

2017-2018

# Restructuration du réseau d'Arconic Toulouse par VLANS

Epreuve E4



Andrieu, Raphael  
ARCONIC

## Table des matières

|   |    |
|---|----|
| Contexte .....                                | 2  |
| Cahier des charges.....                       | 2  |
| Solution proposée .....                       | 2  |
| Ressources.....                               | 3  |
| Configuration du Switch Cisco.....            | 3  |
| VLANS .....                                   | 3  |
| Création des VLANS.....                       | 3  |
| Mises en place des PORTS sur les VLANS .....  | 5  |
| Configuration du mode TRUNK .....             | 7  |
| Ajout d'un mot de passe de configuration..... | 8  |
| Sauvegarde de la configuration.....           | 8  |
| Configuration du routeur Cisco .....          | 9  |
| Configuration des sous-interfaces.....        | 9  |
| Mise en place des Access-List.....            | 10 |
| Ajout d'un mot de passe de configuration..... | 11 |
| Attribution d'un nom .....                    | 12 |
| Sauvegarde de la configuration.....           | 12 |
| Récapitulatif table de routage.....           | 12 |
| Mise en place du serveur DHCP .....           | 13 |
| Configuration réseau.....                     | 13 |
| Installation du service .....                 | 14 |
| Activation du routage et du NAT.....          | 16 |
| Activation du routage.....                    | 16 |
| Activation du nat .....                       | 16 |
| Automatiser le montage du NAT .....           | 17 |
| Ajout des routes sur le routeur Debian.....   | 16 |

