OSI 3 : routage et VLAN

1. Routage et VLAN

Les VLAN permettent une isolation des LAN : aucune communication n'est possible... à moins d'installer un routeur entre les VLANs (ou d'utiliser un switch de niveau 3, ce qui revient « à peu près » au même).
Par principe, même si ce n'est pas obligatoire, chaque VLAN est dans un réseau (ou sousréseau) IP spécifique. C'est très fortement conseillé, car le jour où vous aurez besoin de les faire communiquer (ne serait-ce que pour des tâches d'administration), vous serez bien content !

1A. Plan d'adressage

Deux scénarii sont envisageables :

1. Votre LAN est en adressage public (classe C en général). Il faudra mettre en œuvre un lan d'adressage de type sous-réseau, en application de la RFC 1878. Pour faire nos calculs, nous pouvons utiliser des sites en ligne (http://www.subnetmask.info/ par exemple) ou une commande disponible sous Linux et sous Windows : ipcalc.

```
# apt-get install ipcalc
```

Supposons que nous soyons titulaires de l'adresse publique 193.193.193.0 et que nous souhaitions 3 sous-réseaux avec 60 hôtes chacun :

```
root@stretch64:~# ipcalc -bs 60 60 60 193.193.193.0/24
Address:   193.193.193.0
Netmask:   255.255.255.0 = 24
Wildcard:  0.0.0.255
=>
Network:   193.193.193.0/24
HostMin:   193.193.193.1
HostMax:   193.193.193.254
Broadcast: 193.193.193.255
Hosts/Net: 254                  Class C

1. Requested size: 60 hosts
Netmask:   255.255.255.192 = 26
Network:   193.193.193.0/26
HostMin:   193.193.193.1
HostMax:   193.193.193.62
Broadcast: 193.193.193.63
Hosts/Net: 62                   Class C

2. Requested size: 60 hosts
Netmask:   255.255.255.192 = 26
Network:   193.193.193.64/26
HostMin:   193.193.193.65
HostMax:   193.193.193.126
Broadcast: 193.193.193.127
Hosts/Net: 62                   Class C

3. Requested size: 60 hosts
Netmask:   255.255.255.192 = 26
Network:   193.193.193.128/26
HostMin:   193.193.193.129
HostMax:   193.193.193.190
Broadcast: 193.193.193.191
Hosts/Net: 62                   Class C

Needed size:  192 addresses.
Used network: 193.193.193.0/24
Unused:
193.193.193.192/26
root@stretch64:~#
```

En conclusion, nous pourrions donc avoir le plan d'adressage suivant :

VLAN100	193.193.193.0/26
VLAN200	193.193.193.64/26
VLAN300	193.193.193.128/26

2. En adressage privé (RFC 1918), vous êtes totalement libre et la solution sous-réseau n'est pas utile. Vous pouvez par exemple mettre une classe C dans chaque sous-réseau :

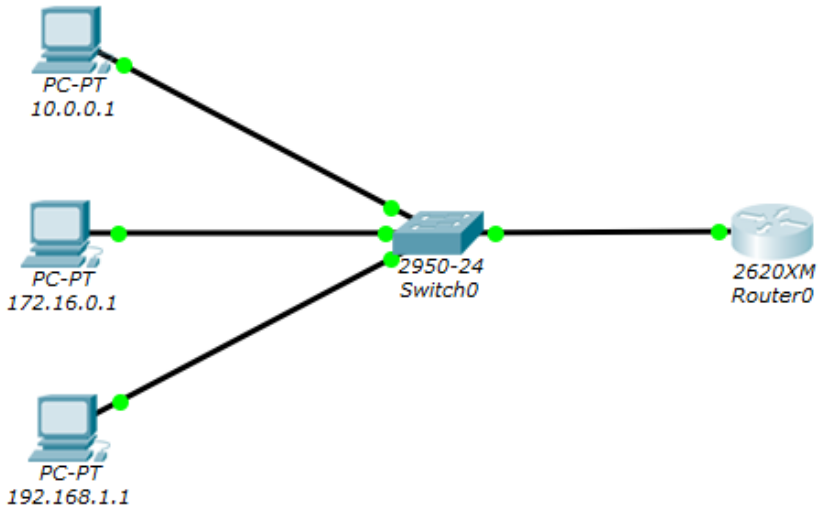
VLAN100 = 192.168.1.0/24, VLAN200 = 192.168.2.0/24, etc.

