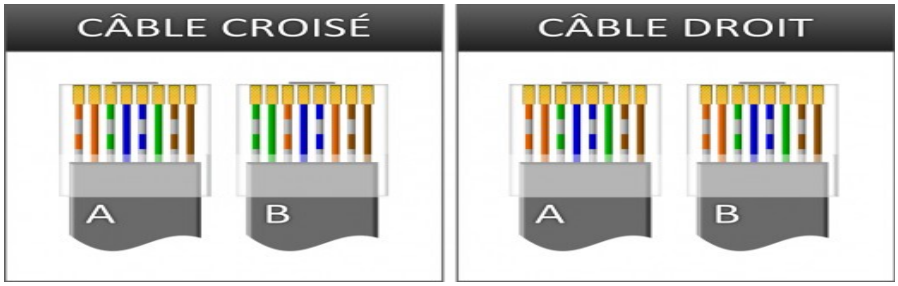
Rappel

I. Les différents câbles



CROISE

Switch	Routeur
Hub	PC

CROISE

DROIT

II. Liaison série

⇨ Comment voir lequel est DCE et DTE:

```
Router0# sh controllers s0/1/0
 Interface Serial0/1/0
 Hardware is PowerQUICC MPC860
 DCE V.35, clock rate 2000000
 idb at 0x81081AC4, driver data structure at 0x81084AC0
 SCC Registers:
 General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
Router1# sh controllers s0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
```

⇨ Et donc la CLOCK se met sur DCE (Router0)

⇨ Router0 (config-if) # clock rate 64000

Configuration de base

I. Configuration d'un routeur  Cisco

La première chose à faire par sécurité est de restaurer le routeur

```
Router # erase startup-config
Router # reload
```

Une fois restauré il faut configurer le nom du routeur :

```
Router (config) # hostname R1
```

Ensuite il faut configurer les différents mots de passe :

a. *Sécuriser l'accès au mode privilégié:*

```
Router (config) # enable secret PWD      => Le mot de passe est crypter
Router (config) # enable password PWD    => Le mot de passe n'est  pas crypter
```

b. *Sécuriser l'accès aux lignes Console*

```
Router (config) # line console 0
Router (config-line) # password VotreMotDePasse
Router (config-line) # exec-timeout minutes [secondes]
Router (config-line) # login
Router (config-line) # loggin synchronous
```

Je vous conseil de mettre 1 min pour exec-timeout, pour éviter qu'un connard vienne vous faire de la merde sur votre routeur quand vous partez.

⇨ loggin synchronous : permet d'éviter d'être interrompus par les mises à jour des interfaces.

c. *Sécuriser l'accès aux lignes VTY*

Ne pas mettre "cisco" comme mot de passe car facile à hacker sinon !

```
Router (config) # line vty ?
  <0-15>  First Line number
Router (config) # line vty 0 15
Router (config-line) # password VotreMotDePasse
Router (config-line) # exec-timeout minutes [secondes]
Router (config-line) # login
Router (config-line) # transport input telnet
Router (config-line) # logging synchronous
```

d. *Ajouter une sécurité supplémentaire en cryptant tous les mots de passe:*

```
Router (config) # service password-encryption
```

Commande de sauvegarde

```
Router # copy running-config startup-config
Router # wr
```

Autre commande utile

```
Router (config) # no ip domain-lookup  => évité d'attendre quand on se trompe de cmd
```

```
Router (config) # default int f0/0  => réinitialise l'interface
```

Configuration d'une interface

```
R1 # conf t
R1 (config) # int f0/0
R1 (config-if) # ip address 192.168.1.1 255.255.255.0
R1 (config-if) # no shut
```

⇨ IDEM pour interface séries mais ne pas oublier le **clock rate 64000** pour le côté **DCE**.

Enlever le mot de passe d'un routeur

1. Faire un power cycle (éteindre et rallumer le routeur physiquement)
2. Tout de suite après avoir rallumer le routeur appuyer sur **CTRL + BREAK**
3. Nous sommes maintenant passer en mode **ROMMON:**

```
monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

4. Ensuite taper les commandes suivantes dans ce mode:

```
rommon 1 > confreg 0x2141
rommon 2 > reset
```

⇨ On peut remarquer maintenant que le mot de passe à disparut:

```
Press RETURN to get started!

Router>
Router>
Router>en
Router#
```

5. Et maintenant on remet le routeur comme au départ sans le mot de passe:

```
Router#erase startup-config

Router(config)#config-register 0x2102
```

⇨ La 2eme commande permet de remettre le registre exactement comme avant.

III. Configuration d'un Switch Cisco

1. Comme pour les routeurs il faut restaurer le Switch

a. Supprimer le fichier VLAN.DAT

```
Switch # show flash:
    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
    5  -rw-         676          <no date>  vlan.dat

Switch # delete flash:vlan.dat
        Delete filename [vlan.dat]?  => ENTER
        Delete flash:/vlan.dat? [confirm]   => ENTER

Switch # show flash:

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.122-25.FX.bin
```

e. Ensuite restaurer le Switch comme un simple routeur

```
Switch # erase startup-config
Switch # reload
```

2. Configuration d'une IP sur un switch

```
R1 # conf t
R1 (config) # int vlan 1
R1 (config-if) # ip address 192.168.1.1 255.255.255.0
R1 (config-if) # no shut
R1 (config) # default gateway adresse masque
```

3. Configuration du VLAN de management

Le vlan de management est le VLAN qui vous nous servir pour superviser le Switch à distance (SSH ou Telnet). Le N° du VLAN nous sera communiquer à l'examen. Moi je vais prendre le VLAN 99 pour mon exemple.

a. Créer le VLAN de management

```
Switch (config) # vlan 99
Switch (config-vlan) # name MANAGEMENT
```

f. Configuration de l'IP du VLAN de management

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

L'IP dépend de votre réseau

g. Affecter les ports pour le VLAN 99 (il peut en avoir plusieurs)

```
Switch (config) # interface F0/1
Switch (config-if) # switchport access vlan 99
```

S

h. Définir la passerelle du Switch

A l'examen la passerelle sera normallement celle du routeur au dessus de votre Switch.

```
Switch (config) # ip default-gateway 172.17.99.1
```

```
Switch (config) # exit
```

i. Vérifier les informations pour le VLAN de management

```
Switch # sh interfaces vlan 99
Vlan99 is up, line protocol is up
  Hardware is CPU Interface, address is 0060.47ac.1eb8 (bia 0060.47ac.1eb8)
  Internet address is 172.17.99.11/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255

Switch #sh vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig1/1, Gig1/2
99   MANAGEMENT                       active    Fa0/1
1002 fddi-default                     act/unsup
```

j. Désactiver l'adresse IP du VLAN 1

```
Switch (config) # interface vlan 1
Switch (config-if) # no ip address
Switch (config-if) # shut

Switch # show ip int brief
Vlan1                  unassigned      YES manual administratively down down
```

4. Transférer le trafic d'un port à un autre

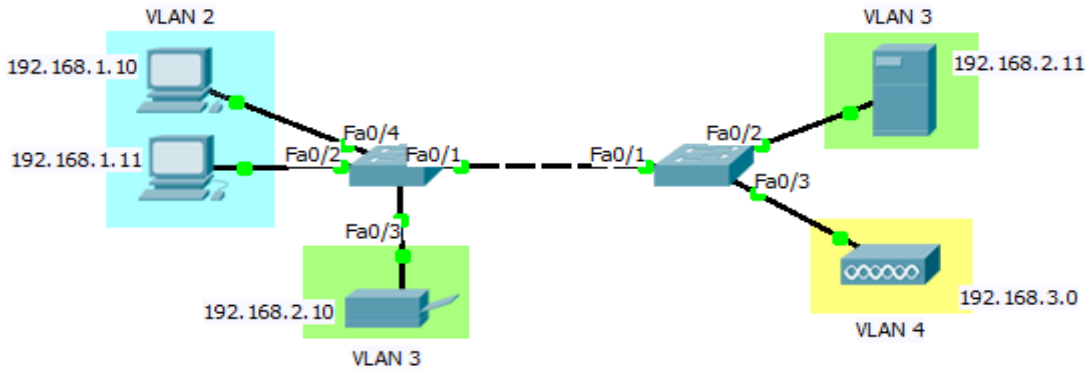
```
Spécifier le port source :
SW(config)# monitor session 1 source interface fa 0/1

