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.

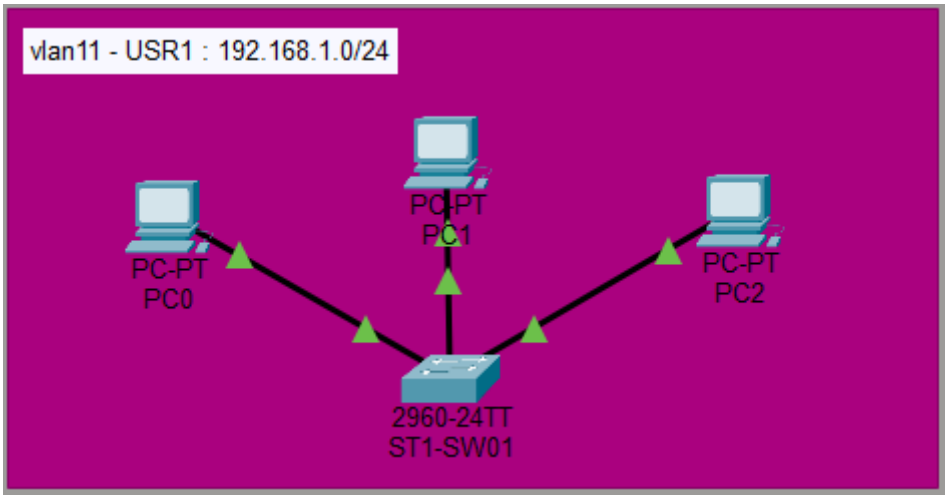
> **Conseil** : Au besoin, une version complétée du TP est disponible ci-joint.

