

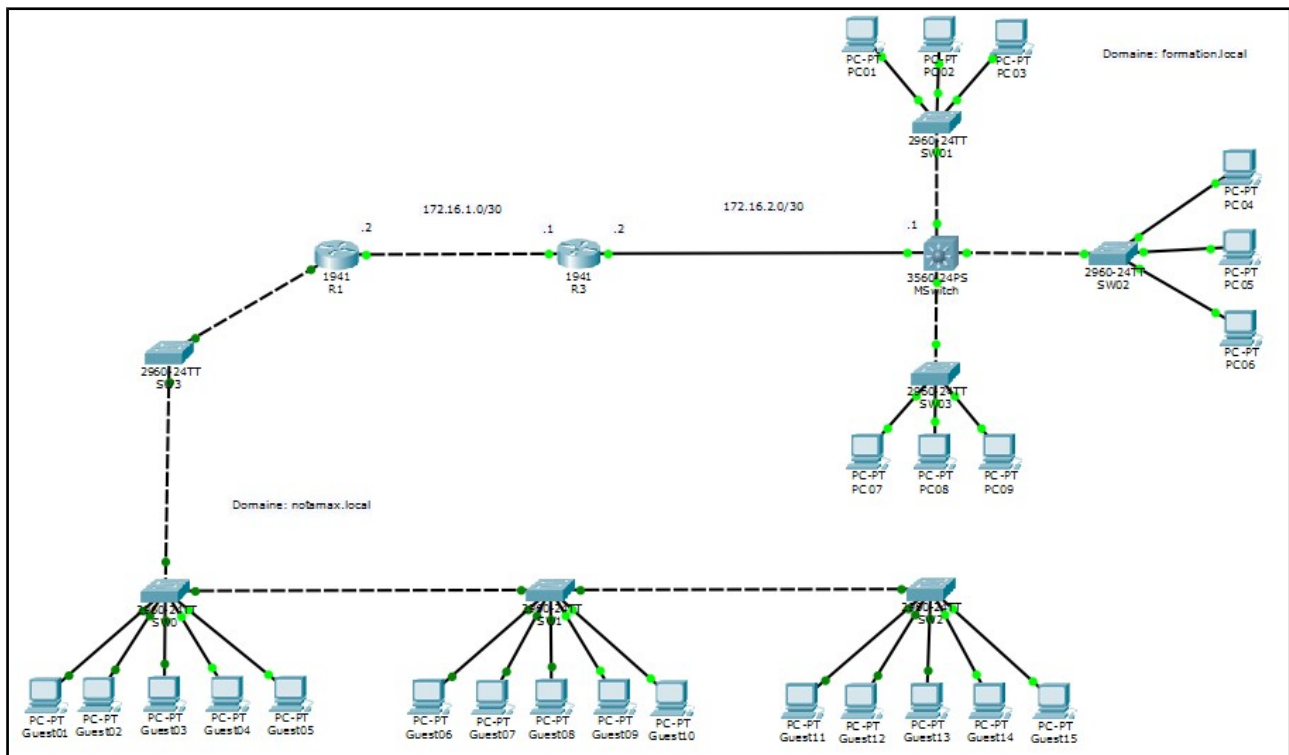
Labo de fin d'année sous Cisco Packet Tracer

Création d'un réseau informatique
cohérent et fonctionnel

Table des matières :

- 1) Présentation
- 2) Configuration pas à pas
- 3) Résumé des principes abordés
- 4) Conclusion

Schéma final:



1) Présentation

Nous allons prendre pour exemple une société fictive de notariat et de comptabilité, nous l'appellerons «Notamax». Elle contient deux LANs différents, chacun illustrant deux concepts de routage inter-vlan.

Spécifications propre à notre réseau LAN n°01 (notamax.local):

3 VLANs + un VLAN de Gestion et un Natif, à savoir:

- ✓ VLAN 10 (Compta, ports 1 à 8)
- ✓ VLAN 20 (Commercial, ports 9 à 16)
- ✓ VLAN 30 (Developpement, ports 17 à 24)
- ✓ VLAN 100 (Gestion)
- ✓ VLAN 99 (Natif)

- Connexion SSH sur chaque équipement, avec clé RSA de 1024bits et timeout d'inactivité de 120 secondes

- Protocole de routage RIPv2 sur chaque routeur

- Chaque VLAN aura 8 ports d'assignés par switch, ce qui est suffisant (possibilité de stacker les switchs dans le futur si besoin)

Concernant le plan d'adressages, le voici :