Il est possible de spécifier un range de ports en source :
SW(config)# monitor session 1 source interface fa 0/1 – 5

Spécifier le port de destination :
SW(config)# monitor session 1 destination interface fa 0/10
```

Switching

I. Configuration de VLANS



Le but d'un VLAN est de permettre la configuration de réseaux différents sur un même Switch (chaque couleur représente un Vlan).

1. Création des VLANS

Une fois la configuration de base réalisé, on peut passer à la création des différents vlan et des différents techniques mise en œuvre. La création d'un vlan est identique à celui de la création du vlan de management.

a. Je m'occupe d'abord du Switch de gauche

```
Switch (config) # vlan 2
Switch (config-vlan) # name CAFETERIA
Switch (config-vlan) # exit
Switch (config) # vlan 3
Switch (config-vlan) # name SERVER
Switch (config-vlan) # exit

Switch (config) # do sh vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
 2   CAFETERIA                        active
 3   SERVER                           active
```

Ne pas oublier **l'EXIT** sinon les vlans ne sont pas pris en compte !!!

k. Je m'occupe ensuite du Switch de droite

```
Switch (config) # vlan 3
Switch (config-vlan) # name SERVER
Switch (config-vlan) # exit
Switch (config) # vlan 4
Switch (config-vlan) # name WIFI
Switch (config-vlan) # exit

Switch (config) # do sh vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
 3   SERVER                           active
 4   WIFI                             active
```

⇨ Pour supprimer un vlan : Switch (config) # no vlan 3

2. Affecté les VLANS aux différents ports correspondant

a. *Switch de gauche*

```
Switch (config) # int fa0/2
Switch (config-if) # switchport mode ?
  access   Set trunking mode to ACCESS unconditionally
  dynamic  Set trunking mode to dynamically negotiate access or trunk mode
  trunk    Set trunking mode to TRUNK unconditionally
Switch (config-if) # switchport mode access
Switch (config-if )# switchport access vlan 2
Switch (config-if )# exit

Switch (config) # int fa0/4
Switch (config-if) # switchport mode access
Switch (config-if )# switchport access vlan 2
Switch (config-if )# exit

Switch (config) # int fa0/3
Switch (config-if) # switchport mode access
Switch (config-if )# switchport access vlan 3
Switch (config-if )# exit

Switch #sh vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    CAFETERIA                        active    Fa0/2, Fa0/4
3    SERVER                           active    Fa0/3
```

I. Switch de droite

```
Switch (config) # int fa0/2
Switch (config-if) # switchport mode access
Switch (config-if )# switchport access vlan 3
Switch (config-if )# exit

Switch (config) # int fa0/3
Switch (config-if) # switchport mode access
Switch (config-if )# switchport access vlan 4
Switch (config-if )# exit

Switch #sh vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
 3    SERVER                           active    Fa0/2
 4    WIFI                             active    Fa0/3
```

⇨ On peut remarquer que maintenant un ping entre les 2 PCs du vlan 2 fonctionne mais un ping vers l'imprimante du vlan 3 ne fonctionne pas (donc c'est ok).

⇨ Par contre, un ping de l'imprimante vers le serveur ne fonctionne pas alors qu'ils sont dans le même vlan !!! il faut donc configuré le TRUNK de Switch à Switch.

3. Configuration du TRUNK

Le mode TRUNK permet de propager plusieurs vlans sur un même lien physique.

Dans le laboratoire il existe 2 types de Switch différent :

- 2960 : les Switchs du début dans le coffret (les bons switchs)
- 2950 : les gros Switchs tout à la fin du coffret

⇨ la configuration d'un TRUNK est différente sur les 2 Switch !!!

Dans mon exemple on va supposer que le Switch de gauche soit un 2960 et le Switch de droite un 2950

a. *Configuration du TRUNK sur le Switch de gauche (2960)*

```
Switch (config) # int F0/1
Switch (config-if) # switchport mode trunk
Switch (config-if) # switchport trunk allowed vlan none
Switch (config-if) # switchport trunk allowed vlan add 2
Switch (config-if) # switchport trunk allowed vlan add 3
```

m. *Configuration du TRUNK sur le Switch de droite (2950)*

```
Switch (config) # int F0/1
Switch (config-if) # switchport mode trunk
Switch (config-if) # switchport trunk encapsulation dot1q
Switch (config-if) # switchport trunk allowed vlan none
Switch (config-if) # switchport trunk allowed vlan add 3
Switch (config-if) # switchport trunk allowed vlan add 4
```

⇨ Et donc maintenant un ping de PC0 au serveur ne fonctionne toujours pas (pas le même vlan), mais par contre un ping de l'imprimante au serveur fonctionne sans problème.

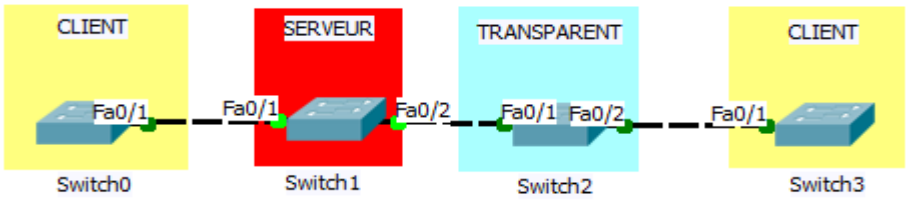
n. *Vérification*

```
Switch # sh running
interface FastEthernet0/1
 switchport trunk allowed vlan 2-3
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 2
 switchport mode access
```

⇨ Pour supprimer un vlan du TRUNK : swichport trunk allowed vlan remove 3

⇨ Pour supprimer le filtrage du TRUNK : no swichport trunk allowed vlan

IV. VTP (Vlan Transport Protocol)



⇨ Le protocole VTP permet la configuration automatique de vlans entre des serveurs VTP et des clients. Le Switch serveur est celui ou on crée les différents vlans qui seront propagé vers les différents clients.

1. Configurer tout les ports TRUNK

a. *Switch 0:*

```
Switch0 (config) # int F0/1
Switch0 (config-if) # switchport mode trunk
```

o. *Switch 1:*

```
Switch1 (config) # int F0/1
Switch1 (config-if) # switchport mode trunk
Switch1 (config) # int F0/2
Switch1 (config-if) # switchport mode trunk
```

p. *Switch 2:*

```
Switch2 (config) # int F0/1
Switch2 (config-if) # switchport mode trunk
Switch2 (config) # int F0/2
Switch2 (config-if) # switchport mode trunk
```

q. *Switch 3:*

```
Switch3 (config) # int F0/1
Switch3 (config-if) # switchport mode trunk
```

2. Configurer le serveur

```
Switch1 (config) # vtp mode server
        Device mode already VTP SERVER.
Switch1 (config) # vtp domain MonDomaine
        Changing VTP domain name from NULL to MonDomaine
Switch1 (config) # vtp password cisco
        Setting device VLAN database password to cisco
```

3. Configurer les clients

```
Switch0 (config) # vtp mode client
        Setting device to VTP CLIENT mode.
Switch0 (config) # vtp domain MonDomaine
        Changing VTP domain name from NULL to MonDomaine
Switch0 (config) # vtp password cisco
        Setting device VLAN database password to cisco
```

```
Switch3 (config) # vtp mode client
        Setting device to VTP CLIENT mode.
Switch3 (config) # vtp domain MonDomaine
        Changing VTP domain name from NULL to MonDomaine
Switch3 (config) # vtp password cisco
        Setting device VLAN database password to cisco
```

4. Configuration du transparent

```
Switch2 (config) # vtp mode transparent
        Setting device to VTP TRANSPARENT mode.
Switch2 (config) # vtp domain MonDomaine
        Changing VTP domain name from NULL to MonDomaine
Switch3 (config) # vtp password cisco
        Setting device VLAN database password to cisco
```

⇨ Sur le transparent on peu configurer des vlans. Le transparent va laisser passer les mises à jour de vlan donc lui ne prendra pas en compte les vlans que le serveur crée !!!

5. Créations de vlans sur le serveur

⇨ Il n'y encore aucun vlan créer, on va créer 2 vlans sur le serveur