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

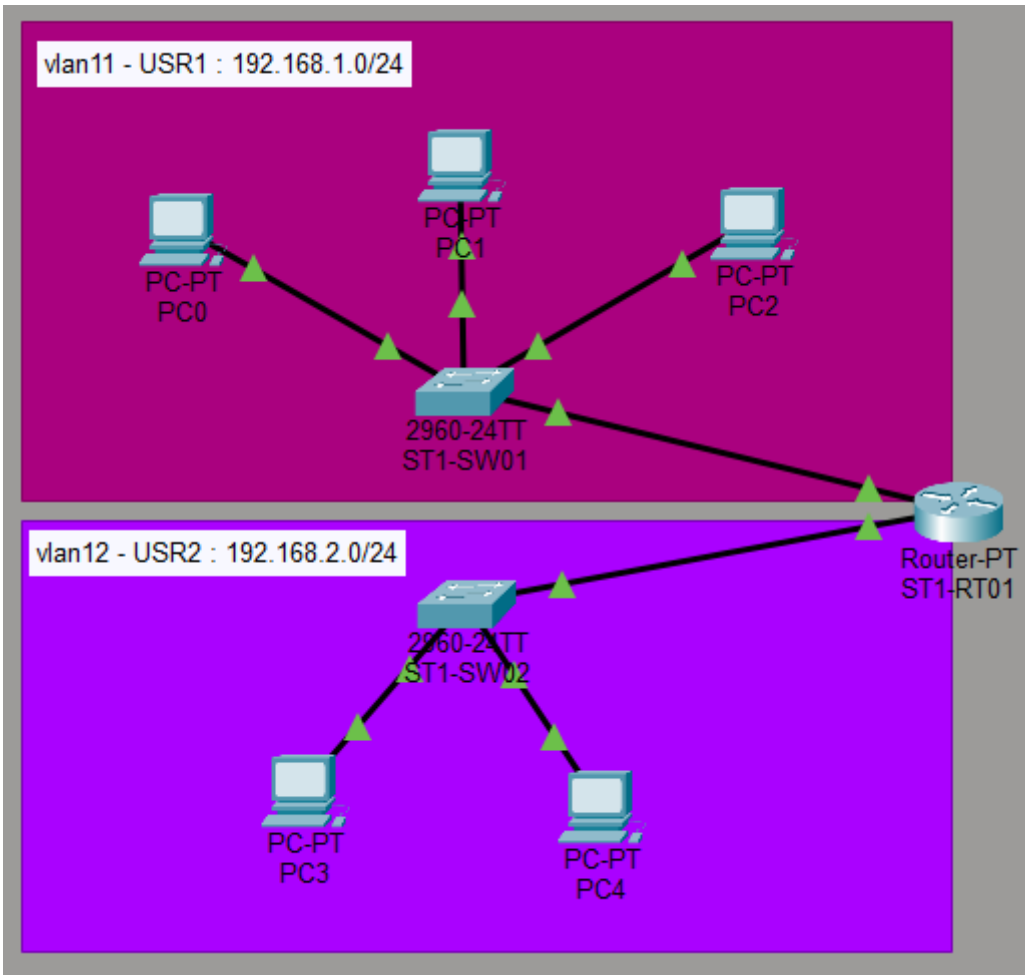
```
# Passer en mode privilège
enable

# 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 :

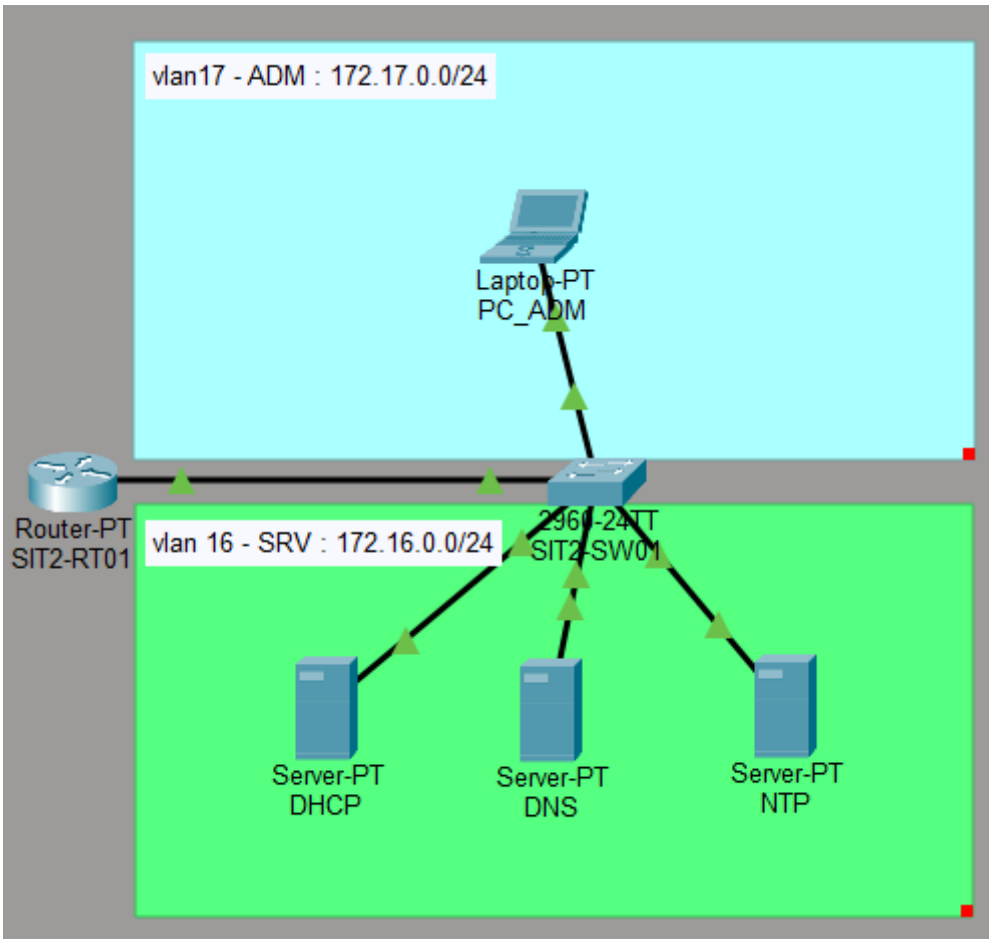
- **Tag Protocol Identifier (TPID)** : identifie qu'il s'agit d'une trame VLAN
- **Tag Control Information (TCI)**, qui inclut :

- **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.

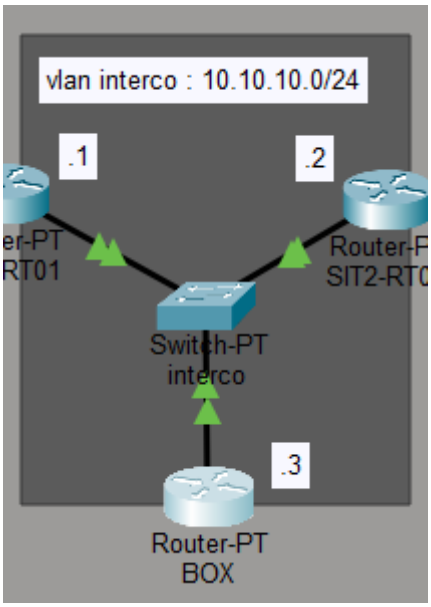
Ajouter un 'PT switch' qui servira de liaison interco. Pas besoin de configuration, il ne servira que pour les liaisons physiques.