VLAN 10 -> Réseau comptabilité, 192.168.1.0/26

VLAN 20 -> Réseau commercial, 192.168.1.64/26

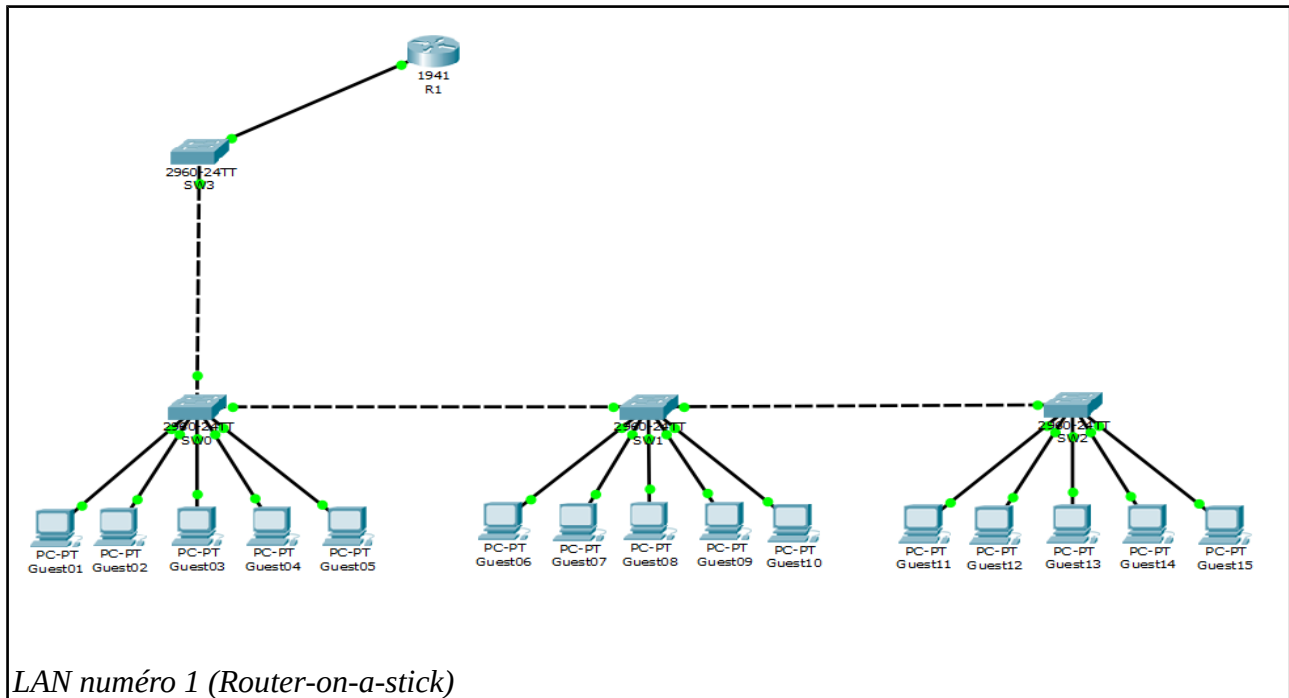
VLAN 30 -> Réseau développement, 192.168.1.128/26

VLAN 100 -> Réseau de gestion, 192.168.1.192/27

Le masque /26 a été choisi car il permet de créer jusqu'à 4 sous-réseaux chacun comptant 62 hôtes possibles (on enlève deux adresses, celle du réseau et celle de diffusion) ce qui convient parfaitement à notre topologie.

Pour le /27, il permet 30 hôtes, ce qui est suffisant pour gérer nos équipements à distance.

2) Configuration pas à pas



Notre réseau est composé de deux LANS, commençons donc par le premier. A noter que la configuration de base est la même pour chaque commutateur.

Switch 0-1-2 et R1:

```
hostname SW0 -1-2 ou R1
```

```
service password-encryption
```

```
enable password cisco
```

```
line console 0
```

```
password cisco
```

```
login
```

```
banner motd #Attention, personnes autorisees seulement ! Ceci est la propriete de Notamax. Des  
poursuites judiciaires peuvent etre encourues en cas d'utilisation non-autorisee de ces  
equipements.#
```

```
ip domain-name notamax.local
```

```
...
```

```
...
crypto key generate rsa
1024
line vty 0 15
transport input ssh
login local
ip ssh version 2
ip ssh time-out 120
username admin01 password cisco
```

Désormais, nos commutateurs et routeurs sont configurés et sécurisés. Il est temps de créer nos VLANs, et y assigner les ports désirés.

Switch 0-1-2:

```
vlan 10
name Compta
vlan 20
name Commercial
vlan 30
name Devs
vlan 100
name Gestion
interface range FastEthernet 0/1-8
switchport mode access
switchport access vlan 10
interface range FastEthernet 0/9-16
switchport mode access
switchport access vlan 20
interface range FastEthernet 0/17-24
switchport mode access
switchport access vlan 30
copy run start
```

Maintenant, nous allons créer le lien trunk sur chaque commutateur.