```
Switch1 (config) # vlan 2
Switch1 (config-vlan) # name ECOLE
Switch1 (config-vlan) # exit
Switch1 (config) # vlan 3
Switch1 (config-vlan) # name BUREAUX
```

a. *Switch 0:*

```
Switch0 # sh vlan
                    2    ECOLE                          active
                    3    BUREAUX                        active
```

r. *Switch 1:*

```
Switch1 # sh vlan
                    2    ECOLE                          active
                    3    BUREAUX                        active
```

s. *Switch 2:*

```
Switch2 # sh vlan
```

⇨ Juste les vlans par défaut (donc n'a pas les vlans ECOLE et BUREAU)

t. *Switch 3:*

```
Switch3 # sh vlan
                    2    ECOLE                          active
                    3    BUREAUX                        active
```

Commande utile:

- Si on a plusieurs interfaces à configuré avec la même config il y a une commande qui permet de configuré toute ces interface en un coup :

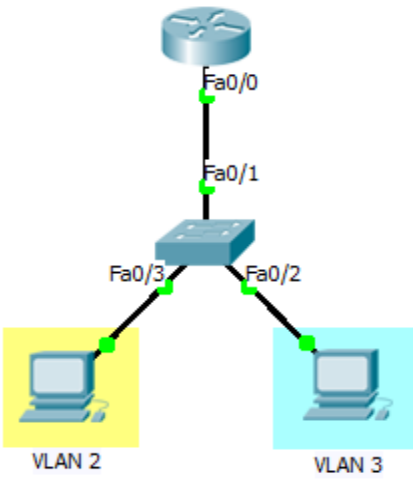
```
Switch (config) # int range f0/1-4, f0/7, F0/9-14
Swicth (config-if-range) # …
```

- Les commandes show

```
Switch # sh vtp status
Switch # sh vlan
Switch # sh interface vlan n°Vlan
```

V. Le routage Inter-Vlan

Comme on a peu le remarquer, faire un ping entre deux vlans différent ne fonctionne pas. Pour ce faire on est obligé d'utiliser un routeur qui permettra le routage entre les différents vlans.



1. Configuration du routeur

Il ne faut surtout pas mettre d'IP sur l'interface f0/0 !!! Voici les étapes pour configurer le routeur :

```
Router (config) # int F0/0
Router (config-if) # no shut

Router (config) # int f0/0.2
Router (config-subif) # encapsulation dot1Q 2
Router (config-subif) # ip address 192.168.1.1 255.255.255.0

Router (config) # int f0/0.3
Router (config-subif) # encapsulation dot1Q 3
Router (config-subif) # ip address 192.168.2.1 255.255.255.0

Router # sh ip int brief
 Interface              IP-Address      OK? Method Status                Protocol

 FastEthernet0/0        unassigned      YES unset  up                    up

 FastEthernet0/0.2      192.168.1.1     YES manual up                    up

 FastEthernet0/0.3      192.168.2.1     YES manual up                    up
```

Les numéros des sous-interfaces correspondent aux différents vlans.

2. Configuration du Switch

a. *Créations des différents vlans*

```
Switch (config) # vlan 2
Switch (config-vlan) # name VLAN2
Switch (config-vlan) # exit
Switch (config) # vlan 3
Switch (config-vlan) # name VLAN3
Switch (config-vlan) # exit
```

u. *Assignation des ports "access"*

```
Switch (config) # int F0/3
Switch (config-if) # switchport mode access
Switch (config-if) # switchport access vlan 2

Switch (config) # int F0/2
Switch (config-if) # switchport mode access
Switch (config-if) # switchport access vlan 2
```

v. *Configuration du TRUNK*

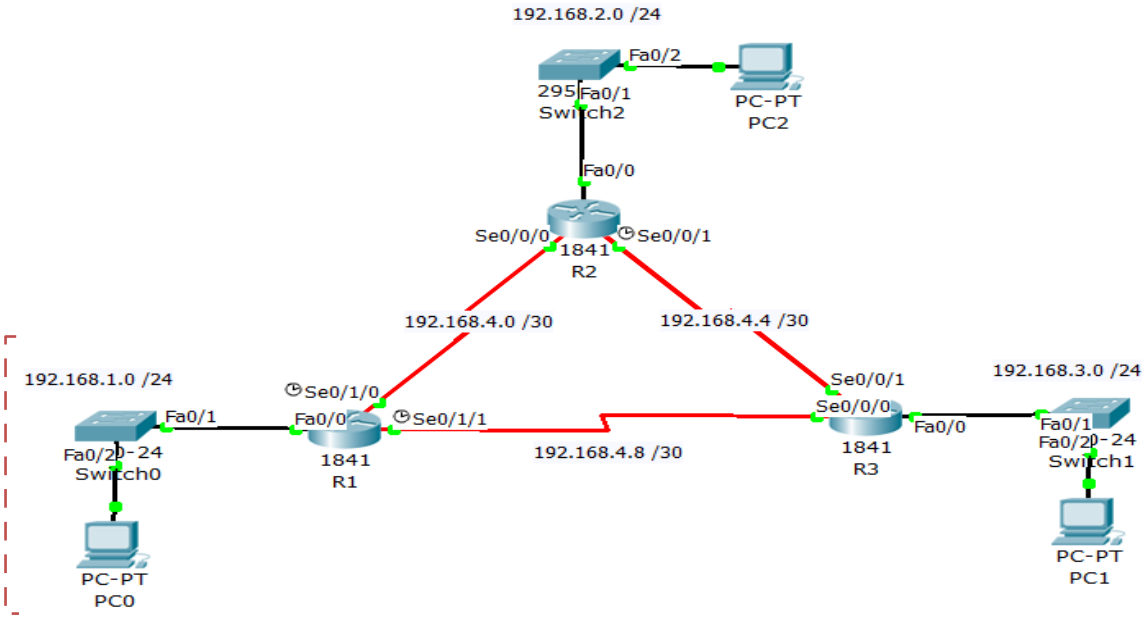
```
Switch(config)#int f0/1
Switch(config-if)#switchport mode trunk

Switch (config-if) # switchport trunk encapsulation dot1q => tout dépend du Switch

Switch(config-if)#switchport trunk allowed vlan none
Switch(config-if)#switchport trunk allowed vlan add 2
Switch(config-if)#switchport trunk allowed vlan add 3
```

⇨ Ensuite il ne reste plus qu'à mettre les IPs sur les PCs avec comme Gateway la sous-interface qui correspond au vlan. Et le ping entre vlan différent fonctionne parfaitement.

Routage : Statique



⇨ Aucun PCs ne sait se pinger car les routeurs ne connaissent pas les réseaux distants.

ROUTEURS	Ce que le routeur ne connaît pas
R1	Le réseau BLEU et ORANGE
R2	Le réseau ROUGE et ORANGE
R3	Le réseau ROUGE et BLEU

On va donc configuré les routes en statiques :

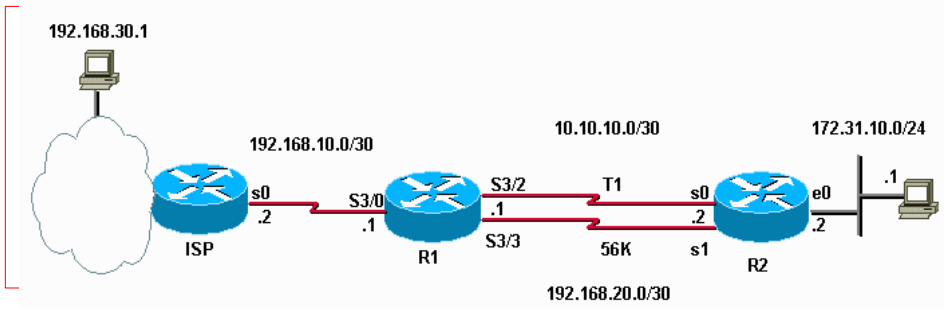
```
(config)# ip route ___ ___ ___ ___ ___ ___ ___ ___
                   Réseaux destination  MASK destination
```

Interface de sortie

Next-Hope (L'IP du prochain routeur)

Quand utiliser l'interface de sortie ou le Next-Hope :

Le Next-Hope sera utilisé dans la plupart des cas. Mais il faut utiliser l'interface de sortie dans un cas précis :



⇨ Sur R1 on mettra un route par défaut vers l'ISP (internet) et on précisera l'interface de sortie : **ip route 0.0.0.0 0.0.0.0 S3/0**

Revenons à la configuration de l'exemple :

a. *Sur R1:*

