config
exit
```

```
# Enregistrer la conf
copy running-config startup-config
```

Il est également possible d'ajouter une bannière à la connexion :

Ajout de bannière

> **Info** : Il existe 4 types de bannières : **MODT** (message apparaissant avant la connexion pour indiquer une maintenance ou autre...), **Login** (apparaissant à la connexion), **Exec** (message apparaissant après la connexion).

Ici, il s'agit d'ajouter une Login banner qui sera affichée au moment de la connexion SSH.

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t

# Mettre en place la banière (les # font partie de la commande)
banner login #
Vous vous connectez sur un équipement de la companie lab.local
Toutes les tentatives de connexions sont enregistrées et tracées.
Si vous accédez à cet equipement par erreur, merci de vous déconnecter.
#

# Sortir du mode configuration
exit

# Enregistrer la configuration
copy runnin-config startup-config
```

6.2 Protection par adresses MAC

Nous allons maintenant activer la protection sur les adresses MAC pour éviter qu'un PC tente de prendre la place du pc d'administration.

Cette manipulation se fait sur le switch sur lequel le poste admin est connecté.

configuration sur SIT2-SW01

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t

# Entrer en mode de configuration sur l'interface sur laquelle le PC admin est branché
interface FastEthernet 0/1

# Activer la protection MAC
switchport port-security

# Deux possibilités : apprendre les adresses une par une manuellement
# switchport port-security mac-address <MACduPC>
# ou lancer une phase d'apprentissage
switchport port-security mac-address sticky
```

Le port rentre en mode apprentissage, la prochaine MAC qui se connectera sera mémorisée et fixée dans la table ARP du port.

Pour lister les MAC sur un port : `show mac-address-table`

```
SIT1-SW01#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    00d0.ff11.04e3    DYNAMIC     Gig0/1
  16    00d0.ff11.04e3    DYNAMIC     Gig0/1
  17    00d0.580c.b3d0    STATIC      Fa0/1
  17    00d0.ff11.04e3    DYNAMIC     Gig0/1
SIT1-SW01#
```

Une fois la MAC apprise, choisir l'action à appliquer :

- **shutdown** : éteinds le port (nécessite une action manuelle pour le restart)
- **protect** : ignore le trafic provenant de la MAC non autorisée mais laisse le port allumé
- **restrict** : idem que protect, mais logue les évènement, incrémente le compteur de violation et peut envoyer une trap snmp.

Pour cela, re-entrer dans la configuration de l'interface et ajouter :

```
# Verouiller l'apprentissage et appliquer les actions de sécu
switchport port-security violation shutdown
exit

# quitter le mode config.
exit

# Enregistrer la conf
copy running-config startup-config
```

A posteriori, il sera possible de vérifier les statuts et les compteurs de violations avec

```
show port-security interface FastEthernet 0/1
```

```
SIT1-SW01#show port-security interface fastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00D0.580C.B3D0:17
Security Violation Count   : 0
```

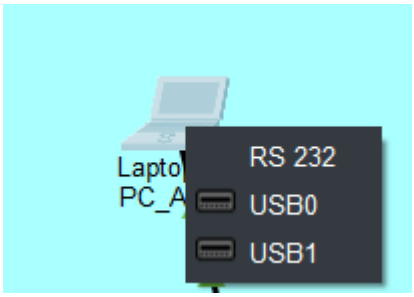
Pour augmenter le nombre d'adresses mémorisées par port, entrer en mode configuration de l'interface puis :

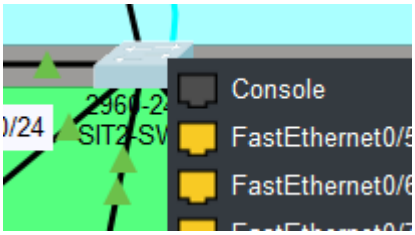
```
switchport port-security maximum <nbAdresseMax>
```

6.3 Activer l'authentification sur le port console

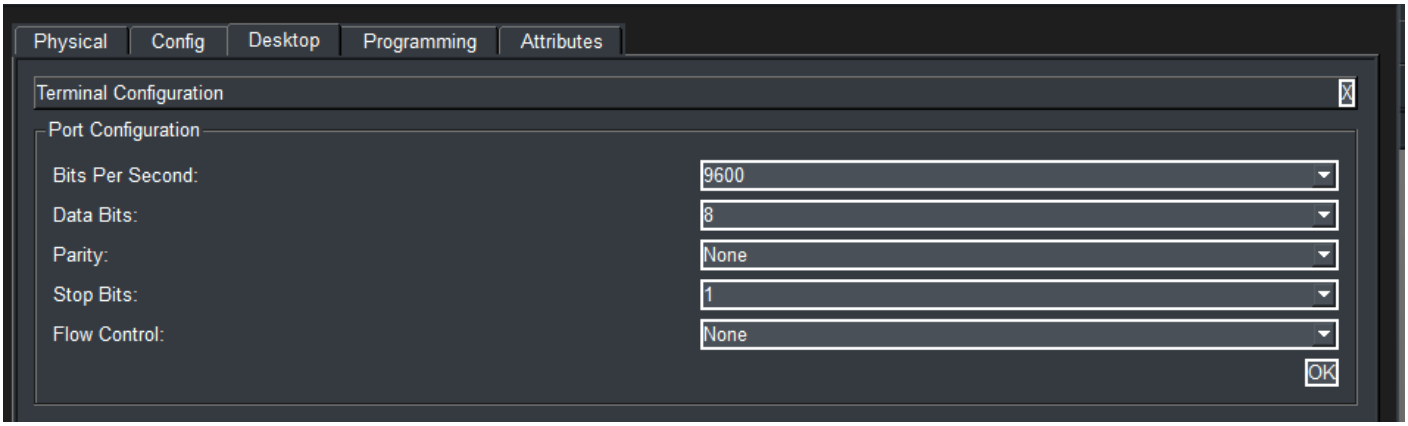
Si l'on tente une connexion en port console aux équipements :

Choisir un câble '***console***', se connecter sur le port '***RS 232***' du PC admin, puis sur le mort console du switch '***SIT2-SW01***'.





Lancer une connexion en mode console depuis le PC portable admin.



La connexion ne demande pas de mot de passe.

Activer l'authentification sur le port console

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t
```

```
# Créer un utilisateur
user admin privilege 15 secret <MotDePasse>

# Configurer l'authentification sur la console
line console 0
login local
end

# Sortir du mode configuration
exit

# Sauvegarder la conf.
copy running-config startup-config
```

6.4 Activer le mot de passe 'enable'

Pour plus de sécurité, il est également possible d'ajouter un mot de passe enable.