1B. Exemple

Dans un but pédagogique, nous mettrons en oeuvre le plan d'adressage suivant :

VLAN100	10.0.0.0/8
VLAN200	172.16.0.0/16
VLAN300	192.168.1.0/24

Réalisez la topologie suivante avec PacketTracer :



Celle-ci est constituée de : 3 PC, 1 commutateur 2950-24, 1 routeur 2620XM.

Sur les PC, vous configurez les adresses IP indiquées et le masque correspondant. Pour l'instant, vous n'indiquez pas de passerelle.
Sur le commutateur, vous configurez les VLANs et le trunk :

Port du commutateur	Affectation	Appareil connecté
FastEthernet 0/1	VLAN100	PC 10.0.0.1
FastEthernet 0/2	VLAN200	PC 172.16.0.1
FastEthernet 0/3	VLAN300	PC 192.168.1.1
FastEthernet 0/4	TRUNK	Port de connexion du routeur

Sur le routeur, les configurations doivent être faites en IOS. Le principe est de créer autant d'interfaces réseau **virtuelles** que de VLAN. Nous mettrons ces interfaces dans un VLAN avec une adresse IP dans le réseau IP correspondant. Celle-ci servira de passerelle à configurer sur les PCs. Le routeur sera alors en mesure de router les paquets IP entre ces réseaux.

Le schéma sur le routeur sera le suivant :

Port du routeur	Affectation	Adresse IP
FastEthernet 0/0.1 (le .1 signifie « sous-interface »)	VLAN100	10.0.0.254
FastEthernet0/0.2	VLAN200	172.16.0.254
FastEthernet0/0.3	VLAN300	192.168.1.254

Voici les commandes à saisir dans l'IOS du routeur. D'abord, activons l'interface physique :

```
Routeur>en
Router#conf t
Enter confi guration commands, one per line. End with CNTL/Z.
Router(confi g)#interface fastEthernet 0/0
Router(confi g-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
Router(confi g-if)#exit
```

Nous entrons maintenant dans l'interface virtuelle .1 (sous-interface de l'interface réseau physique FastEthernet 0/0, Vous pouvez en créer autant que vous le voulez) :

```
Router(confi g)#int FastEthernet 0/0.1
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed
state to up
```

Comme le lien qui nous relie au switch est en mode trunk, nous devons informer le routeur d'encapsuler et de marquer (tag) les paquets qu'il envoie sur l'interface en utilisant la norme IEEE 802.1Q (dot1Q). Les paquets doivent être marqués à destination du VLAN 100 :

```
Router(confi g-subif)#encapsulation dot1Q 100
Router(confi g-subif)#ip address 10.0.0.254 255.0.0.0
Router(confi g-if)#exit
```

Nous faisons de même pour l'interface virtuelle .2, sauf que les paquets sont pour le VLAN 200 :

```
Router(confi g)#int FastEthernet 0/0.2
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed
state to up
Router(confi g-subif)#encapsulation dot1Q 200
Router(confi g-subif)#ip address 172.16.0.254 255.255.0.0
Router(confi g-subif)#exit
```

Et enfin pour la troisième :

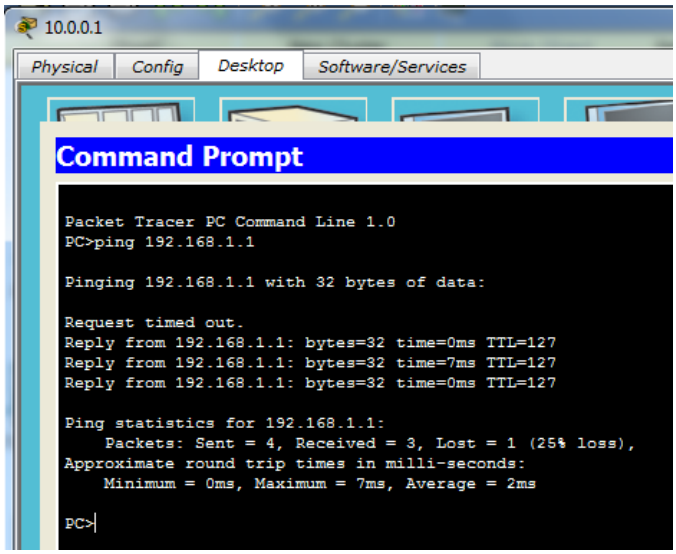
```
Router(confi g)#int FastEthernet 0/0.3
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed
```

```
state to up
Router(confi g-subif)#encapsulation dot1Q 300
Router(confi g-subif)#ip address 192.168.1.254 255.255.255.0
Router(confi g-subif)#exit
```

En dernier lieu, vous configurez la passerelle par défaut sur les PC en indiquant l'adresse IP côté routeur.