```
R1 (config) # ip route 192.168.2.0 255.255.255.0 192.168.4.2
R1 (config) # ip route 192.168.3.0 255.255.255.0 192.168.4.9
```

w. *Sur R2:*

```
R2 (config) # ip route 192.168.1.0 255.255.255.0 192.168.4.1
R2 (config) # ip route 192.168.3.0 255.255.255.0 192.168.4.6
```

x. *Sur R3:*

```
R3 (config) # ip route 192.168.1.0 255.255.255.0 192.168.4.10
R3 (config) # ip route 192.168.2.0 255.255.255.0 192.168.4.5
```

Comment supprimer une route statique :

```
R1 (config) # no ip route 192.168.2.0 255.255.255.0
```

Commande show:

```
R1 # sh ip route
```

Route de backup :

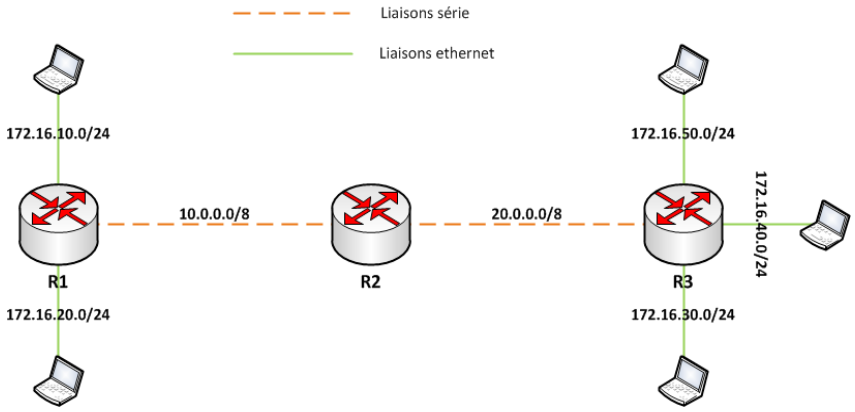
```
R1 (config) # ip route 192.168.2.0 255.255.255.0 192.168.4.2 metric
```

Routage : RIP

1. Le problème de RIPv1:

RIPv1 ne prend pas en charge le masque de sous-réseau dans les mises à jour de la table de routage.

Avec RIPv1, lorsque R1 et R3 enverront leur table de routage à R2, l'information fournie par les deux routeurs sera 172.16.0.0. RIPv1 fonctionnant avec le système de classe réseau et ne prenant pas en charge les masques de sous-réseaux. Celui-ci va voir 5 adresses réseaux identiques.



La solution au problème consiste à configurer le protocole de routage en version 2, qui prend en charge les masques de sous-réseaux.

2. Configuration du protocole RIP (schéma page 14)

a. Sur R1:

```
R1 (config) # router rip
R1 (config-router) # version 2
R1 (config-router) # network 192.168.1.0
R1 (config-router) # network 192.168.4.0
R1 (config-router) # passive-interface f0/0
R1 (config-router) # no auto-summary
```

y. Sur R2:

```
R2 (config) # router rip
R2 (config-router) # version 2
R2 (config-router) # network 192.168.2.0
R2 (config-router) # network 192.168.4.0
R2 (config-router) # passive-interface f0/0
R2 (config-router) # no auto-summary
```

z. Sur R3:

```
R3 (config) # router rip
R3 (config-router) # version 2
R3 (config-router) # network 192.168.3.0
R3 (config-router) # network 192.168.4.0
R3 (config-router) # passive-interface f0/0
R2 (config-router) # no auto-summary
```

⇨ passive-interface f0/0 : permet de ne pas envoyer les mises à jour vers les LANs

⇨ no auto-summary : Désactive le résumé automatique des routes dans les tables de routages.

3. Supprimer le protocole de routage RIP:

```
R1 (config) # no router rip
```

4. Commande de Debug:

```
R1 # show ip protocols
R1 # show ip route
R1 # debug ip rip
```

5. Comment redistribuer une route par défaut :

```
R1 (config-router) # default-information originate
```

6. Comment redistribuer une route statique

```
R1 (config-router) # redistribute static
```

7. Summarization

```
R2 (config) # router rip
R2 (config-router) # no auto-summary
R2 (config-router) # auto-summary
```

Routage : EIGRP

1. Configuration du protocole EIGRP (schéma page 14)

a. Sur R1:

```
R1 (config) # router eigrp 1
R1 (config-router) # network 192.168.1.0     0.0.0.255
R1 (config-router) # network 192.168.4.0     0.0.0.3
R1 (config-router) # network 192.168.4.8     0.0.0.3
R1 (config-router) # passive-interface f0/0
R1 (config) # no auto-summary
```

N° du système autonome

Pour trouver le widcard mask :
255.255.255.255 - 255.255.255.0
= 0.0.0.255

aa. Sur R2:

```
R2 (config) # router eigrp 1
R2 (config-router) # network 192.168.1.0 0.0.0.255
R2 (config-router) # network 192.168.4.4 0.0.0.3
R2 (config-router) # network 192.168.4.0 0.0.0.3
R2 (config-router) # passive-interface f0/0
R2 (config) # no auto-summary
```

bb. Sur R3:

```
R3 (config) # router eigrp 1
R3 (config-router) # network 192.168.1.0 0.0.0.255
R3 (config-router) # network 192.168.4.8 0.0.0.3
R3 (config-router) # network 192.168.4.4 0.0.0.3
R3 (config-router) # passive-interface f0/0
R3 (config) # no auto-summary
```

2. Comment modifier le métrique d'EIGRP

Il faut se rendre sur une interface et modifier la bande passante ou le delay:

```
R1 (config-if) # bandwidth 1500000 (kbs)
R1 (config-if) # delay 1200 (10µsec)
```

Ne modifie pas la bande passante physique de la liaison

⇨ METRIC = 256 * (int) (BP + DELAY)

3. Commande de Debug:

```
R1 # show ip eigrp neighbors          => afficher les voisins
R1 # show ip eigrp topology           => affiche la table de la topologie
R1 # show ip eigrp interfaces         => afficher les interface EIGRP activé
R1 # show ip route                    => afficher la table de routage
```

4. Comment redistribuer une route statique ou une route par défaut :