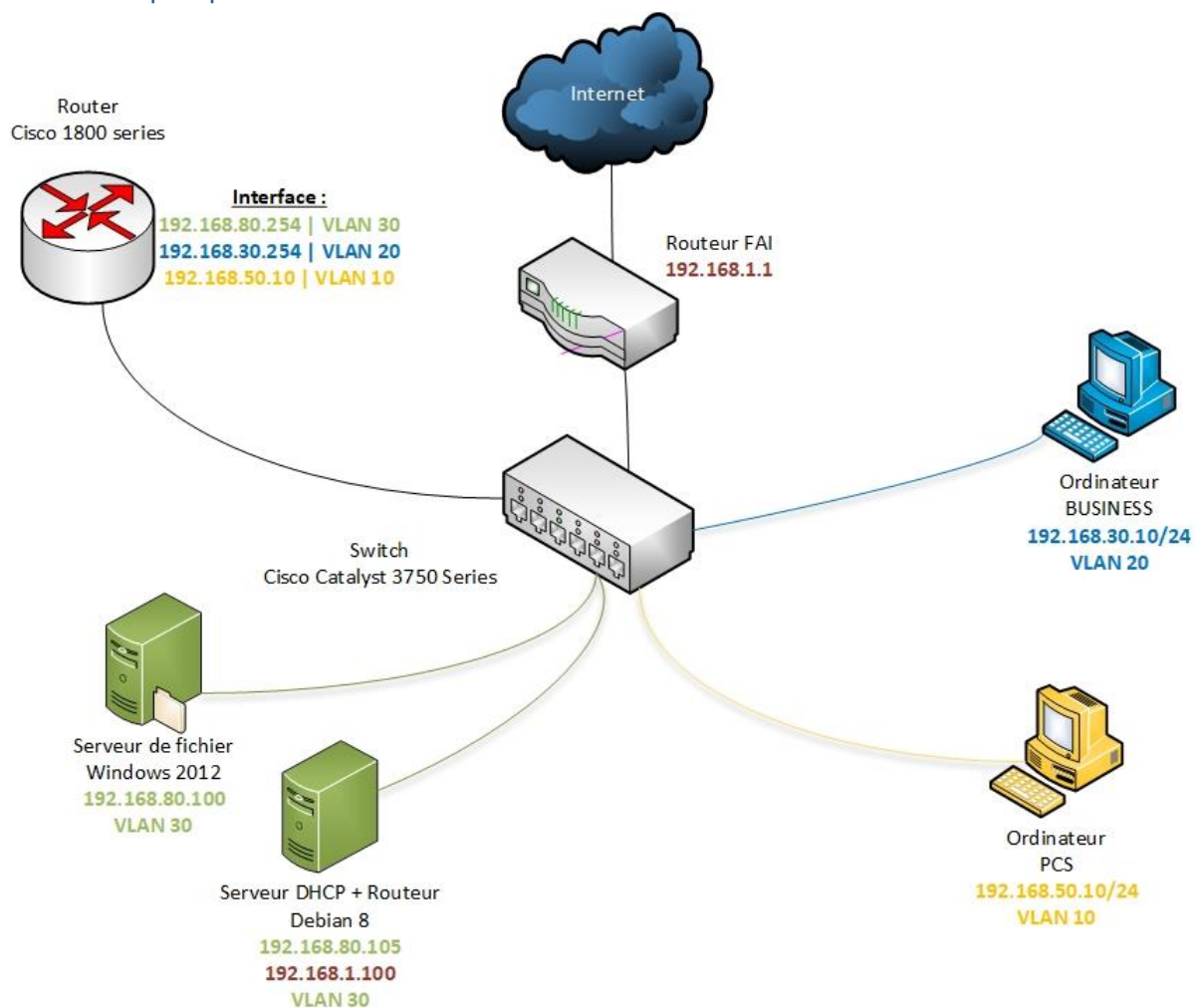
## Contexte

Depuis de nombreuses années, le service Expédition n'a pas fait l'objet d'évolution. Aujourd'hui, l'organisation et les méthodes de travail ne sont plus adaptées à l'activité et ne permettent pas d'atteindre un niveau de performance satisfaisant. L'objectif étant donc d'améliorer la qualité et l'efficacité du service. Face à cette réorganisation, l'administrateur réseau a décidé de mettre en place un nouveau switch dans la baie des Expéditions et de remplacer un ancien router afin de sécuriser les nouveaux postes de travail des salariés en séparant les flux réseau.

## Cahier des charges

- Séparer les différents matériels informatiques en paramétrant 3 VLAN sur le nouveau switch
  - Business
  - PCS
  - Serveur
- Routage inter-VLAN
- Mise en place des ACL : Interdire toute communication entre le réseau BUSINESS et le réseau PCS
- Paramétrage d'un serveur DHCP
  - Business : Adresse en 192.168.30.0
  - PCS : Adresse en 192.168.50.0

## Solution proposée



## Ressources

Nous disposons pour ce projet :

- Un switch Cisco Catalyst 3750
- Deux ordinateurs (1 Business, 1 PCS)
- Un serveur DHCP et Router sous Debian 8
- Un serveur de fichier sous Windows serveur 2012

## Configuration du Switch Cisco

### VLANS

Création des VLANS

Nous allons tout d'abord mettre en place les VLANS (Virtual Lan), c'est-à-dire les différents réseaux virtuels qui nous permettrons de segmenter le réseau, pour ainsi augmenter la sécurité.