Switch 0:

```
interface GigabitEthernet0/2
switchport mode trunk
interface GigabitEthernet0/1
switchport mode trunk
```

Switch 1:

```
interface GigabitEthernet0/2
switchport mode trunk
interface GigabitEthernet0/1
switchport mode trunk
```

Switch 2:

```
interface GigabitEthernet0/1
switchport mode trunk
```

Bien, désormais il ne nous reste plus qu'à créer des sous-interfaces pour chaque VLAN sur le routeur R1

R1:

```
interface GigabitEthernet0/0
no shutdown
interface GigabitEthernet0/0.10
encapsulation dot1q 10
ip address 192.168.1.1 255.255.255.192
interface GigabitEthernet0/0.20
encapsulation dot1q 20
ip address 192.168.1.65 255.255.255.192
interface GigabitEthernet0/0.30
encapsulation dot1q 30
ip address 192.168.1.129 255.255.255.192
interface GigabitEthernet0/0.100
encapsulation dot1q 100
ip address 192.168.1.193 255.255.255.192
copy run start
```

A ce stade, nous pouvons presque faire du routage inter-vlan de type "Router on a Stick" via le routeur R1. Nous allons simplement attribuer une adresse IP et une passerelle à chaque station, et effectuer des pings dans le même vlan, puis dans des vlans différents.

Attention, il ne faut pas oublier de configurer une adresse IP sur chaque commutateur et routeurs pour pouvoir les administrer à distance (configurer une adresse ip sur l'interface du VLAN de gestion donc).

Les guests du VLAN 10:

Passerelle -> 192.168.1.1
Guest01 -> 192.168.1.2
Guest02 -> 192.168.1.3
Guest06 -> 192.168.1.4
Guest07 -> 192.168.1.5
Guest11 -> 192.168.1.6
Guest12 -> 192.168.1.7

Les guests du VLAN 20:

Passerelle -> 192.168.1.65
Guest03 -> 192.168.1.66
Guest08 -> 192.168.1.67
Guest13 -> 192.168.1.68

Les guests du VLAN 30:

Passerelle -> 192.168.1.129
Guest04 -> 192.168.1.130
Guest05 -> 192.168.1.131
Guest09 -> 192.168.1.132
Guest10 -> 192.168.1.133
Guest14 -> 192.168.1.134
Guest15 -> 192.168.1.135

SW0:

Passerelle -> 192.168.1.193
SW0 -> 192.168.1.194

SW1:

Passerelle -> 192.168.1.193

SW1 -> 192.168.1.195

SW2:

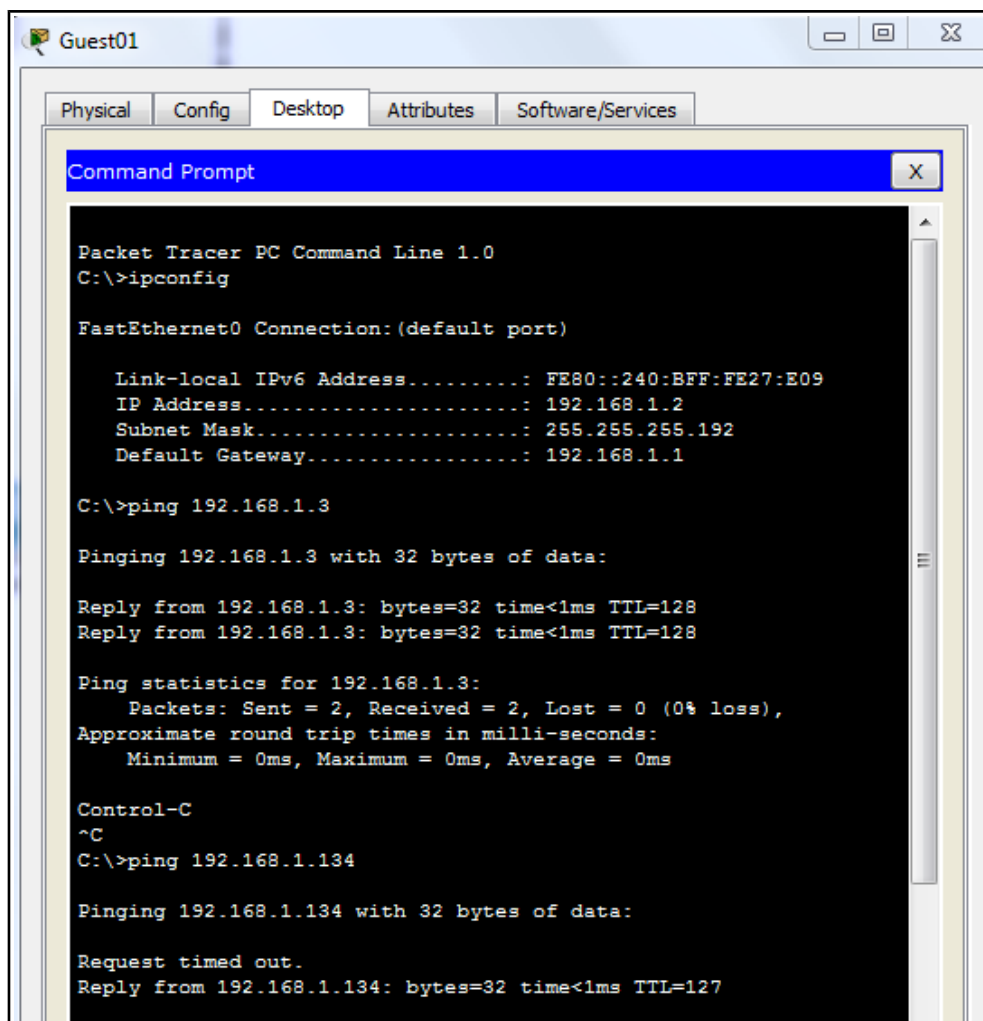
Passerelle -> 192.168.1.193

SW2 -> 192.168.1.196

SW3:

Passerelle -> 192.168.1.193

SW3 -> 192.168.1.197



```
Guest01
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Link-local IPv6 Address . . . . . : FE80::240:BFF:FE27:E09
    IP Address . . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.192
    Default Gateway . . . . . : 192.168.1.1

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>ping 192.168.1.134

Pinging 192.168.1.134 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.134: bytes=32 time<1ms TTL=127
```

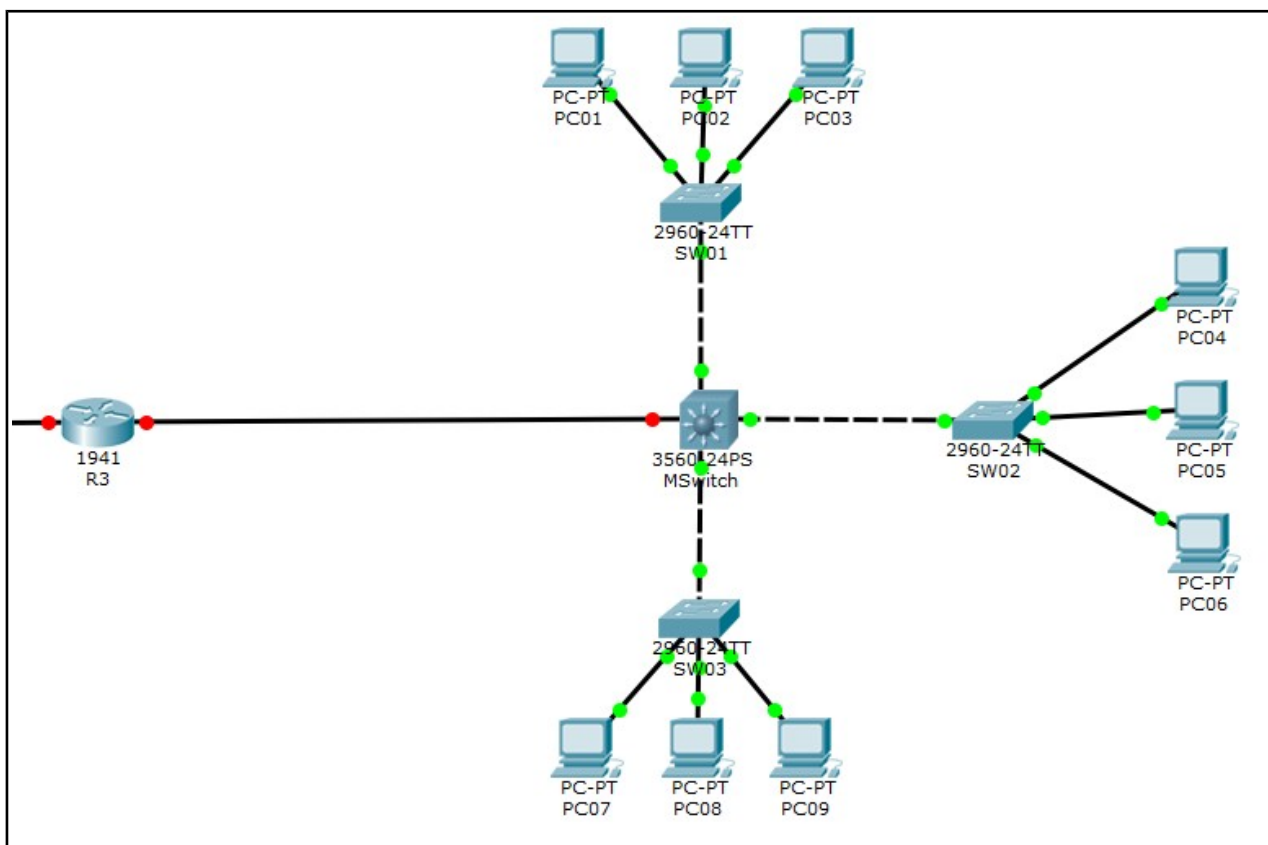
Comme montré sur la capture d'écran ci-dessus, Guest01 arrive bien à pinguer Guest02 (même VLAN), mais aussi à pinguer Guest14 (VLAN différent). A noter que le premier ping ne passe pas, cela est dû à la requête ARP pour récupérer la MAC Adress de Guest14.

Le LAN n°1 est donc fonctionnel, le routage inter-vlan de type « Router-on-a-stick » est bien mis en place.

Vient maintenant le LAN n°2 : même chose qu'avant, nous allons le configurer basiquement dans un premier temps puis créer d'autre vlans, d'autre trunks, et bien-sûr entamer la configuration du commutateur de couche 3 pour un nouveau mode de routage inter-vlan.

Ensuite, nous configurerons le protocole RIP sur le routeur R1 et R3.