```
R3 (config-router) # redistribute static
```

5. SUCCESSOR et FEASIBLE SUCCESSOR

a. *SUCCESSOR:*

C'est la route désignée comme la meilleure (la métrique la plus basse) pour aller d'un routeur A à un routeur B.

cc. FEASIBLE SUCCESSOR

C'est une route de BACK UP qui est considéré comme la seconde meilleure route dans une topologie (sans boucle de routage).

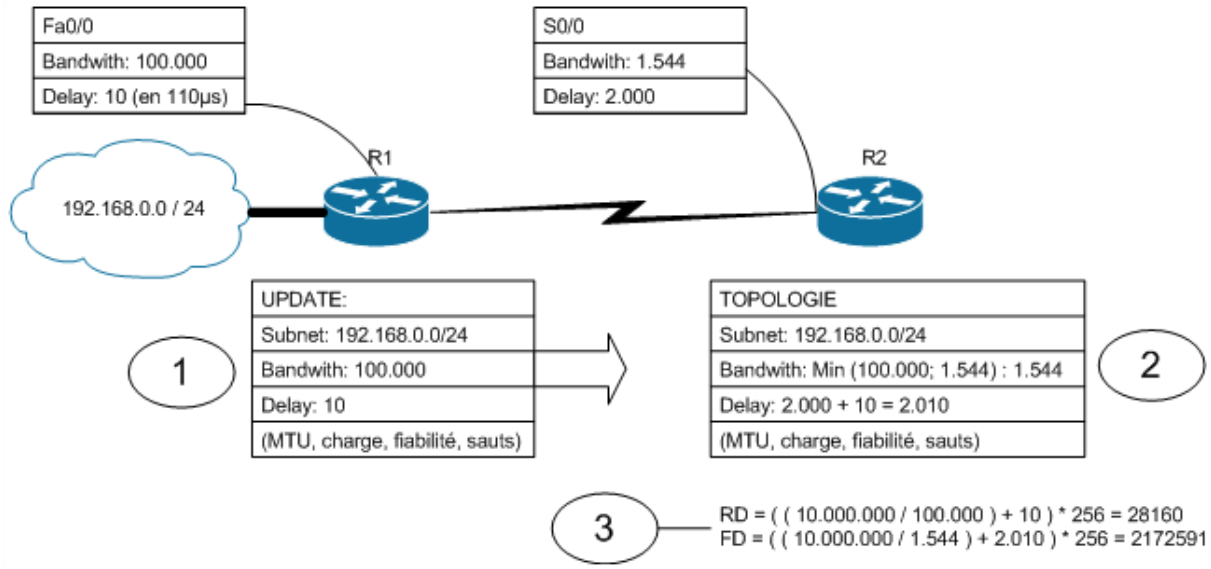
Comment déterminer une FEASIBLE SUCCESSOR :

Il faut que la RD (Reported Distance) soit plus petite que la FD (Feasible Distance) du SUCCESSOR.

La FD est la métrique pour un subnet du point de vue du routeur lui-même, utilisée pour choisir la meilleure route vers ce subnet.

La RD est la métrique pour un subnet du point de vue du routeur voisin (La métrique annoncée par le routeur voisin).

Voici comment faire pour calculer RD et FD :



Routage : OSPF

1. Configuration du protocole OSPF (schéma page 14)

a. Sur R1

```
R1 (config) # router ospf 1
R1 (config-router) # network 192.168.1.0 0.0.0.255 area 1
R1 (config-router) # network 192.168.4.0 0.0.0.3 area 1
R1 (config-router) # network 192.168.4.8 0.0.0.3 area 1
R1 (config-router) # passive-interface f0/0
```

dd. Sur R2:

```
R2 (config) # router ospf 1
R2 (config-router) # network 192.168.1.0 0.0.0.255 area 1
R2 (config-router) # network 192.168.4.0 0.0.0.3 area 1
R2 (config-router) # network 192.168.4.8 0.0.0.3 area 1
R2 (config-router) # passive-interface f0/0
```

ee. Sur R3:

```
R3 (config) # router ospf 1
R3 (config-router) # network 192.168.1.0 0.0.0.255 area 1
R3 (config-router) # network 192.168.4.0 0.0.0.3 area 1
R3 (config-router) # network 192.168.4.8 0.0.0.3 area 1
R3 (config-router) # passive-interface f0/0
```

2. Commande de Debug

```
R1 # show ip ospf neighbors [detail]
R1 # show ip ospf interface
R1 # show ip ospf database
R1 # clear ip ospf process (relancer le mécanisme d'élection)
```

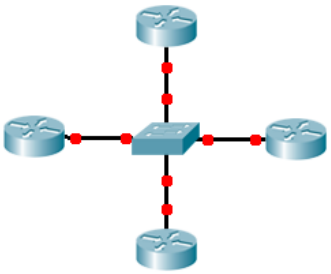
3. Redistribuer une route par défaut

```
R1 (config-router) # default-informations originate
```

4. Redistribuer une route statique

```
R1 (config-router) # redistribute static
```

5. DR & BDR (dans le cas de réseaux Multi Access)



DR : Designate Routeur

BDR : Backup Designate Routeur

⇨ Plus la priorité est haute plus on a des chances d'être élu DR (entre 0 et 255).

Commande pour modifier la priorité :

```
Router (config-if) # ip ospf priority [de 0 à 255]
```

⇨ C'est bien sur l'interface qu'il faut faire la commande

L'élection est permanente, tant qu'il y a une DR qui est élu il reste élu tant qu'il est UP !!! Pour refaire une sélection il faut :

- reboot
- clear ip ospf process

VI. ACL

1) ACL standard 1->99

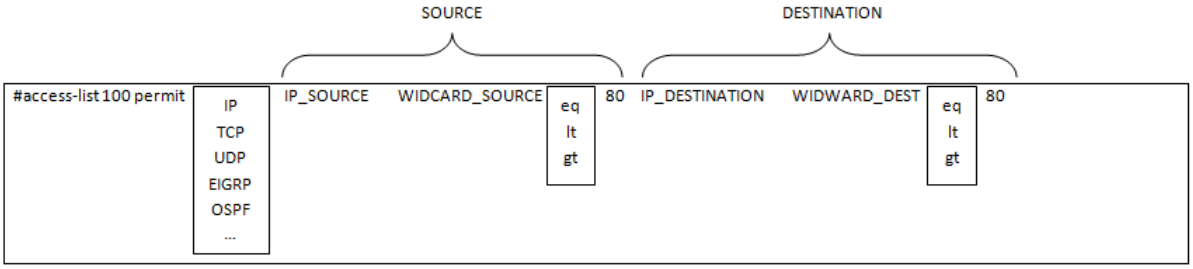
a. *Création de l'ACL*

```
Router(config)#access-list 1 permit 192.168.1.1 0.0.0.0
Router(config)#access-list 1 deny 192.168.1.11 0.0.0.0
```

ff. *Appliquer l'ACL sur l'interface*

```
Router(config-if)#ip access-group 1 [in ou out]
```

1) ACL etendue 100->199



- eq : égale le N°port
- lt : plus petite que le N° port
- gt : plus grand que le N° port

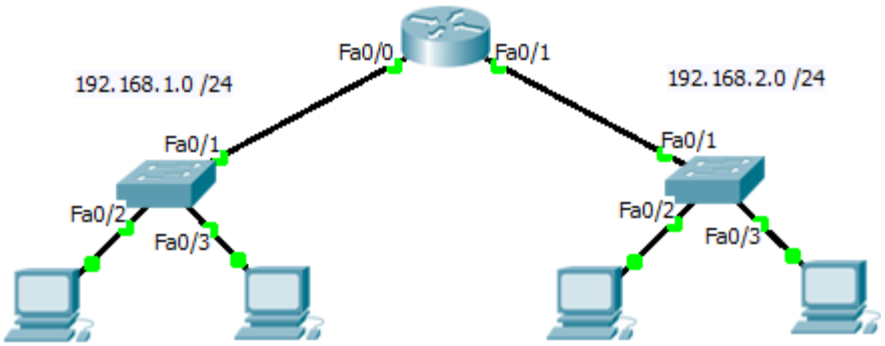
a. *Création de l'ACL*

```
Router(config)# access-list 100 permit tcp 192.168.1.1 0.0.0.0 eq pop3
Router(config)# access-list 100 permit ip any any
```

gg. *Appliquer l'ACL sur l'interface*

```
Router(config-if)#ip access-group 1 [in ou out]
```

VII. DHCP



Je vais configurer le routeur pour qu'il puisse fournir des adresses IP pour chaque PC des deux LANS différents.

a. Configuration du premier POOL (celui du LAN de gauche)

```
Router(config)#ip dhcp pool R1Fa0
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
```

hh. Configuration du deuxième POOL (celui du LAN de droite)

```
Router(config)#ip dhcp pool R1Fa1
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
```

⇨ default-router 192.168.2.1 permet d'enlever du POOL l'adresse de la Gateway.

Il est possible de fournir l'adresse d'un serveur DNS : dns-server 192.168.23.2

Et on peut aussi exclure des adresses du pool grâce à la commande suivante :