**VLAN BUSINESS : 16 ports**

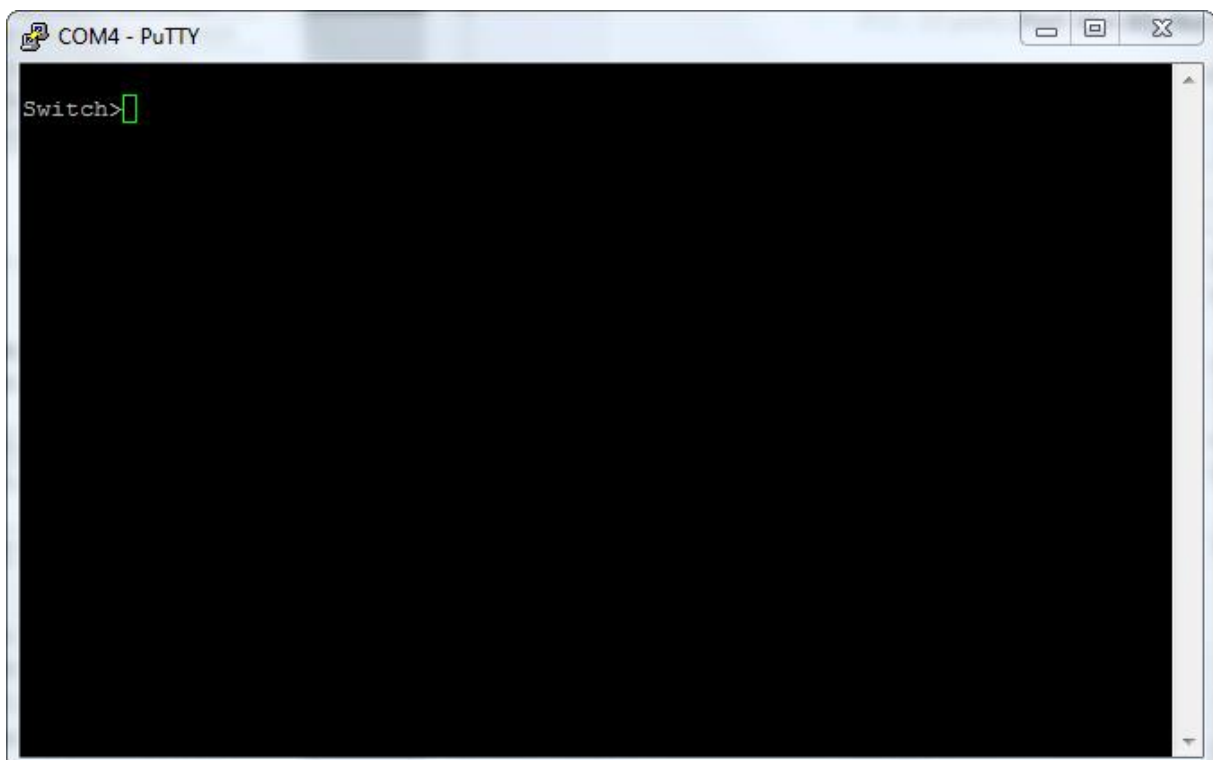
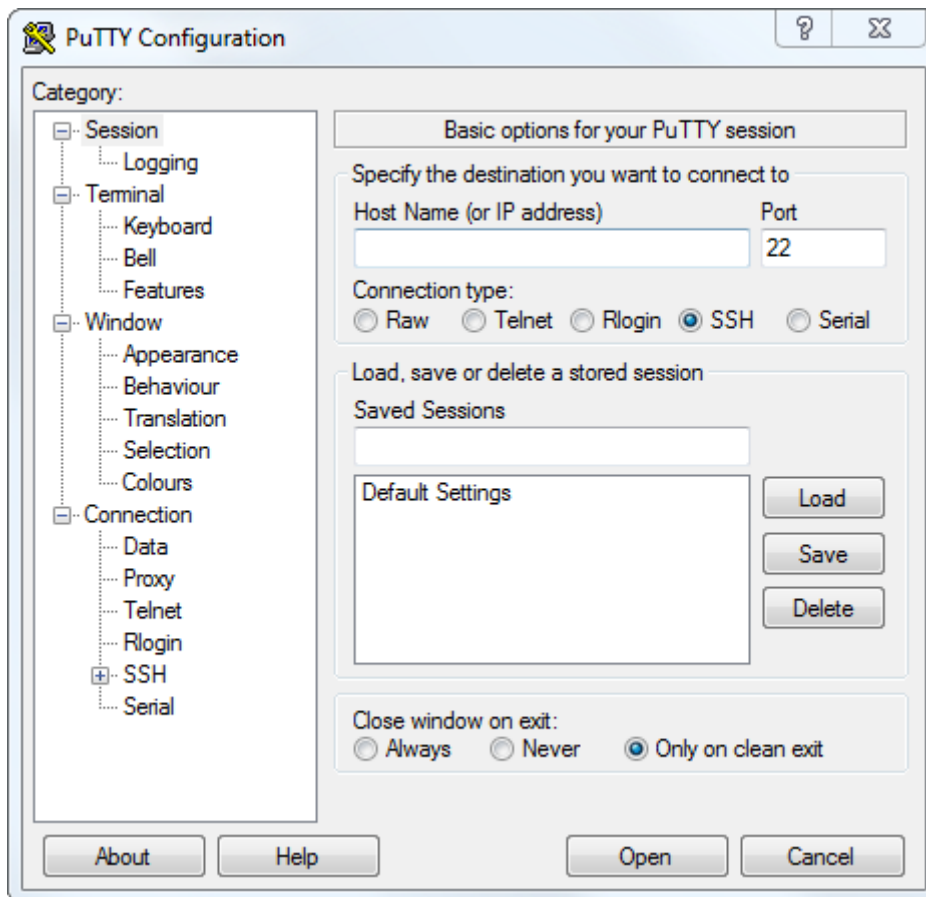
**VLAN PCS : 16 ports**

**VLAN SERVEUR : 6 ports**

Les VLANS à mettre en place sont :

- Business : 16 ports (Port 1 à 16), Numéro : 20
- PCS : 16 ports (Port 17 à 32), Numéro : 10
- Serveur : 6 ports (Port 33 à 38), Numéro : 30

Nous nous connectons pour cela au Switch Cisco à l'aide du port console et du logiciel Putty.