Ajout de mot de passe enable et configure.

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t

# Activer le secret Enable
enable secret <MotDePasse>

# Quitter le mode configuration
exit

# Sauvegarder la conf.
copy running-config startup-config
```

VII. Mise en place des ACL

7.1 Restreindre la connexion SSH au PC admin

Pour des raisons de sécurité, il faut interdire l'accès au port SSH aux réseaux non autorisés afin que seul le réseau admin puisse y accéder.

Création ACL SSH

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t

# Créer les ACL
ip access-list extended SSH
permit tcp 172.17.0.0 0.0.0.255 any eq 22
deny tcp any any eq 22
exit

# Ajout des acl dans la conf SSH
line vty 0 15
access-class SSH in
exit

# Quitter le mode configuration
exit

# Enregistrer la conf.
copy running-config startup-config
```

```
SIT2-RT01#show access-lists
Extended IP access list SSH
    10 permit tcp 172.17.0.0 0.0.0.255 any eq 22 (2 match(es))
    20 deny tcp any any eq 22 (32 match(es))
```

7.2 Interdire l'accès au réseau admin depuis les autres réseaux.

Il est également nécessaire de protéger le réseaux admin d'éventuels mouvements latéraux.

Création d'ACL "pare-feu"

```
# Entrer en mode privilège
enable

# Entrer en mode configuration
conf t

# Créer les ACL
ip access-list extended ADMIN
permit ip 172.17.0.0 0.0.0.255 any
deny ip any 172.17.0.0 0.0.0.255
permit any any
exit

# Appliquer les ACL
interface GigabitEthernet 1/0
ip access-group ADMIN in
exit

# Sortir du mode configuration
exit

# Sauvegarder la conf.
copy running-config stratup-config
```

Fiche TP - PacketTracer - Révisions 2

> ***DISCLAIMER : Cette page est actuellement en cours de rédaction et son contenu peut être incomplet ou inexact***

I. Introduction

Cette fiche de TP vise à mettre en pratique les notions de bases du réseau sur cisco packet tracer.

Ce TP récapitulera les notions vues en première année, telles que :

- Protocoles redondance de lien (LAGG, LACP)
- Protocole de routage dynamique (RIP, OSPF)
- Protocole de redondance de routage (VRRP)
- Protocole de topologie (RSTP)

> **Prérequis** : Pour commencer ce TP, il faut télécharger et installer Cisco Packet Tracer et disposer d'un compte netacad.

> **Info** : Ce TP fait suite à : **Fiche TP - CiscoPacketTracer - Révisions 1**

> **Conseil** : Au besoin, une version complétée du TP est disponible ci-joint.