```
Router(config)# ip dhcp excluded-address (de) 192.168.1.1 (à) 192.168.1.10
```

VIII. NAT

1) NAT dynamique

a. ETAPE 1 : configuration d'un POOL d'IP publique

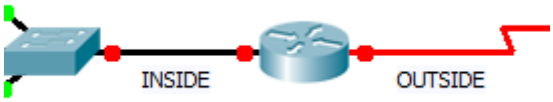
```
Router(config)#ip nat pool POOL_NAME    80.0.0.1      80.0.0.4 netmask 255.255.255.0
```

RANGE d'adresse IP Publique

ii. ETAPE 2: Il faut déterminer qui va subir le NAT (donc une ACL)

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

jj. ETAPE 3 : Les interfaces concernées




```
Router(config)#int F0/0
Router(config-if)#ip nat inside

Router(config)#int S0/0/0
Router(config-if)#ip nat ouside
```

kk. ETAPE 4: Activation du NAT

```
Router(config)# ip nat inside source list 1 pool POOL_NAME
```

- ⇨ Commande show: sh ip nat translation
- ⇨ Commande clear: clear ip nat translation *

2) PAT dynamique

CAS N°1 : Je possède une IP publique FIXE:

a. ETAPE 1 : configuration d'un POOL d'IP publique

```
Router(config)#ip nat pool POOL_NAME    80.0.0.1    80.0.0.1 netmask 255.255.255.0
```

ll. ETAPE 2: Il faut déterminer qui va subir le NAT (donc une ACL)

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

mm. ETAPE 3 : Les interfaces concernées

```
Router(config)#int F0/0
Router(config-if)#ip nat inside

Router(config)#int S0/0/0
Router(config-if)#ip nat ouside
```

nn. ETAPE 4: Activation du NAT

```
Router(config)# ip nat inside source list 1 pool POOL_NAME overload
```

CAS N°2 : je possède un IP publique dynamique

a. *ETAPE 1: Il faut déterminer qui va subir le NAT (donc une ACL)*

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

oo. *ETAPE 2 : Les interfaces concernées*

```
Router(config)#int F0/0
Router(config-if)#ip nat inside

Router(config)#int S0/0/0
Router(config-if)#ip nat ouside
```

pp. *ETAPE 3: Activation du NAT*

```
Router(config)# ip nat inside source list 1 interface S0/0/0 overload
```

3) NAT statique

a. *ETAPE 1 : Les interfaces concernées*

```
Router(config)#int F0/0
Router(config-if)#ip nat inside (côté LAN)

Router(config)#int S0/0/0
Router(config-if)#ip nat ouside (côté WAN)
```

qq. *ETAPE 2: Activation du NAT*

```
Router(config)# ip nat inside source static 192.168.2.1 80.0.0.3
```

4) PAT statique

b. *ETAPE 1 : Les interfaces concernées*

```
Router(config)#int F0/0
Router(config-if)#ip nat inside (côté LAN)

Router(config)#int S0/0/0
Router(config-if)#ip nat ouside (côté WAN)
```

rr. *ETAPE 2: Activation du NAT*