### Commandes

### Explications

Switch>Enable

On passe en mode privilégié pour modifier la configuration

Switch#conf t

On entre dans la configuration

|                                   |  |
|-----------------------------------|--|
| Switch(config)#vlan 20            | On crée le VLAN 20, qui nous servira pour la segmentation du service Business    |
| Switch(config-vlan)#name BUSINESS | On lui donne le nom « BUSINESS »   |
| Switch(config-vlan)#exit          | On retourne en mode config   |
| Switch(config)#vlan 10            | On crée ensuite le VLAN 10, qui nous servira pour la segmentation du service PCS |
| Switch(config-vlan)#name PCS      | On lui donne le nom « PCS »  |
| Switch(config-vlan)#exit          | On retourne en mode config   |
| Switch(config)#vlan 30            | On crée ensuite le VLAN 30, qui nous servira pour la segmentation des serveurs   |
| Switch(config-vlan)#name SERVEUR  | On lui donne le nom « SERVEUR »  |
| Switch(config-vlan)#end           | On sort de la configuration du switch  |

```
Switch(config)#vlan 20
Switch(config-vlan)#name BUSINESS
Switch(config-vlan)#exit
Switch(config)#vlan 10
Switch(config-vlan)#name PCS
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name SERVEUR
Switch(config-vlan)#end
Switch#
```

Nous pouvons maintenant exécuter la commande « show vlan » pour s'assurer que les 3 VLANS ont bien été mis en place.

```
Switch#show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa2/0/1, Fa2/0/2, Fa2/0/3
                                           Fa2/0/4, Fa2/0/5, Fa2/0/6
                                           Fa2/0/7, Fa2/0/8, Fa2/0/9
                                           Fa2/0/10, Fa2/0/11, Fa2/0/12
                                           Fa2/0/13, Fa2/0/14, Fa2/0/15
                                           Fa2/0/16, Fa2/0/17, Fa2/0/18
                                           Fa2/0/19, Fa2/0/20, Fa2/0/21
                                           Fa2/0/22, Fa2/0/23, Fa2/0/24
                                           Fa2/0/25, Fa2/0/26, Fa2/0/27
                                           Fa2/0/28, Fa2/0/29, Fa2/0/30
                                           Fa2/0/31, Fa2/0/32, Fa2/0/33
                                           Fa2/0/34, Fa2/0/35, Fa2/0/36
                                           Fa2/0/37, Fa2/0/38, Fa2/0/39
                                           Fa2/0/40, Fa2/0/41, Fa2/0/42
                                           Fa2/0/43, Fa2/0/44, Fa2/0/45
                                           Fa2/0/46, Fa2/0/47, Fa2/0/48
                                           Gi2/0/1, Gi2/0/2, Gi2/0/3
                                           Gi2/0/4
10   PCS                    active
20   BUSINESS               active
30   SERVEUR                 active
```

Mises en place des PORTS sur les VLANS

Nous allons maintenant définir la tranche des ports de chaque VLAN.