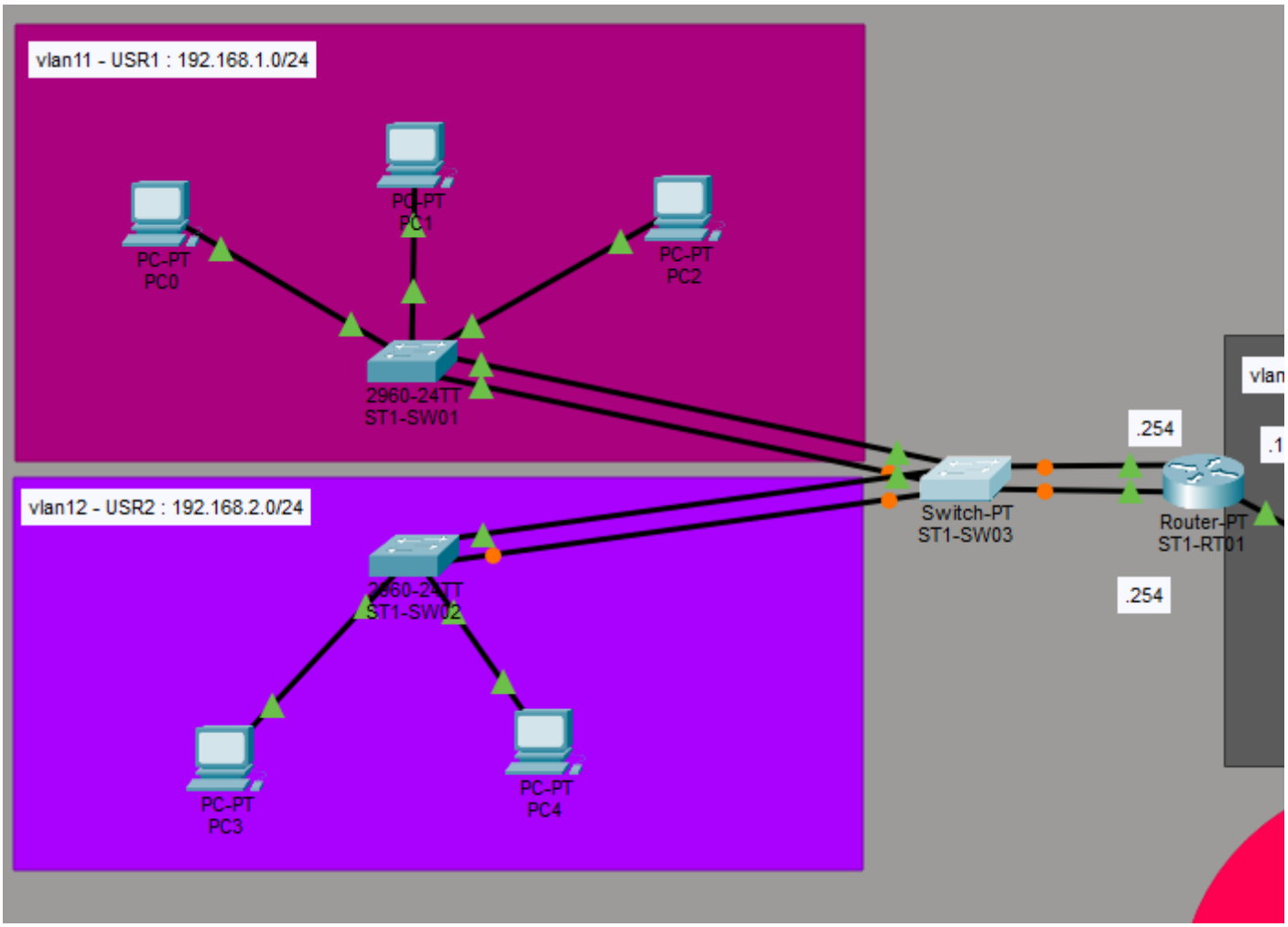
II. Protocoles de redondance de lien

2.1 Paramétrage du LACP (switches)

> **Info** : Plus d'information sur la redondance de lien : **Réseau - L'agrégation de liens (LAGG)**

Le premier objectif sera d'ajouter un switch central côtés VLAN utilisateurs afin de pouvoir ajouter de nouveaux VLANs ou bâtiments dans le futur. Puis de configurer du LACP entre les switch upstream et downstream afin de créer de la redondance de lien.

> **Attention** : pour éviter les erreurs et les boucles réseaux, il faut connecter les liens à la fin (après que les configurations soient faites).



Il va falloir :

1. Ajouter les cartes réseaux nécessaires sur les différents équipements.
2. Déclarer les VLAN sur les différents switches
3. Attribuer les ports aux VLAN
4. Configurer les LAGG
5. Configurer le LAGG / Trunk sur le ST1-SW03
6. Configurer les LAGG / Trunk sur le routeur

Les différents mode de LAGG sont les suivants :

```
ST1-SW01(config-if-range)#channel-group 1 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
```

Les différents protocoles sur les switches sont :

```
ST1-SW01(config-if-range)#channel-protocol ?
  lacp  Prepare interface for LACP protocol
  pagp  Prepare interface for PAgP protocol
```

Paramétrage ST1-SW01

> **Info** : Pas d'interfaces à ajouter.

```
# Passer en mode privilège
enable

# Passer en mode configuration ( fonctionne aussi avec 'conf t')
configure terminal

# Configurer le VLAN 11
vlan 11
name VLAN11-USR

# Sortir de la config du VLAN
exit

# Attribuer les ports du siwtch au vlan
int range fa 0/1 - 24
sw mode access
sw access vlan 11
exit

# Monter le LAGG
int range gi 0/1-2
channel-group 1 mode active
channel-protocol lacp
exit

# Paramétrer le vlan sur le LAGG
int port-channel 1
sw mode access
sw access vlan 11
exit
```

```
# Sortir du mode config
exit

# Sauvegarder la configuration
copy running-config startup-config
```

Paramétrage ST1-SW02

> **Info** : Pas d'interfaces à ajouter.

```
# Passer en mode privilège
enable

# Passer en mode configuration ( fonctionne aussi avec 'conf t')
configure terminal

# Configurer le VLAN 12
vlan 12
name VLAN12-USR

# Sortir de la config du VLAN
exit

# Attribuer les ports du siwtch au vlan
int range fa 0/1 - 24
sw mode access
sw access vlan 12
exit

# Monter le LAGG
int range gi 0/1-2
channel-group 2 mode active
channel-protocol lacp
exit

# Paramétrer le vlan sur le LAGG
```

```
int port-channel 2
sw mode access
sw access vlan 12
exit

# Sortir du mode config
exit

# Sauvegarder la configuration
copy running-config startup-config
```

Paramétrage ST1-SW03

Créer un PT-Switch et ajouter 6 interfaces CGE.


```
# Passer en mode privilège
enable

# Passer en mode configuration ( fonctionne aussi avec 'conf t')
conf t

# Faire la configuration de base
hosname ST1-SW03
ip domain-name lab.local
clock timezone CET 1
exit
clock set hh:mm:ss mois jour année

# Revenir en mode config
conf t

# Configurer les vlan
vlan 11
name VLAN11-USR
vlan 12
```

```
name VLAN12-USR
exit

# Monter les LAGG
int range gi 0/1, gi 1/1
channel-group 1 mode active
channel-protocol lacp

int range gi 2/1, gi 3/1
channel-group 2 mode active
channel-protocol lacp

exit

# Paramétrer les vlan sur les LAGG
int port-channel 1
sw mode access
sw access vlan 11

int port-channel 2
sw mode access
sw access vlan 12

int gi 4/1
sw mode access
sw access vlan 11

int gi 5/1
sw mode access
sw access vlan 12

exit

# Sortir du mode config
exit

# Sauvegarder la configuration
copy running-config startup-config
```

Pour vérifier l'état des différent lagg

```
show etherchannel summary
```

```
ST1-SW03>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: 3
Number of aggregators:           3

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------

1      Po1(SU)           LACP   Gig0/1(P) Gig1/1(P)
2      Po2(SU)           LACP   Gig2/1(P) Gig3/1(P)
3      Po3(SD)           LACP   Gig4/1(D) Gig5/1(D)
ST1-SW03>
```

A ce stade, toutes les adresses peuvent être PING et le fait de couper un lien ne coupe pas le réseau.

Cependant, lors de la reconnexion, quelques paquets sont perdus le temps que le LACP recalcule. Cela ne s'observe pas avec autant de latence dans la vie réelle.

2.2 Paramétrage du LACP (routeur)

Pour le routeur, cela va se compliquer.