```
Router(config)# ip nat inside source static tcp 192.168.2.1 80     80.0.0.3 80
```

N° de port

IX. LINUX CONFIG

Mettre ssh :
sudo nano /etc/apt/sources.list et mettre universe multiverse partout
sudo apt-get update
sudo apt-get install openssh-client-ssh1

Connection à un routeur en ssh :
ssh1 cisco@10.59.48.2 -p 500X -1

>service network-manager stop

Il est possible qu'on vous demande de mettre votre PC en serveur HTTP pour ce faire :

- >sudo apt-get update
- >sudo apt-get install apache 2

Pour configuré un SERVEUR HTTP sur un routeur :

- ip http server

a. Configuration de l'adresse IP

sudo dhclient *nom-interface* ->DHCP
sudo ifconfig *nom-interface* _-_-_-_ netmask _-_-_-_
sudo ifconfig *nom-interface* up/down
ifconfig

b. Configuration de la passerelle par défaut

sudo route add default gw _-_-_-_
route -n

c. Configuration de l'adresse du serveur DNS

sudo nano /etc/resolv.conf
nameserver 10.59.4.2
cat /etc/resolv.conf

X. IPV6

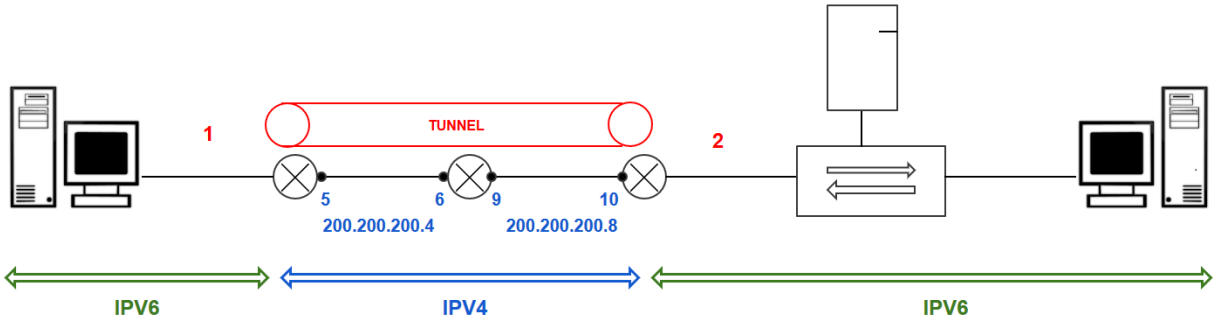
a. Commandes de base

(config) #ipv6 unicast-routing
(config-if)#ipv6 address 2001 :600 ::1/64 (adresse/masque)
#sh ipv6 interface brief
#sh ipv6 route
(config)#ipv6 route *adresse_réseau_destination/masque nom_interface_de_sortie*
Mettre ::/0 si on prend une route pas défaut.

b. RIP

Sur les interfaces des routeurs concernés
(config-if)#ipv6 rip MYRIP enable

XI. Tunnel IPV6



Pour le coté 1 sur le schéma :
int tunnel 0
tunnel source fa 0/0
tunnel dest 200.200.200.10
tunnel mode ipv6ip

Pour le coté 2 :
int tunnel 0
tunnel source fa 0/0
tunnel dest 200.200.200.0
tunnel mode ipv6ip
ipv6 address (pas sur)

ip -6 address add 2001 :600 ::1 :64 dev x où x est le nom de l'interface
ip link set dev x up/down
ip -6 route add default via 2001:600::2

Vérification : route -6 -n
ping 6

XII. SNMP

a. Installation

sudo apt update
sudo apt-get install snmp
sudo apt-get install snmpd
apt-get install snmp-mibs-downloader
export MIBS=ALL

b. Configuration agent Windows

Control Panel -> Ajout de composants Windows -> Ajouter les 2 composants commençant par snmp

c. Configuration agent Cisco

#sh snmp

(config)# snmp-server community MDP ro //pour read-only
(config)#snmp-server community MDP rw //pour read-write

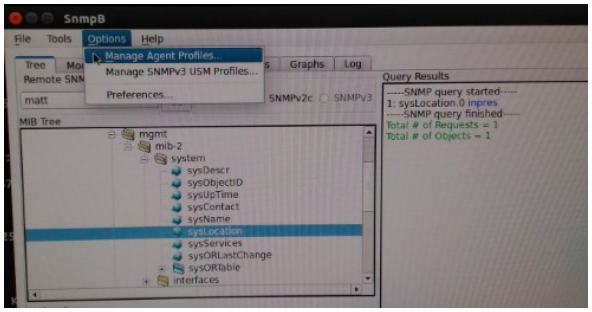
Comment sécuriser ? Utiliser une access-list pour définir qui va pouvoir lire les informations sur ce router.
access-list 50 permit host 192.168.1.100(où cette IP est l'ip de la station NMS)
(config)#snmp-server community MDP ro 50

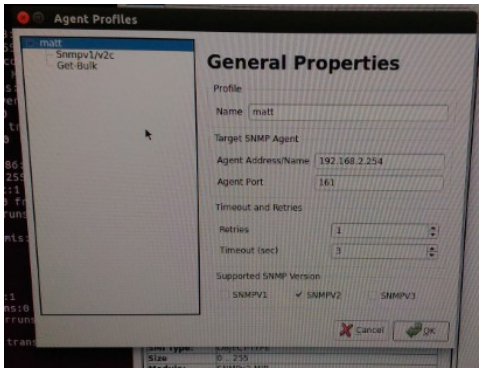
Création d'une vue en snmp : (faire la commande pour chaque élément que l'on veut voir)
(config)#snmp-server view VUELIMITEE 1.3.6.1.4.100 included/excluded

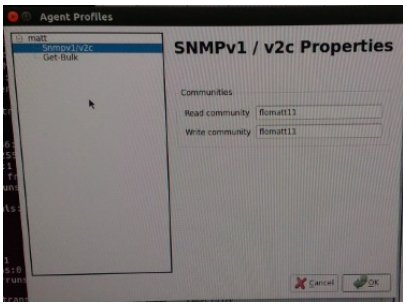
Comment appliquer la vue ?
(config)#snmp-server community MDP view VUELIMITEE ro 50
(config)#snmp-server contact… (on met ici le nom du contact)
(config)#snmp-server location… (on met ici l'emplacement de l'équipement)

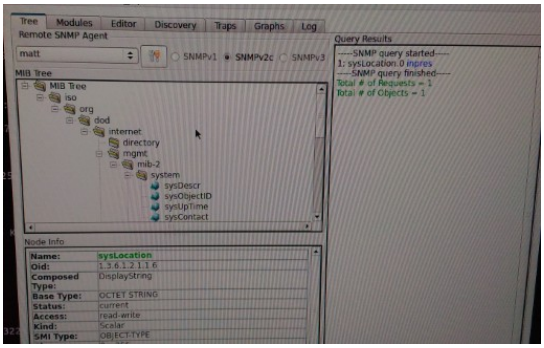
d. Utilisation SNMPB

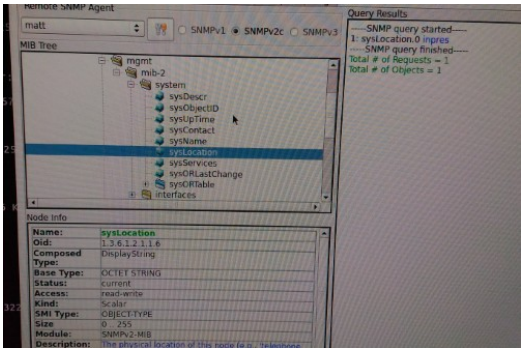
Pour l'installation voir SNMPBProcédureInstall

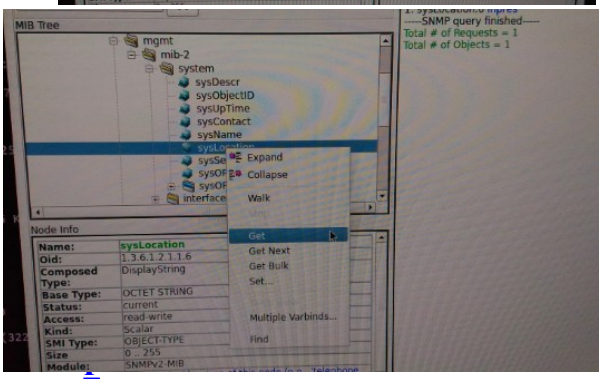












[C](#)

[ation traps](#)

(config) #snmp-server host 192.168.1.100 (IP NMS)
Question : comment n'autoriser que les traps ? Dans l'access-list 50, mettre un deny any.

En linux :
apt-get install snmptrapd
snmptrapd -Le -f
En linux, mais snmpb :
Traps apparaissent dans l'onglet trap

XIII. VPN

a. Commande phase 1

A répéter sur les 2 routeurs qui sont entre les tunnels
#crypto isakmp policy 1
#authentication pre-share
#encryption aes 128
#hash md5
#group 2
#lifetime ?

Vu qu'on a fait avec authentication pre-share, il faut définir une clé :
#crypto isakmp key SECRET address 192.168.2.2 -> ip du routeur opposé

b. Commandes phase 2 :

#crypto ipsec transform-set MYSET ah-sha-hmac esp-aes 128(faire non crypter)
#crypto map MYMAP 1 ipsec-isakmp
#set peer 192.168.2.2 -> ip du routeur opposé
#set transform-set MYSET
#match address 100
#access-list 100 permit icmp host 192.168.1.1 host 192.168.3.1
#interface f0/1
#crypto map MYMAP

On vérifie le bon fonctionnement du tunnel à l'aide de la commande :
#sh crypto iskamp sa
qui permet de montrer le nombre de paquets que le routeur a crypté.

XIV. 802.1x

a. Commande sur le switch

Création des VLANs et ne pas oublier de mettre une ip au switch pour le VLAN où se trouve le serveur Windows

(config)#dot1x system-auth-control