(Pour les besoins du LAB, nous allons omettre certains passages vus précédemment : inutile de les recopier bêtement, seul les IP et noms d'hôtes sont susceptibles de changer, les commandes restent les même).



Dans ce LAN n°2 (formation.local), nous aurons donc :

2 VLANs + un VLAN de Gestion et un Natif, à savoir:

- ✓ VLAN 40 (Stagiaires, ports 1 à 18)
- ✓ VLAN 50 (Managers, ports 18 à 21)
- ✓ VLAN 200 (Gestion)
- ✓ VLAN 99 (Natif)

Concernant le plan d'adressages, le voici :

VLAN 40 -> Réseau stagiaires, 10.1.1.0/27

VLAN 50 -> Réseau managers, 10.1.1.32/27

VLAN 100 -> Réseau de gestion, 10.1.1.192/27

Le masque /27 a été choisi car il ne permet que 30 hôtes en un sous-réseau, ce qui convient parfaitement à notre topologie.

Nous allons donc commencer par la configuration basique des équipements, puis des VLANs, trunks, et SVI.

MSwitch:

- Créer un user que l'on va appeler admin02, avec comme mot de passe «cisco»
- Connecter les interfaces FastEthernet 0/22, 0/23, et 0/24 en mode trunk au différents commutateurs, comme suit:

Fa0/22 -> SW01

Fa0/23 -> SW02

Fa0/24 -> SW03

Attention, étant donné que c'est un commutateur de couche 3, il faudra utiliser la commande «switchport trunk encapsulation dot1q» avant de pouvoir passer l'interface en trunk.

- Créer un VLAN 40, Stagiaires
- Créer un VLAN 50, Managers
- Créer un VLAN 200, Gestion
- Créer un VLAN 99, Natif
- Assigner l'ip 10.1.1.1 à l'interface VLAN 40
- Assigner l'ip 10.1.1.33 à l'interface VLAN 50
- Assigner l'ip 10.1.1.194 à l'interface VLAN 200

SW01-02-03 :

- Créer un user que l'on va appeler admin02, avec comme mot de passe «cisco».
- Connecter l'interface FastEthernet 0/24 en mode trunk à MSwitch.
- Créer un VLAN 40, Stagiaires
- Créer un VLAN 50, Managers
- Créer un VLAN 200, Gestion
- Créer un VLAN 99, Natif
- Assigner l'ip 10.1.1.195 à l'interface VLAN 200 de SW01
- Assigner l'ip 10.1.1.196 à l'interface VLAN 200 de SW02
- Assigner l'ip 10.1.1.197 à l'interface VLAN 200 de SW03
- Attribuer les interfaces Fa0/1 à Fa0/20 au VLAN 40
- Attribuer les interfaces Fa0/21 à Fa0/23 au VLAN 50
- ip default-gateway 10.1.1.193
- switchport trunk native vlan 99 (*pour chaque interface sous trunk, on notifie le changement de VLAN natif*)

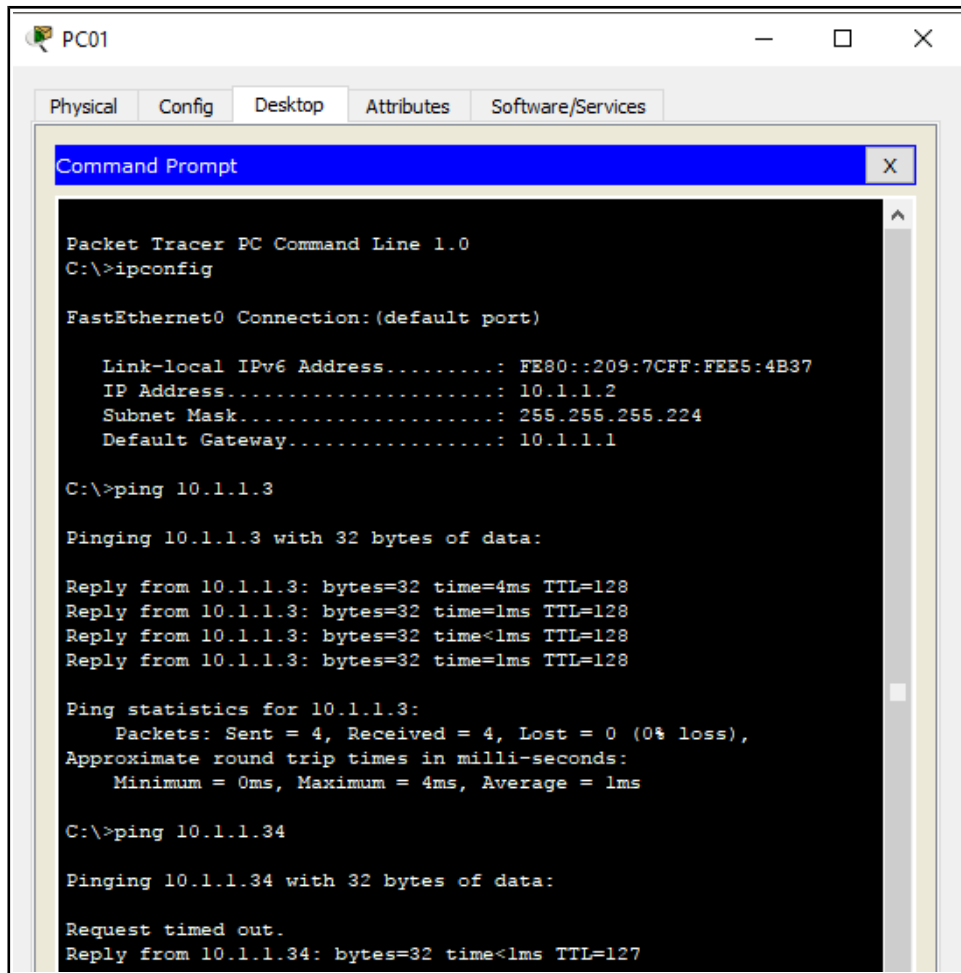
Les guests du VLAN 40:

Passerelle -> 10.1.1.1
PC01 -> 10.1.1.2
PC02 -> 10.1.1.3
PC04 -> 10.1.1.4
PC05 -> 10.1.1.5
PC07 -> 10.1.1.6
PC08 -> 10.1.1.7

Les guests du VLAN 50:

Passerelle -> 10.1.1.33
PC03 -> 10.1.1.34
PC06 -> 10.1.1.35
PC09 -> 10.1.1.36

Testons à présent la connectivité local...



```
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Link-local IPv6 Address . . . . . : FE80::209:7CFF:FEE5:4B37
    IP Address . . . . . : 10.1.1.2
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 10.1.1.1

C:\>ping 10.1.1.3

Pinging 10.1.1.3 with 32 bytes of data:

Reply from 10.1.1.3: bytes=32 time=4ms TTL=128
Reply from 10.1.1.3: bytes=32 time=1ms TTL=128
Reply from 10.1.1.3: bytes=32 time<1ms TTL=128
Reply from 10.1.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ping 10.1.1.34

Pinging 10.1.1.34 with 32 bytes of data:

Request timed out.
Reply from 10.1.1.34: bytes=32 time<1ms TTL=127
```

Comme montré sur la capture d'écran ci-dessus, PC01 arrive bien à pinguer PC02 (même VLAN), mais aussi à pinguer PC03 (VLAN différent). A noter que le premier ping ne passe pas : cela est dû à la requête ARP pour récupérer la MAC Adress de PC03.

Passons maintenant à la liaison du routeur R3 à MSwitch.

A noter que nous n'allons pas recopier ici la configuration de base des deux routeurs (ssh 1024 bits, création d'un utilisateur admin02 pour R3 et admin01 pour R3...) mais nous allons par contre détailler plus loin les commandes du protocole RIPv2.

MSwitch:

- interface GigabitEthernet 0/1
- no switchport (*pour passer l'interface en mode L3, comme une interface de routeur et non plus de simple commutateur*)
- ip address 172.16.2.1 255.255.255.252
- ip route 0.0.0.0 0.0.0.0 172.16.2.2 (*la commande ip route 0.0.0.0 0.0.0.0 est utilisée lorsque la commande ip-routing est précédemment activée, elle va 'servir' de default-gateway*)
- switchport trunk native vlan 99 (*pour chaque interface en mode trunk, on notifie le changement de VLAN natif*)

R3:

- Assigner l'ip 172.16.2.2 à l'interface GigabitEthernet 0/1
- ip route 10.1.1.0 255.255.255.0 172.16.2.1 (*ici, on indique au routeur que le réseau 10.1.1.0/24 est disponible via l'interface 172.16.2.1*)
- redistribute-static

Le LAN n°2 est à présent entièrement fonctionnel, le routage inter-vlan de type « Switch layer 3 » est bien mis en place, et les VLANs peuvent sortir du réseau via le routeur R3.

Vient donc ensuite le routage entre les deux LANs. Nous allons utiliser le protocole de routage RIPv2, car il est très simple d'utilisation, rapide à configurer, et idéal pour les réseaux de petites tailles comme le nôtre (pas besoin de déployer OSPF...).

R1:

- Assigner l'adresse ip 172.16.1.2/30 à l'interface GigabitEthernet 0/1
- router rip
- version 2
- network 172.16.1.0
- network 192.168.1.0