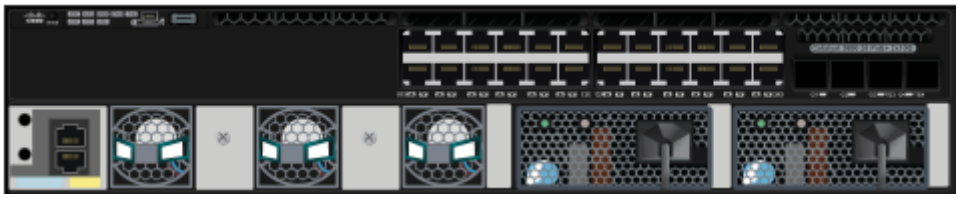
En effet, les routeurs ne travaillent que sur la L3 et le LACP est un protocole L2.

Les deux problématiques (routages / LACP) deviennent donc inconciliables.

C'est notamment pour répondre à ces problématiques qu'il va faloir introduire un nouvel équipement : Le switch L3.

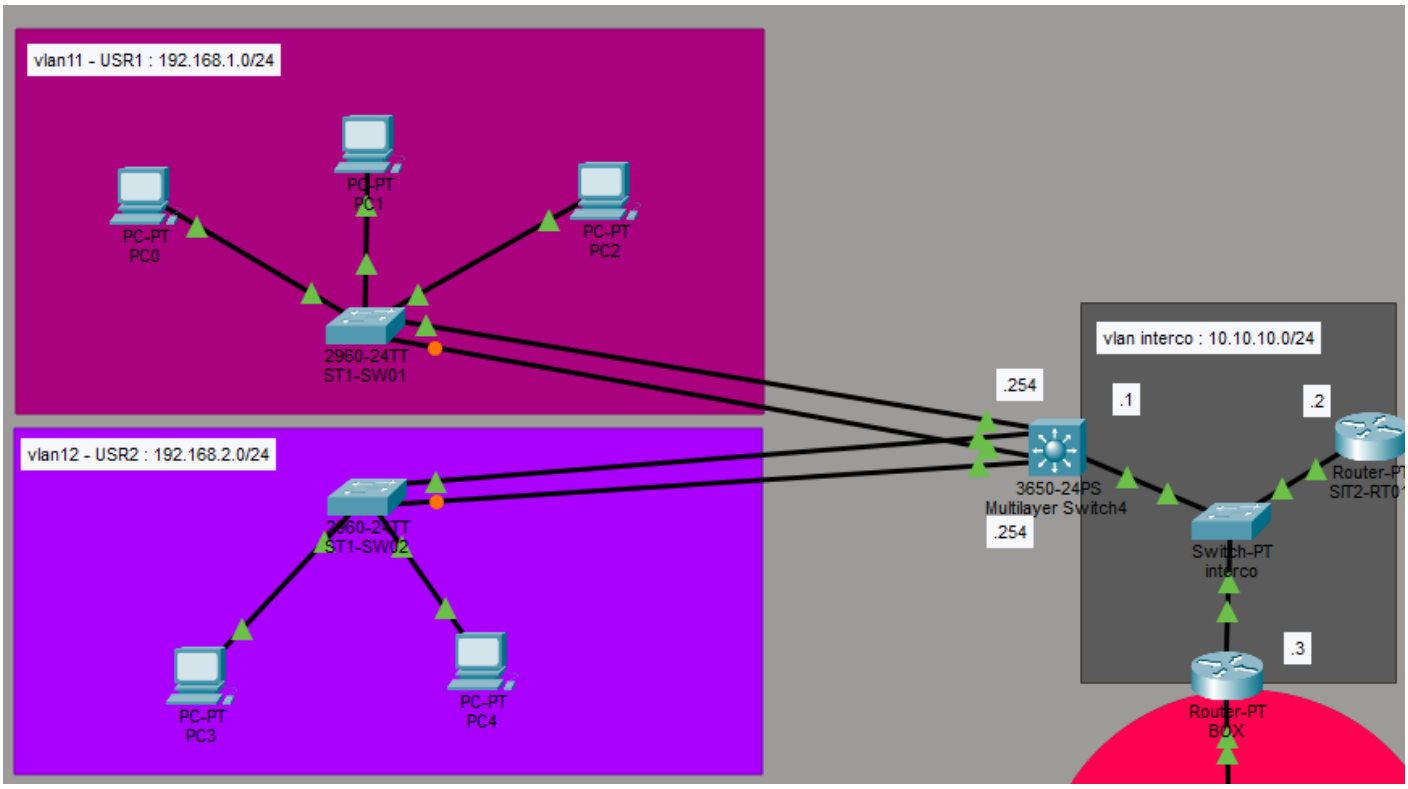
Il s'agit de switches manageables, capables de gérer à la fois la couche L2 et la couche L3. Ce switch viendra alors remplacer à la fois le ST1-SW03 et le ST1-RT01 et agira donc en qualité de

switch/routeur.



Modèle 3650-24PS

Voici la nouvelle topologie :



Il faut enfin configurer le switch L3.

Paramétrage ST1-RT01

```
# Passer en mode privilège
enable

# Passer en mode configuration ( fonctionne aussi avec 'conf t')
conf t
```

```
# Faire la configuration de base
hosname ST1-RT01
ip domain-name lab.local
clock timezone CET 1
exit
clock set hh:mm:ss mois jour année

# Revenir en mode config
conf t

# Configurer les vlan
vlan 11
name VLAN11-USR

vlan 12
name VLAN12-USR

exit

# créer les LACP
int range gi 1/0/1-2
channel-group 1 mode active
channel-protocol lacp

int range gi 1/0/3-4
channel-group 2 mode active
channel-protocol lacp

exit

# Configurer les interfaces (L2)
int port-channel 1
sw mode access
sw access vlan 11

int port-channel 2
sw mode access
sw access vlan 12
```

```
int gi 1/0/24
sw mode access
sw access vlan 1

exit

# Configurer les interfaces (L3)
int vlan 11
ip addr 192.168.1.254 255.255.255.0

int vlan 12
ip addr 192.168.2.254 255.255.255.0

exit

# Paramétrage interface interco
interface vlan 1
ip address 10.10.10.1 255.255.255.0
no shut
exit

# Activer la fonction routage
ip routing

# Refaire les tables de routages
ip route 172.16.0.0 255.255.255.0 10.10.10.2
ip route 172.17.0.0 255.255.255.0 10.10.10.2
ip route 0.0.0.0 0.0.0.0 10.10.10.3
exit

# Refaire les pools dhcp
ip dhcp pool CLI1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.254
dns-server 172.16.0.2
domain-name lab.local
exit
```

```
ip dhcp pool CLI2
network 192.168.2.0 255.255.255.0
default-router 192.168.2.254
dns-server 172.16.0.2
domain-name lab.local
exit

# Refaire les plages d'exclusions
ip dhcp excluded-address 192.168.1.21 192.168.1.254
ip dhcp excluded-address 192.168.2.21 192.168.2.254

# Sortir du mode config
exit

# Sauvegarder la configuration
copy running-config startup-config
```

Les liens entre les switches terrain et le central L3 sont désormais redondés.