(config)# aaa new-model
(config)# aaa authentication dot1x default group radius
(config)# radius-serveur host <ip serveur> key SECRET

(config)#int f0/1 // Sur l'interface connectée au supplicant
(config-if)#switchport mode access
(config-if)#spanning-tree portfast
(config-if)#dot1x port-control auto // Sur l'interface connectée au supplicant
(config-if)#authentication host-mode multi-host //Si VM (plusieurs mac sur 1 port)

(config)#aaa authorization network default group radius

(config)#ip dhcp pool vlan3
(config-if) #network 192.168.3.0/24
(config-if)#default-router 192.168.3.254
(config-if)#dns-server 192.168.1.10
(config-if)# exit
(config)#ip dhcp pool vlan4
(config-if)#network 192.168.4.0/24
(config-if)#default-router 192.168.4.254
(config-if)#dns-server 192.168.1.10

c. Commande sur le routeur

Création des VLANs
Sur chaque sous-interface :

- (config-if)# encapsulation dot1Q ***NUMERO_VLAN***
- (config-if)# ip address ***ADRESSE MASQUE***
- (config-if)# ip helper-address ***ADRESSE_SERVEUR_DHCP***

d. Serveur Windows

1) Ajouter des utilisateurs et des groupes

➔ Cliquer sur "Tools" -> "Add users"
➔ Clic droit sur "user" dans la colonne de gauche puis "add group" ou "add user"
➔ Décocher la case "user must reset password"

2) Intaller NPS

➔ Manage
➔ Add roles and features

➔ Choose Network Policy Service

3) Ajouter Client Radius

➔ Cliquer sur « NAP » puis dans « Servers » clic droit sur notre serveur
➔ Choose NPS
➔ Clic droit sur « Radius Client » et on en crée un nouveau
➔ Ajouter l'ip du switch comme ip du client

4) Ajouter Connection Request Policy

➔ New Connection Request Policy
➔ Ajout d'un nom
➔ Ajout d'une condition « NAS-PORT-TYPE »

5) Ajouter Network Policy

➔ New Network Policy
➔ Ajout d'un nom
➔ Ajouter condition « NAS-PORT-TYPE -> ethernet » et « user groups »
➔ Tout décocher et prendre seulement PEAP

6) Enregistré dans l'Active Directory

➔ Clic droit sur « NPS(local) » puis « Register in active directory »

7) DHCP

➔ Choose DHCP dans le menu gauche du dashbord
➔ Ajouter les VLAN au Network Policy dans les options « Standards »
  - Ajouter « Tunnel-Medium-Type » en default
  - Ajouter « Tunnel-Pvt-Group-Id » et mettre le numéro de VLAN correspondant au client
  - Ajouter Tunnel-Type en default

Fonctionnement du vlan dynamique : Le client va contacter la sous interface du router qui via le ip helper-adress va contacter le serveur radius.

De là, le serveur va aller rechercher la policy correspondante au groupe dans lequel est enregistré l'utilisateur.

Ensuite le serveur va dire au switch de mettre le port qui l'a contacté (celui sur lequel est branché le client) dans le vlan spécifié dans la policy.

Seulement après ça, le client va pouvoir faire une requete DHCP.

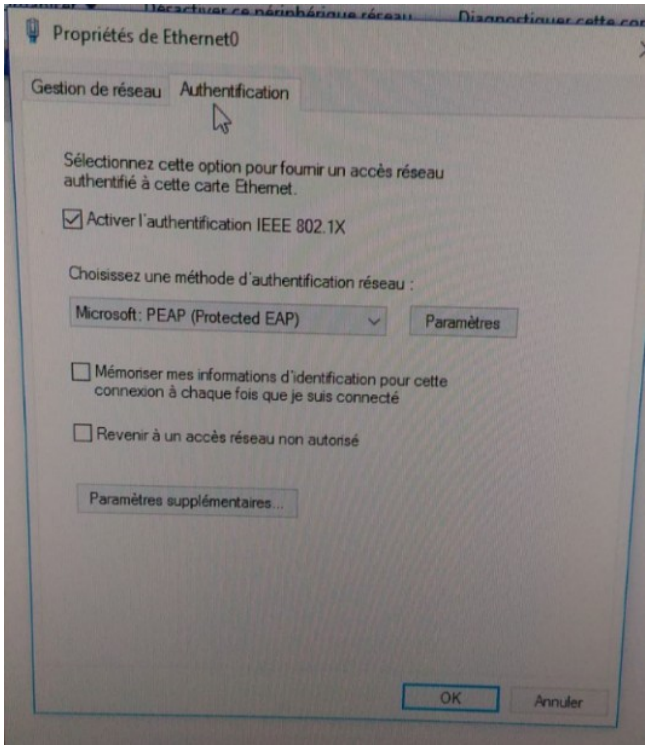
Les utilisateurs se connectant se verront attribuer une IP en fonction de leur groupe et de la policy auquel ce groupe est associé.

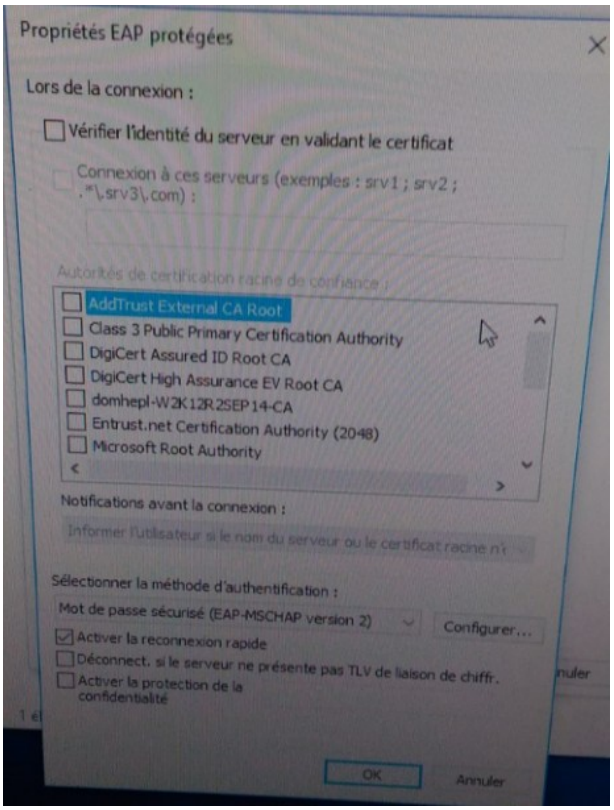
e. Client Windows

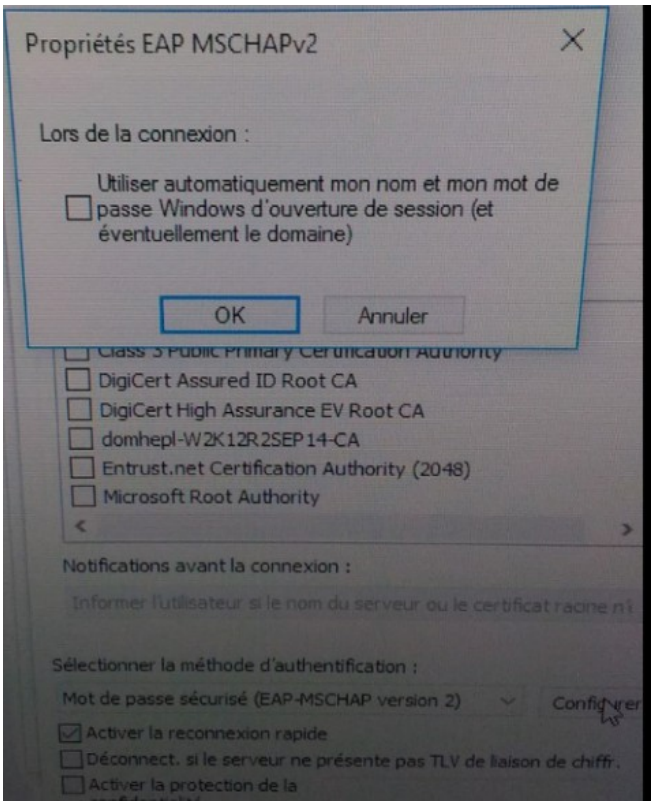
➔ Lancer le service « configuration automatique du réseau câblé »

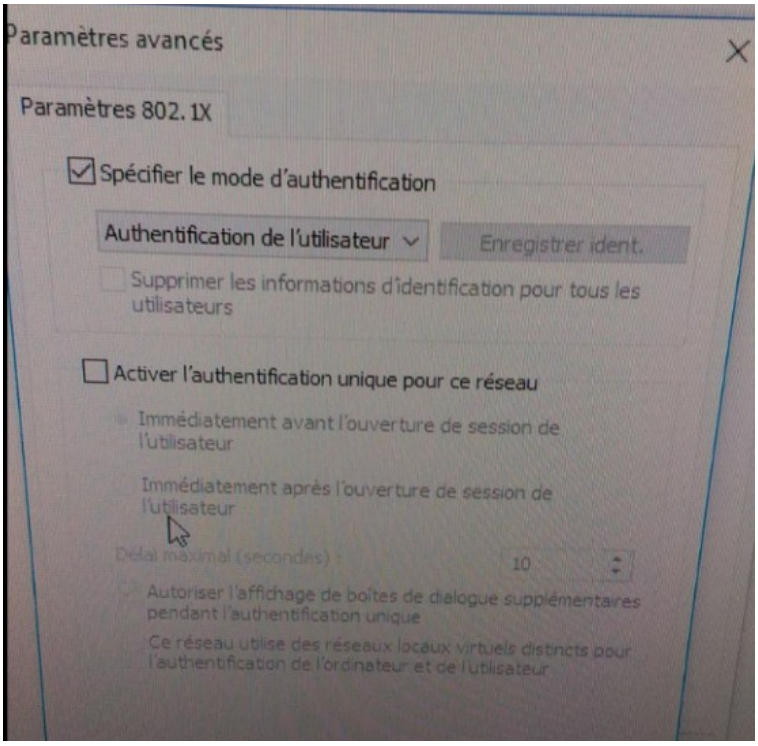
➔ Vérifier dans ncpa.cpl dans l'onglet de IPv4 que nous avons un nouvel onglet à configurer

➔ Dans « Paramètres avancés », dans « enregistré identifiant » il faut entrer le nom de domaine et le mdp afin de se connecter au serveur radius






Propriétés EAP MSCHAPv2
Lors de la connexion :
Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session (et éventuellement le domaine)
OK
Annuler
DigiCert Assured ID Root CA
DigiCert High Assurance EV Root CA
domhepl-W2K12R2SEP14-CA
Entrust.net Certification Authority (2048)
Microsoft Root Authority
Notifications avant la connexion :
Sélectionner la méthode d'authentification :
Mot de passe sécurisé (EAP-MSCHAP version 2)
Activer la reconnexion rapide


Paramètres avancés
Paramètres 802.1X
Spécifier le mode d'authentification
Authentification de l'utilisateur
Enregistrer ident.
Supprimer les informations d'identification pour tous les utilisateurs
Activer l'authentification unique pour ce réseau
Immédiatement avant l'ouverture de session de l'utilisateur
Immédiatement après l'ouverture de session de l'utilisateur
Délai maximal (secondes) :
10
Autoriser l'affichage de boîtes de dialogue supplémentaires pendant l'authentification unique
Ce réseau utilise des réseaux locaux virtuels distincts pour l'authentification de l'ordinateur et de l'utilisateur