| Commandes   | Explications  |
|---|---|
| Switch>Enable                                     | On passe en mode privilégié pour modifier la configuration                        |
| Switch#conf t                                     | On entre dans la configuration  |
| Switch(config)#int range FA2/0/1-16               | On sélectionne les ports FastEthernet(FA) de 1 à 16                               |
| Switch(config-if-range)#description BUSINESS      | On ajoute une description pour ces ports  |
| Switch(config-if-range)#switchport mode access    | On définit le mode ACCESS pour ces ports (C'est-à-dire qu'un seul VLAN circulera) |
| Switch(config-if-range)#switchport access VLAN 20 | On définit le VLAN 10 pour ces ports  |
| Switch(config-if-range)#exit                      | On retourne en mode config  |
| Switch(config)#int range FA2/0/17-32              | On sélectionne les ports FastEthernet(FA) de 17 à 32                              |
| Switch(config-if-range)#description PCS           | On ajoute une description pour ces ports  |
| Switch(config-if-range)#switchport mode access    | On définit le mode ACCESS pour ces ports (C'est-à-dire qu'un seul VLAN circulera) |
| Switch(config-if-range)#switchport access VLAN 10 | On définit le VLAN 20 pour ces ports  |
| Switch(config-if-range)#exit                      | On retourne en mode config  |
| Switch(config)#int range FA2/0/33-38              | On sélectionne les ports FastEthernet(FA) de 33 à 38                              |
| Switch(config-if-range)#description SERVEUR       | On ajoute une description pour ces ports  |
| Switch(config-if-range)#switchport mode access    | On définit le mode ACCESS pour ces ports (C'est-à-dire qu'un seul VLAN circulera) |
| Switch(config-if-range)#switchport access VLAN 30 | On définit le VLAN 20 pour ces ports  |
| Switch(config-if-range)#end                       | On sort de la configuration du switch   |

```
Switch(config)#int range FA2/0/1-16
Switch(config-if-range)#description BUSINESS
Switch(config-if-range)#swi
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access VLAN 20
Switch(config-if-range)#exit
Switch(config)#int range FA2/0/17-32
Switch(config-if-range)#description PCS
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access VLAN 10
Switch(config-if-range)#exit
Switch(config)#int range FA2/0/33-38
Switch(config-if-range)#description SERVEUR
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access VLAN 30
Switch(config-if-range)#end
Switch#
```

Nous pouvons maintenant exécuter la commande « show vlan » pour nous assurer que les VLANS sont bien configuré.

```
Switch#show vlan
VLAN Name                Status    Ports
-----
1    default                active    Fa2/0/39, Fa2/0/40, Fa2/0/41
                                           Fa2/0/42, Fa2/0/43, Fa2/0/44
                                           Fa2/0/45, Fa2/0/46, Fa2/0/47
                                           Fa2/0/48, Gi2/0/1, Gi2/0/2
                                           Gi2/0/3, Gi2/0/4
10   PCS                    active    Fa2/0/17, Fa2/0/18, Fa2/0/19
                                           Fa2/0/20, Fa2/0/21, Fa2/0/22
                                           Fa2/0/23, Fa2/0/24, Fa2/0/25
                                           Fa2/0/26, Fa2/0/27, Fa2/0/28
                                           Fa2/0/29, Fa2/0/30, Fa2/0/31
                                           Fa2/0/32
20   BUSINESS              active    Fa2/0/1, Fa2/0/2, Fa2/0/3
                                           Fa2/0/4, Fa2/0/5, Fa2/0/6
                                           Fa2/0/7, Fa2/0/8, Fa2/0/9
                                           Fa2/0/10, Fa2/0/11, Fa2/0/12
                                           Fa2/0/13, Fa2/0/14, Fa2/0/15
                                           Fa2/0/16
30   SERVEUR                active    Fa2/0/33, Fa2/0/34, Fa2/0/35
                                           Fa2/0/36, Fa2/0/37, Fa2/0/38
```

### Configuration du mode TRUNK

Nous allons mettre en place un port en mode TRUNK, ce qui nous permettra de faire circuler les paquets des VLANS jusqu'au routeur.

| Commandes   | Explications  |
|---|---|
| Switch>Enable   | On passe en mode privilégié pour modifier la configuration              |
| Switch#conf t   | On entre dans la configuration  |
| Switch(config)#int FA2/0/48                             |   |
| Switch(config-if)#description R1                        | On ajoute une description sur ce port                                   |
| Switch(config-if)# switchport trunk encapsulation dot1q | On définit le protocole 802.1Q* sur cette interface                     |
| Switch(config-if)# switchport mode trunk                | On définit le mode TRUNK pour ce port                                   |
| Switch(config-if)#Switchport trunk allowed vlan 2-99    | On définit la tranche des VLANS qui seront en mode TRUNK, ici de 2 à 99 |
| Switch(config-if)#end                                   | On sort de la configuration du switch                                   |

\*Explication de l'encapsulation dot1q : La norme 802.1q indique que les trames sont étiquetées pour contenir le chiffre du VLAN a laquelle elles sont destinées ou attribuées pour ainsi permettre au routeur d'acheminé la trame correctement vers les postes que nous voulons.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa2/0/48
Switch(config-if)#description R1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 2-99
Switch(config-if)#end
Switch#
```



Vous pouvez vérifier la configuration de chaque port avec la commande « show run »