III. Passage en routage dynamique

3.1 RIP (Legacy)

> **Info** : Plus d'informations sur le RIP : **Réseau - Protocole RIP**

3.1.1 Configuration

Il est possible sur les routeurs d'activer des protocole de routage dynamique.

Ils vont ainsi s'échanger leur réseaux connus afin d'apprendre eux-même leurs table de routage.

Il va pour cela falloir configurer les trois routeurs.

Paramétrage ST1-RT01

```
# Passer en mode privilège
enable

# Passer en mode configuration ( fonctionne aussi avec 'conf t')
conf t

# Supprimer les routes internes et ne garder que la default en statique
no ip route 172.16.0.0 255.255.255.0 10.10.10.2
no ip route 172.17.0.0 255.255.255.0 10.10.10.2

# Activer le RIP
router rip
version 2
no auto-summary
network 192.168.1.0
network 192.168.2.0
network 10.10.10.0

# N'écouter que sur les interfaces nécessaires
passive-interface default
no passive interface vlan 1

exit

# Sortir du mode config
exit

# Sauvegarder la configuration
```

```
copy running-config startup-config
```

Paramétrage ST2-RT01

```
# Passer en mode privilège
enable

# Passer en mode configuration ( fonctionne aussi avec 'conf t')
conf t

# Supprimer les routes internes et ne garder que la default en statique
no ip route 192.168.1.0 255.255.255.0 10.10.10.1
no ip route 192.168.2.0 255.255.255.0 10.10.10.1

# Activer le RIP
router rip
version 2
no auto-summary
network 172.16.0.0
network 172.17.0.0
network 10.10.10.0

# N'écouter que sur les interfaces nécessaires
passive-interface default
no passive interface gi 0/0

exit

# Sortir du mode config
exit

# Sauvegarder la configuration
copy running-config startup-config
```

Paramétrage Box

```
# Passer en mode privilège
enable

# Passer en mode configuration ( fonctionne aussi avec 'conf t')
conf t

# Supprimer les routes internes et ne garder que la default en statique
no ip route 192.168.1.0 255.255.255.0 10.10.10.1
no ip route 192.168.2.0 255.255.255.0 10.10.10.1
no ip route 172.16.0.0 255.255.255.0 10.10.10.2
no ip route 172.17.0.0 255.255.255.0 10.10.10.2

# Activer le RIP
router rip
version 2
no auto-summary
network 10.10.10.0

# N'écouter que sur les interfaces nécessaires
passive-interface default
no passive interface gi 0/0

exit

# Sortir du mode config
exit

# Sauvegarder la configuration
copy running-config startup-config
```

3.1.2 Commandes utiles

Voici les commandes utiles pour le RIP :

- Vérifier les synchro en temps réel

```
# activer le debug
debug ip rip


# désactiver le debug
undebug all
```

```
RIP: build update entries
      172.16.0.0/24 via 0.0.0.0, metric 1, tag 0
      172.17.0.0/24 via 0.0.0.0, metric 1, tag 0
RIP: received v2 update from 10.10.10.1 on GigabitEthernet0/0
      192.168.1.0/24 via 0.0.0.0 in 1 hops
      192.168.2.0/24 via 0.0.0.0 in 1 hops
RIP: sending  v2 update to 224.0.0.9 via GigabitEthernet0/0 (10.10.10.2)
```

- Vérifier le contenu des tables de routage RIP

```
show ip route rip
```

```
SIT2-RT01#show ip route rip
     172.17.0.0/24 is subnetted, 1 subnets
R    192.168.1.0/24 [120/1] via 10.10.10.1, 00:00:24, GigabitEthernet0/0
R    192.168.2.0/24 [120/1] via 10.10.10.1, 00:00:24, GigabitEthernet0/0
```

- Vérifier les partenaires de synchro

```
show ip rip database
```

```
SIT2-RT01#show ip rip database
10.10.10.0/24    auto-summary
10.10.10.0/24    directly connected, GigabitEthernet0/0
172.16.0.0/24    auto-summary
172.16.0.0/24    directly connected, GigabitEthernet1/0.1
172.17.0.0/24    auto-summary
172.17.0.0/24    directly connected, GigabitEthernet1/0.2
192.168.1.0/24    auto-summary
192.168.1.0/24
    [1] via 10.10.10.1, 00:00:21, GigabitEthernet0/0
192.168.2.0/24    auto-summary
192.168.2.0/24
    [1] via 10.10.10.1, 00:00:21, GigabitEthernet0/0
```

- Vérifier le status du RIP

```
show ip protocols
```

3.1.3 Propager la route par défaut

Il est également possible de propager la route par défaut à l'ensemble des routeurs.

Retirer des routeurs **ST1-RT01** et **ST2-RT01** la route par défaut avec

```
no route 0.0.0.0 0.0.0.0 10.10.10.3
```

Puis sauvegarder les configurations.

Paramétrage BOX

```
# Entrer en mode privilèges
enable

# Entrer en mode configuration
conf t

# Configurer la propagation de la route par défaut
router rip
default-information originate
exit

# Sortir du mode config
exit

# Enregirstrer les modifications
copy running-config startup-config
```

3.1.4 Authentification RIP

> **Attention** : Cisco packet tracer ne prends pas en charge l'authentification RIP. Seuls les firmwares IOS le prennent en charge.

Pour plus de sécurité, il est préférable d'authentifier les flux RIP.