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)

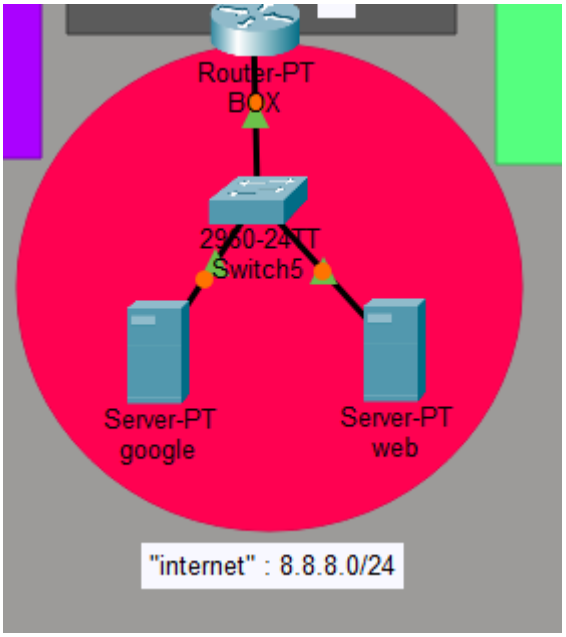
Le ***PAT***, parfois appelé **NAT surcharge (overload)**, est une extension du NAT permettant à plusieurs hôtes privés de partager une seule adresse IP publique.

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 :

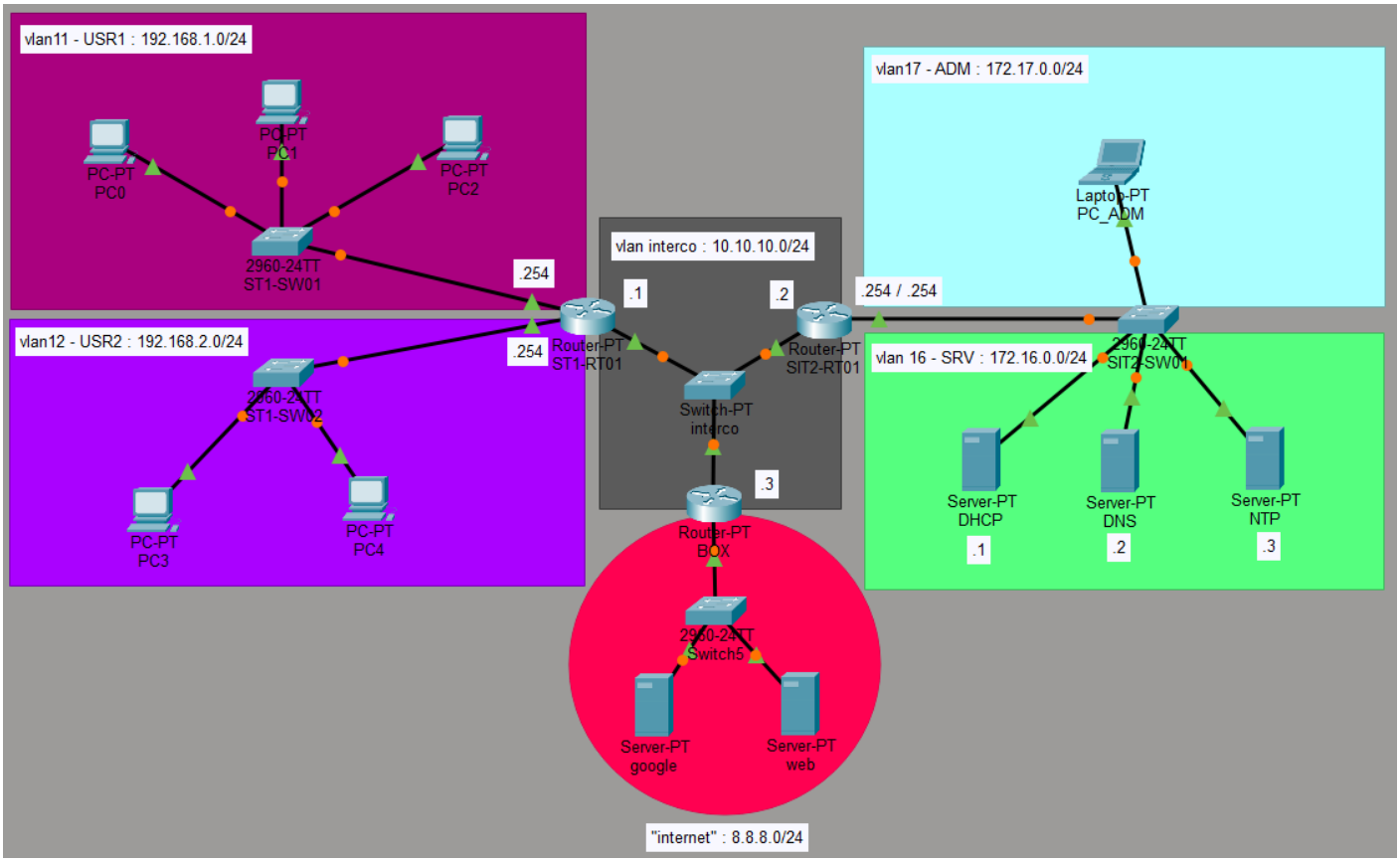
- Economie d'adresses publiques encore plus importante
- Fonctionne peut importe le nombre d'hôtes sortants
- Transparent pour les utilisateurs



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
```