```
interface FastEthernet2/0/48
description R1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 2-99
switchport mode trunk
```

### Ajout d'un mot de passe de configuration

Nous allons sécuriser le switch en lui ajoutant un mot de passe, pour ainsi protéger la configuration pour une personne n'étant pas autorisé à y accéder. Il y a deux possibilités pour le mot de passe, soit nous ajoutons un mot de passe qui ne sera pas crypté par la suite dans la configuration, et donc lisible en clair grâce à une commande, ou alors nous avons la possibilité de crypter ce mot de passe.

Nous choisissons de crypter le mot de passe, pour cela tapez la commande

| Commandes                                | Explications   |
|--|--|
| Switch>Enable                            | On passe en mode privilégié pour modifier la configuration |
| Switch#conf t                            | On entre dans la configuration                             |
| Switch(config)#enable secret 0 Arconic31 | On définit un mot de passe (ici Arconic31)                 |
| Switch(config)#end                       | On sort de la configuration du switch                      |

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable secret 0 Arconic31
Switch(config)#end
Switch#
```

### Attribution d'un nom

| Commandes             | Explications                     |
|-----------------------|----------------------------------|
| Switch>conf t         | On entre dans la configuration   |
| Switch # hostname SW1 | On attribue le nom SW1 au switch |

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1
SW1(config)#
```

### Sauvegarde de la configuration

A chaque redémarrage, le switch perd sa configuration, c'est pour cela que nous allons la sauvegarder.

| Commandes                               | Explications  |
|---|---|
| SW1>En                                  | On passe en mode privilégié pour modifier la configuration                |
| SW1# copy running-config startup-config | On copie la configuration actuelle du switch vers le fichier de démarrage |

```

SW1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW1#

```

## Configuration du routeur Cisco

### Configuration des sous-interfaces

Nous allons maintenant mettre en place les sous-interfaces. Les sous-interfaces nous permettent d'économiser en termes d'interface et de câblage, car ce sont des interfaces que nous configurons directement sur une autre interface, ce qui permet d'en mettre plusieurs sur la même interface.

Nous allons créer trois sous interfaces, une pour chaque vlan, une interface 0.10, une 0.20 et une 0.30, nous allons attribuer à chaque interface une adresse ip :

- 0.10 : 192.168.50.254 (PCS)
- 0.20 : 192.168.30.254 (BUSINESS)
- 0.30 : 192.168.80.254 (SERVEUR)

Puis nous allons indiquer à chacune de ces interfaces l'adresse du DHCP, de base les requêtes ARP ne traversent par les interfaces des routeurs, c'est pour cela que nous allons lui attribuer un agent de relai.

| Commandes  | Explications   |
|--|--|
| Router>En  | On passe en mode privilégié pour modifier la configuration |
| Router# conf t   | On entre en mode configuration                             |
| Router(config)#int fa0/0.20                                  | On sélectionne la sous-interface (VLAN BUSINESS)           |
| Router(config-subif)#encapsulation dot1q 20                  | On procède à l'encapsulation                               |
| Router(config-subif)#ip address 192.168.30.254 255.255.255.0 | On ajoute une adresse IP à cette interface                 |
| Router(config-subif)#description Passerelle BUSINESS         | On ajoute une description                                  |
| Router(config-subif)#ip helper-address 192.168.80.105        | On renseigne l'adresse du serveur DHCP                     |
| Switch(config-if-range)#exit                                 | On retourne en mode config                                 |
| Router(config)#int fa0/0.10                                  | On sélectionne la sous-interface (VLAN PCS)                |
| Router(config-subif)#encapsulation dot1q 10                  | On procède à l'encapsulation                               |
| Router(config-subif)#ip address 192.168.50.254 255.255.255.0 | On ajoute une adresse IP à cette interface                 |
| Router(config-subif)#description Passerelle PCS              | On ajoute une description                                  |
| Router(config-subif)#ip helper-address 192.168.80.105        | On renseigne l'adresse du serveur DHCP                     |
| Switch(config-if-range)#exit                                 | On retourne en mode config                                 |
| Router(config)#int fa0/0.30                                  | On sélectionne la sous-interface (VLAN SERVEUR)            |
| Router(config-subif)#encapsulation dot1q 30                  | On procède à l'encapsulation                               |
| Router(config-subif)#ip address 192.168.80.254 255.255.255.0 | On ajoute une adresse IP à cette interface                 |

|   |  |
|---|--|
| Router(config-subif)#description Passerelle SERVEUR   | On ajoute une description              |
| Router(config-subif)#ip helper-address 192.168.80.105 | On renseigne l'adresse du serveur DHCP |
| Switch(config-if-range)#exit                          | On retourne en mode config             |
| Switch(config)#int fa0/0                              | On sélectionne la sous-interface       |
| Switch(config-if)#no sh                               | On active l'interface sélectionnée     |

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0.20
Router(config-subif)#en
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.30.254 255.255.255.0
Router(config-subif)#description Passerelle BUSINESS
Router(config-subif)#ip helper-address 192.168.80.105
Router(config-subif)#exit
Router(config)#int fa0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.50.254 255.255.255.0
Router(config-subif)#description Passerelle PCS
Router(config-subif)#ip helper-address 192.168.80.105
Router(config-subif)#exit
Router(config)#int fa0/0.30
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 192.168.80.254 255.255.255.0
Router(config-subif)#description Passerelle SERVEUR
Router(config-subif)#ip helper-address 192.168.80.105
Router(config-subif)#exit
Router(config)#