PC	Adresse IP de passerelle
10.0.0.1	10.0.0.254
172.16.0.1	172.16.0.254
192.168.1.1	192.168.1.254

Au bout de quelques instants, toutes les machines peuvent se pinguer. Ce n'est pas un miracle car notre routeur a joué son rôle de... routeur.



Voyons sa table de routage :

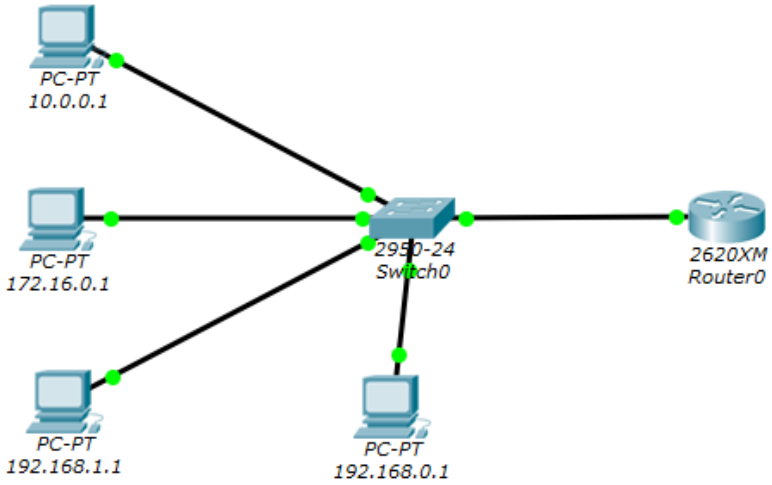
```
Router(confi g)#exit
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
C 10.0.0.0/8 is directly connected, FastEthernet0/0.1
C 172.16.0.0/16 is directly connected, FastEthernet0/0.2
C 192.168.1.0/24 is directly connected, FastEthernet0/0.3
```

Notre routeur sait joindre chacun des 3 réseaux, ce qui est normal puisqu'il est directement connecté. Il est donc capable de mettre chaque réseau en relation avec les deux autres.

2. Accès par SSH

Nous allons configurer un accès SSH d'un PC vers le routeur pour pouvoir l'administrer depuis le réseau de façon donc … sécurisée.

On connecte un PC sur le port fa0/5. On affecte une IP 192.168.0.1 et on place le port dans le VLAN d'administration (1000 par exemple à créer).



Sur le routeur, on configure une quatrième interface virtuelle (fa 0/0.4) que l'on place dans le VLAN 1000 et sur laquelle on met une IP 192.168.0.254. Ensuite, il faut générer une paire de clés de chiffrement (privée, publique), puisque ssh peut reposer sur un algorithme de chiffrement asymétrique :

```
Router(confi g)#hostname router0
router0(confi g)#ip domain-name labo.local
router0(confi g)#crypto key generate rsa
The name for the keys will be: router0.labo.local
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
*mars 1 0:8:2.292: RSA key size needs to be at least 768 bits for ssh
version 2
*mars 1 0:8:2.292: %SSH-5-ENABLED: SSH 1.5 has been enabled
```

Nous devons maintenant créer un utilisateur habilité à se connecter :

```
router0(confi g)#aaa new-model
router0(confi g)#username util1 password pass1
```

Nous forçons l'accès à distance en mode ssh :

```
router0(confi g)#line vty 0 15
router0(confi g-line)#transport input ssh
```

Il faudra également définir un mot de passe pour enable, mais ça vous savez déjà le faire.

Ensuite du PC, testez la connexion ssh :

```
PC>ssh -l util1 192.168.0.254
Open
Password:
router0>en
Password:
router0#
```

Vérifiez bien que la connexion par telnet ne fonctionne pas :

```
PC>telnet 192.168.0.254
Trying 192.168.0.254 ...Open

[Connection to 192.168.0.254 closed by foreign host]
PC>
```