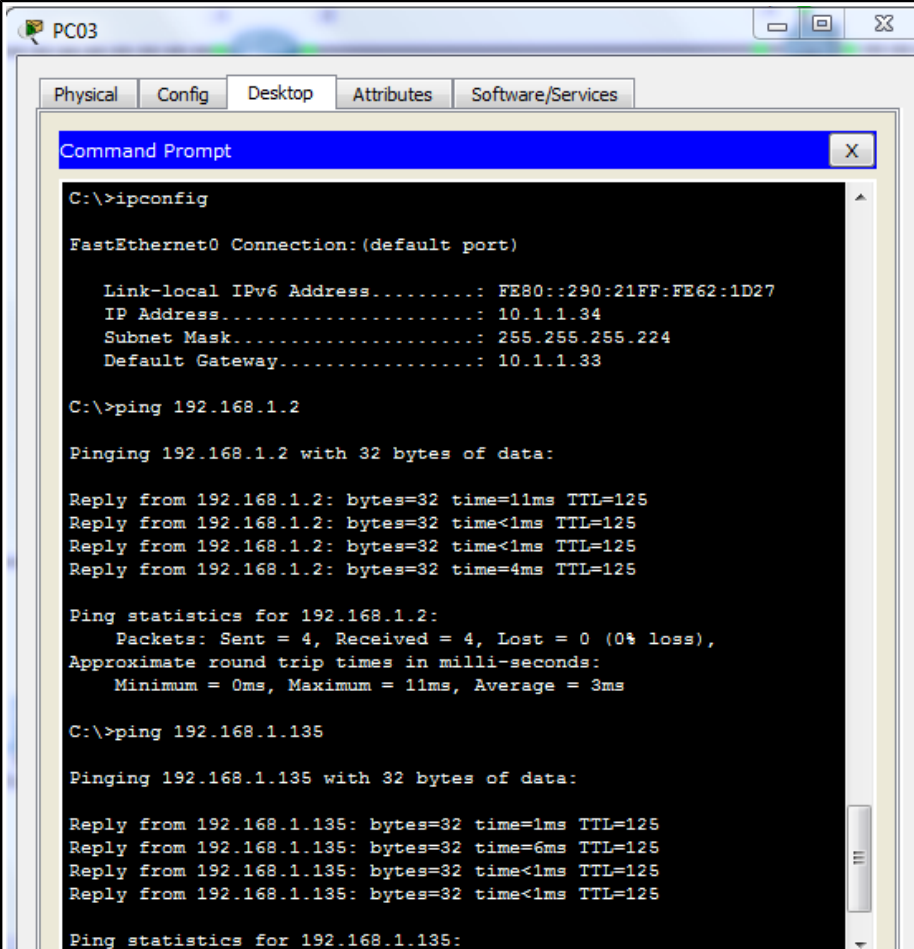
R3:

- Assigner l'adresse ip 172.16.1.1/30 à l'interface GigabitEthernet 0/0
- Assigner l'adresse ip 172.16.2.2/30 à l'interface GigabitEthernet 0/1
- router rip
- version 2
- network 172.16.1.0
- network 10.1.1.0
- redistribute static (*étant donnée que la liaison MSWitch et R3 est une route statique, nous devons activer cette commande pour que les autre routeurs -comme R1- prenne connaissance de cette route*)

Le masque /30 été choisi car il ne permet que 2 hôtes en un sous-réseau, ce qui convient parfaitement à notre utilisation : une adresse IP par interface, ni plus, ni moins.

Nous pouvons à présent tester la connectivité entre les deux LANs.

PC01 arrive bien à pinguer Guest01, et même Guest15 :



```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Link-local IPv6 Address . . . . . : FE80::290:21FF:FE62:1D27
    IP Address . . . . . : 10.1.1.34
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 10.1.1.33

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=11ms TTL=125
Reply from 192.168.1.2: bytes=32 time<1ms TTL=125
Reply from 192.168.1.2: bytes=32 time<1ms TTL=125
Reply from 192.168.1.2: bytes=32 time=4ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

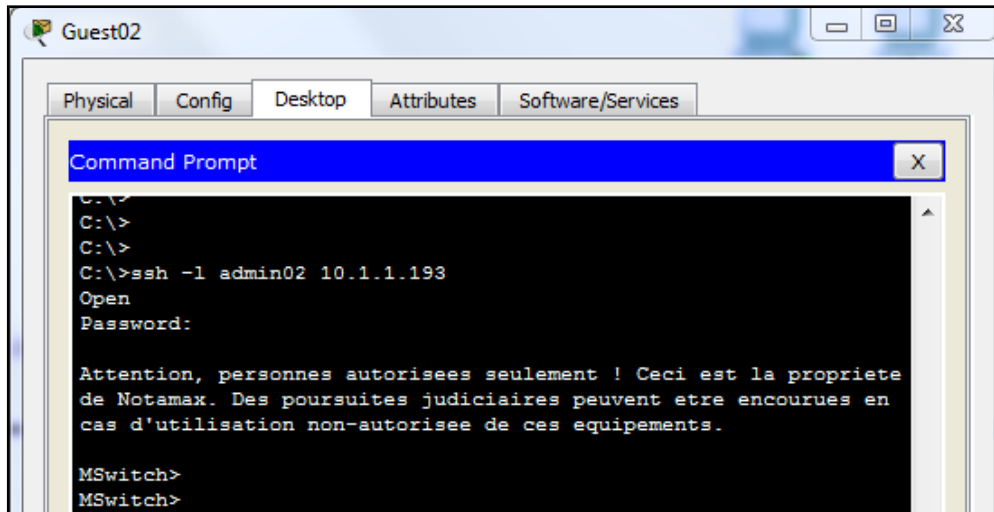
C:\>ping 192.168.1.135

Pinging 192.168.1.135 with 32 bytes of data:

Reply from 192.168.1.135: bytes=32 time=1ms TTL=125
Reply from 192.168.1.135: bytes=32 time=6ms TTL=125
Reply from 192.168.1.135: bytes=32 time<1ms TTL=125
Reply from 192.168.1.135: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.1.135:
```

Guest02 arrive bien à se connecter à distance sur MSwitch (VLAN de management):



Nous pouvons à présent essayer d'améliorer notre réseau en y ajoutant par exemple un **serveur DHCP pour chaque LAN**, de manière à ce que les VLANs (hormis celui de gestion) obtiennent des adresses IP de manière automatique.