Les routeurs seront ainsi en mesure de se reconnaitre et rejeter les modification effectuées par un routeur non authentifié.

Pour cela, il faut utiliser une clé et les routeurs doivent utiliser :

- Le même nom de clé
- le même numéro de clé
- le même contenu de clé

Voici les configuration à effectuer sur chaque routeur :

Paramétrage des routeurs

```
# Passer en mode privilège
enable

# Passer en mode configuration ( fonctionne aussi avec 'conf t')
conf t

# Déclarer la clé
key chain RIP-KEYS
key 1
key-string <LaCléIci>
exit
exit

# Configurer l'authentification sur l'interface
interface vlan 1
ip rip authentication mode md5
ip rip authentication key-chain RIP-KEYS

# Sortir du mode config
exit

# Sauvegarder la configuration
```

```
copy running-config startup-config
```

3.2 OSPF

IV. RSTP

> **Info** : Par défaut, il n'est pas possible de créer des boucles réseaux, cela entrainerait des tempêtes de broadcast. Le protocole STP/RSTP, permet de répondre à cette problématique. Plus d'informations :

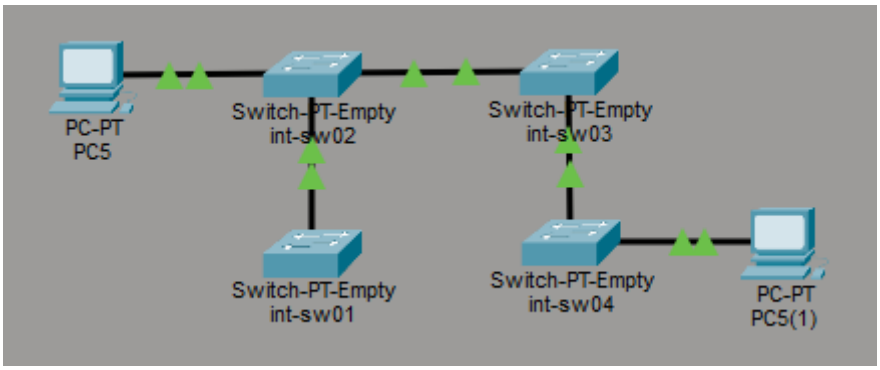
> **Conseil** : Il est préférable, pour éviter les tempêtes de broadcast, de ne brancher les câbles de fermeture de la boucles qu'une fois le paramétrage des ports terminés.

4.1 RSTP (boucle)

Ajouter tout d'abord 4 switch-PT-Empty. Puis changer les interfaces CFE par des interfaces CGE.

Relier les 3 premiers switches. Pour plus de facilité, l'on peut partir de l'interface 0/1 de chaque switch pour arriver sur l'interface 1/1 du suivant.

Ajouter 2 PC qui vont être branchés sur les switchs opposés pour tester les ruptures de liens (sur les ports 3/1, car c'est là que viendrons se brancher les routeurs par la suite).



Configurer les switches :

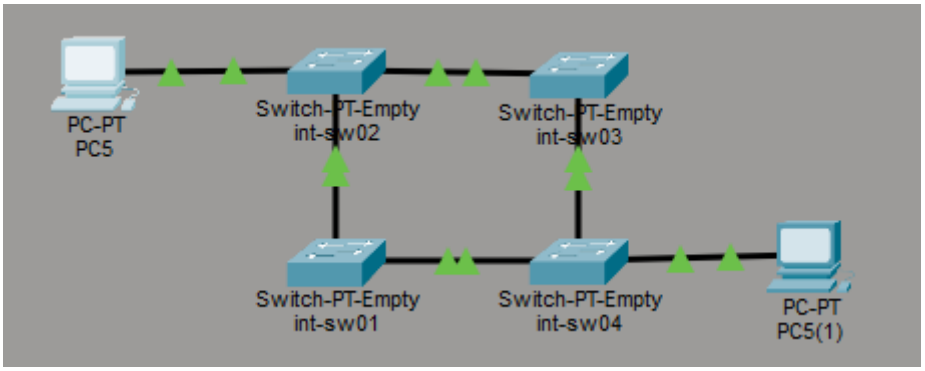
Paramétrage 4 switches interco

```
# Entrer en mode privilèges
enable

# Entrer en mode configuration
conf t

# Faire la configuration de base
hosname INT-SW01
ip domain-name lab.local
clock timezone CET 1
exit
clock set hh:mm:ss mois jour année

# Revenir en mode config
conf t

# Configurer les vlan
vlan 100
name interco
exit

# Activer le rstp
spanning-tree mode rapid-pvst

# Passer le switch en master ( !!!!! que pour le sw01 !!!!! )
spanning-tree vlan 100 priority 4096
```