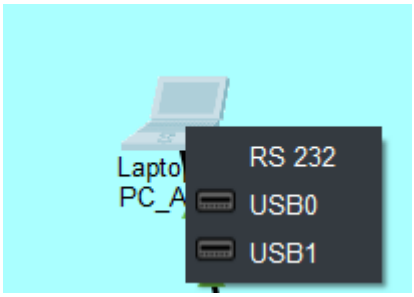
Pour augmenter le nombre d'adresses mémorisées par port, entrer en mode configuration de l'interface puis :

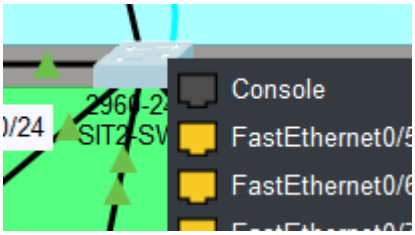
```
switchport port-security maximum <nbAdresseMax>
```

6.3 Activer l'authentification sur le port console

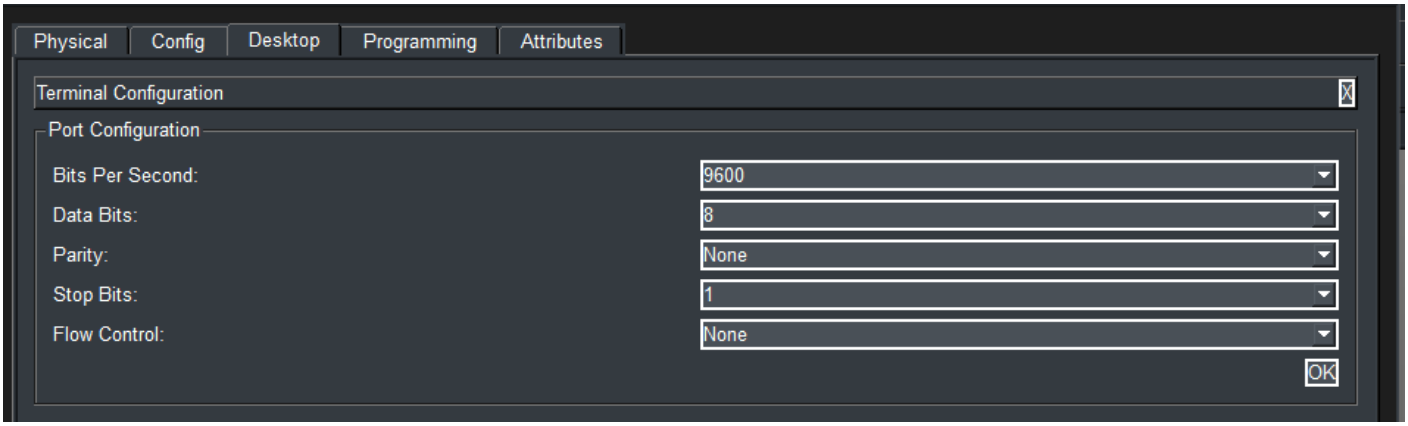
Si l'on tente une connexion en port console aux équipements :

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
```

Revision #2
Created 2026-07-17 22:20:37 UTC by Olivier
Updated 2026-07-17 22:24:28 UTC by Olivier