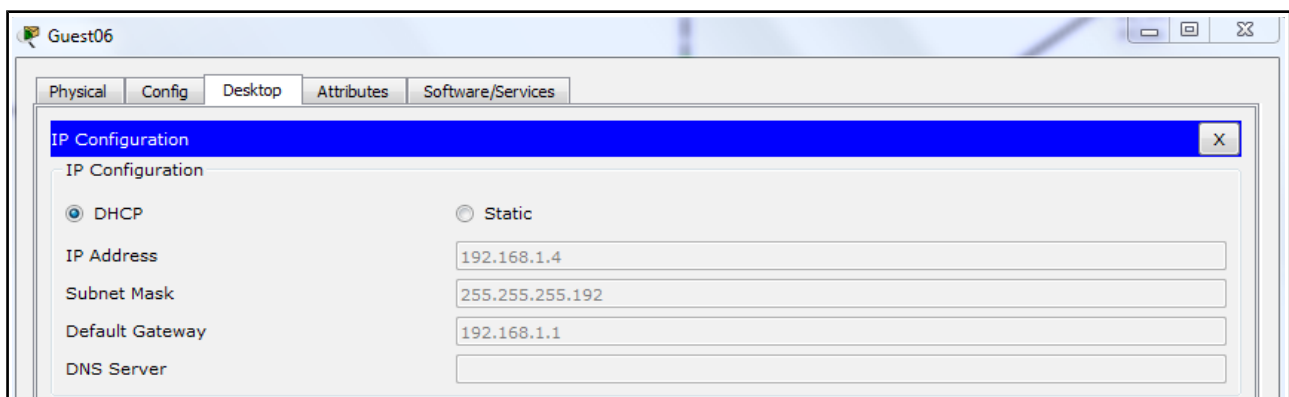
R1:

- ip dhcp pool vlan10
- network 192.168.1.0
- default-router 192.168.1.1
- ip dhcp pool vlan20
- network 192.168.1.64
- default-router 192.168.1.65
- ip dhcp pool vlan30
- network 192.168.1.128
- default-router 192.168.1.129
- ip dhcp excluded-address 192.168.1.1
- ip dhcp excluded-address 192.168.1.65
- ip dhcp excluded-address 192.168.1.129

MSwitch:

- ip dhcp pool vlan40
- network 10.1.1.0
- default-router 10.1.1.1
- ip dhcp pool vlan50
- network 10.1.1.32
- default-router 10.1.1.33
- ip dhcp excluded-address 10.1.1.1
- ip dhcp excluded-address 10.1.1.33

Ensuite, on reconfigure chaque périphérique pour passer la configuration IP en mode DHCP et non plus statique :



3) Résumé des principes abordés

- Protocole SSH : Création d'une clé SSH de 1024 bits, remplacement des lignes VTY par SSH au lieu de Telnet pour plus de sécurité. Implémentation d'un time-out.
- Technologie VLAN : Création de différents VLANs, création d'un VLAN natif pour plus de sécurité, création d'un VLAN de gestion pour l'administration à distance.
- Routage inter-vlan Router-on-a-Stick : Réalisation d'un routage inter-vlan via un routeur dédié. Création de sous-interfaces et de liaisons trunks.
- Routage inter-vlan Switch layer 3 : Approche et paramétrage d'un switch de couche 3, création de SVI pour chaque VLANs et routage interne.
- Protocole de routage RIPv2 : Implémentation du protocole de routage et redistribution de routes statiques.
- Serveur DHCP : Création de différents pools pour chaque VLANs, exclusions d'adresses IP appartenants aux gateways ou autre.

4) Conclusion

Par la réalisation de ce lab sous Packet Tracer, j'espère avoir su vous montrer que je maîtrise les concepts énoncés plus haut. Alors bien entendu, certains passages de configuration ou autre ont été raccourcis ou même ignorés : par exemple, j'aurais très bien pu créer des utilisateurs différents sur chaque équipement, et en dédier un bien spécifique pour l'administration locale et un autre pour l'administration distante, pour encore plus de sécurité.

Pour ce qui est des réseaux utilisés, j'aurais pu utiliser des masques plus grands ou plus petits pour encore mieux gérer mes adresses IP.

Bref, tout cela pour vous dire que ce labo avait avant tout pour but de vous prouver ma maîtrise pour ces concepts réseaux ainsi que, comme vous nous l'aviez demandé « vous épater avec des choses non vues en cours ». Il me servira aussi par ailleurs de notes de cours, ou pour d'autres projets futurs.

Fin.