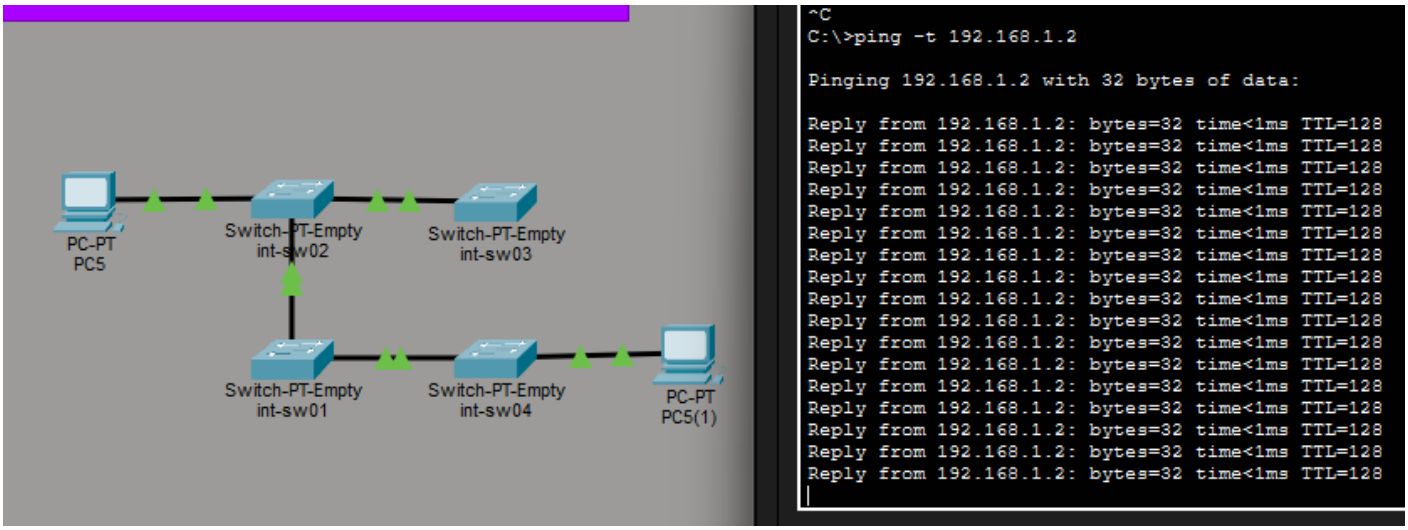
```
# Configurer les ports de liaisons avec les autres switches
int range gi 0/1, gi 1/1, gi 2/1
sw mode trunk
sw trunk allowed vlan 100
spanning-tree link-type point-to-point
no shut
exit

# Configurer le port 3/1 qui recevra le routeur
int gi 3/1
sw mod access
sw access vlan 100
spanning-tree portfast
# Protéger le port des packets BPDU
spanning-tree bpduguard enable
exit

# Sortir du mode configuration et sauvegarder la configuration
exit
copy run start
```

Fermer la boucle.

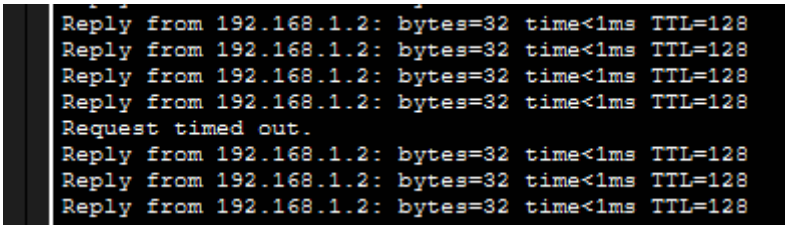
Si tout c'est bien passé, le réseau ne déclenche pas de tempête de broadcast (voyants clignotants frénétiquement) et ne désactive pas les ports.



Les deux pc sont joignables et ce, même si l'on coupe un lien.

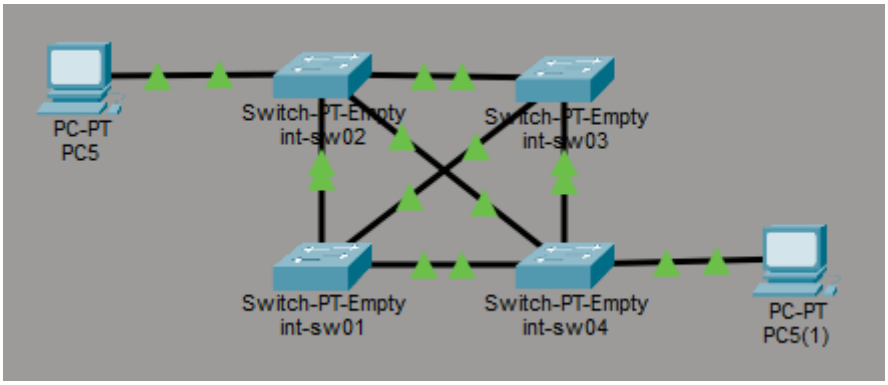


Si il s'agissait du chemin utilisé, le poste loupe un ping, le temps que la cicatrisation réseau se fasse.



4.2 RSTP (mesh)

Les ports 2/1 ayant déjà été configurés à l'étape précédente, ils participent déjà la la topologie. Il ne reste qu'a les brancher.



Il est possible de vérifier le status du RSTP et des interfaces avec :

```
show spanning-tree active
```

```
inst-sw01#show spanning-tree active
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     0002.178B.B911
              Cost        24
              Port        3(GigabitEthernet2/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.FFB7.A10D
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Altn BLK 4         128.1    P2p
Gi1/1            Altn BLK 4         128.2    P2p
Gi2/1            Root FWD 4         128.3    P2p

VLAN0100
  Spanning tree enabled protocol rstp
  Root ID     Priority    4196
              Address     00D0.FFB7.A10D
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4196  (priority 4096 sys-id-ext 100)
              Address     00D0.FFB7.A10D
              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         128.1    P2p
Gi1/1            Desg FWD 4         128.2    P2p
Gi2/1            Desg FWD 4         128.3    P2p
```

```
show spanning-tree detail
```

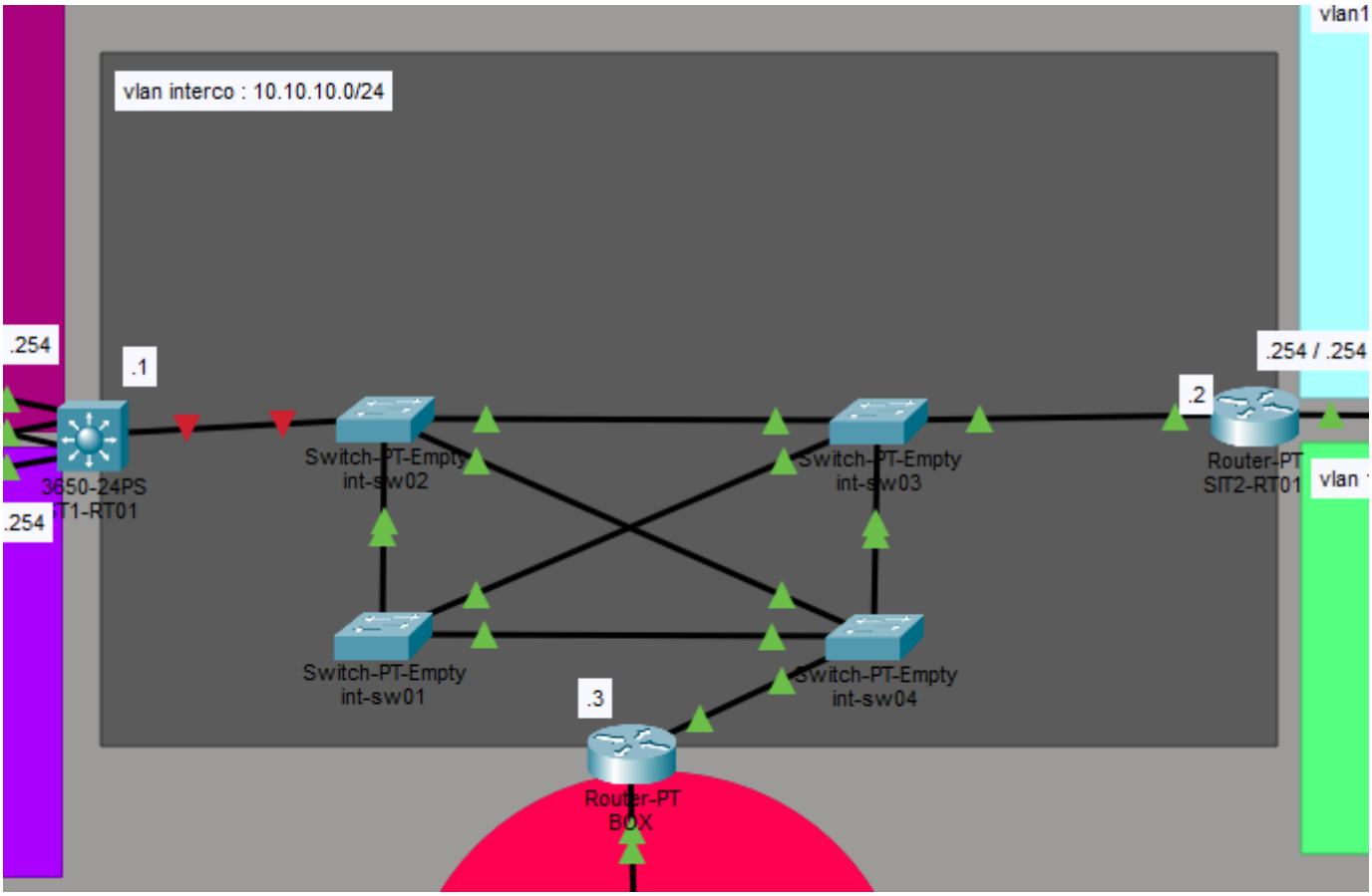
```
VLAN0100 is executing the rstp compatible Spanning Tree Protocol
  Bridge Identifier has priority of 4096, sysid 100, 00D0.FFB7.A10D
  Configured hello time 2, max age 20, forward delay 15
  We are the root of the spanning tree
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 00:00:00 ago
                  from FastEthernet0/1
  Times:  hold 1, topology change 35, notification 2
                      hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

Port 1 (GigabitEthernet0/1) of VLAN0100 is designated forwarding
  Port path cost 4, Port priority 128, Port Identifier 128.1
  Designated root has priority 4196, address 00D0.FFB7.A10D
  Designated bridge has priority 4196, address 00D0.FFB7.A10D
  Designated port id is 128.1, designated path cost 4
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point

Port 2 (GigabitEthernet1/1) of VLAN0100 is designated forwarding
  Port path cost 4, Port priority 128, Port Identifier 128.2
  Designated root has priority 4196, address 00D0.FFB7.A10D
  Designated bridge has priority 4196, address 00D0.FFB7.A10D
  Designated port id is 128.2, designated path cost 4
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point

Port 3 (GigabitEthernet2/1) of VLAN0100 is designated forwarding
  Port path cost 4, Port priority 128, Port Identifier 128.3
  Designated root has priority 4196, address 00D0.FFB7.A10D
  Designated bridge has priority 4196, address 00D0.FFB7.A10D
  Designated port id is 128.3, designated path cost 4
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point
```

Ainsi que plusieurs commandes supplémentaires.

```
inst-sw01#show spanning-tree ?
  active              Report on active interfaces only
  detail              Detailed information
  inconsistentports   Show inconsistent ports
  interface           Spanning Tree interface status and configuration
  summary             Summary of port states
  vlan                VLAN Switch Spanning Trees
  <cr>
```

4.3 Raccordement

Maintenant que tout est configuré, il est possible de raccorder l'interco meshée au reste de l'infra en remplacement du switch de base.



Comme visible sur ce schéma, le port qui relie le switch L3 s'est désactivé instantanément. En effet le BPDU guard a fait son travail.

Le switch L3 tel que configuré permet bien de faire le routage, mais le port qui le relie est en mode switch. Il est donc capable d'envoyer et d'interpréter les trames BPDU. Ce qui a activé la sécurité sur le switch int-sw02.

Pour remédier à ce problème, il faut tout d'abord reconfigurer le ST1-RT01 correctement.

Paramétrage ST1-RT01

```
# Passer en mode privilège
enable

# Passer en mode configuration
conf t

# Désactiver les interfaces de vlan.
vlan 1
no ip addr
exit
```

```
# Confugrer l'interface 1/0/24 en interface de routeur et non en port de switch.
int gi 1/0/24
no switchport
ip addr 10.10.10.1 255.255.255.0
exit

# Sortir du mode config et sauvegarder le fichier
exit
copy run start
```

Puis vérifier le status sur le switch int-sw02 et résactiver le port.

```
show interfaces status
```

```
int-sw02#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Gig0/1                       connected    trunk      a-full  a-100 10/100/1000BaseTX
Gig1/1                       connected    trunk      a-full  a-100 10/100/1000BaseTX
Gig2/1                       connected    trunk      a-full  a-100 10/100/1000BaseTX
Gig3/1                       err-disabled 100        auto    auto  10/100/1000BaseTX
```

Le port gi 3/1 est bien en mode "***err-disabled***"

Pour le réactiver, se mettre sur l'interface et la réinitialiser avec un '***shut / no shut***'.