```

Nous allons maintenant ajouter une route par défaut pour l'accès à internet via notre Routeur Debian que nous allons configurer prochainement.

| Commandes  | Explications   |
|--|--|
| Router>En  | On passe en mode privilégié pour modifier la configuration |
| Router# conf t   | On entre en mode configuration                             |
| Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.80.105 | On définit la route par défaut vers notre Routeur Debian   |
| Router(config)#end                                     | On sort de la configuration du routeur                     |

### Mise en place des Access-List

Nous allons maintenant mettre en place les ACL pour ainsi interdire toute communication entre le réseau BUSINESS et le réseau PCS.

| Commandes      | Explications   |
|----------------|--|
| Router>En      | On passe en mode privilégié pour modifier la configuration |
| Router# conf t | On entre en mode configuration                             |

|   |  |
|---|--|
| Router(config)#ip access-list standard 1            | On crée une nouvelle ACL pour le réseau PCS      |
| Router(config-std-nacl)#deny 192.168.30.0 0.0.0.255 | On refuse les paquets du réseau BUSINESS         |
| Router(config-std-nacl)#permit any                  | On autorise les packets des autres réseaux       |
| Router(config-std-nacl)#exit                        | On retourne en mode config                       |
| Router(config)#ip access-list standard 2            | On crée une nouvelle ACL pour le réseau BUSINESS |
| Router(config-std-nacl)#deny 192.168.50.0 0.0.0.255 | On refuse les paquets du réseau PCS              |
| Router(config-std-nacl)#permit any                  | On autorise les packets des autres réseaux       |
| Router(config-std-nacl)#exit                        | On retourne en mode config                       |
| Router(config)#int fa0/0.20                         | On sélectionne la sous-interface BUSINESS        |
| Router(config-subif)#ip access-group 2 out          | On applique l'ACL                                |
| Router(config-std-nacl)#exit                        | On retourne en mode config                       |
| Router(config)#int fa0/0.10                         | On sélectionne la sous-interface PCS             |
| Router(config-subif)#ip access-group 1 out          | On applique l'ACL                                |
| Router(config)#end                                  | On sort de la configuration du routeur           |

```

Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list standard 1
Router(config-std-nacl)#deny 192.168.30.0 0.0.0.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#ip access-list standard 2
Router(config-std-nacl)#deny 192.168.50.0 0.0.0.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#end
Router#
*Mar 24 13:51:45.951: %SYS-5-CONFIG_I: Configured from console by console
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0.20
Router(config-subif)#ip access-group 2 out
Router(config-subif)#exit
Router(config)#int fa0/0.10
Router(config-subif)#ip access-group 1 out
Router(config-subif)#end
Router#

```

### Ajout d'un mot de passe de configuration

| Commandes                                 | Explications   |
|---|--|
| Router>Enable                             | On passe en mode privilégié pour modifier la configuration |
| Router#conf t                             | On entre dans la configuration                             |
| Router (config)#enable secret 0 Arconic31 | On définit un mot de passe (ici Arconic31)                 |
| Router (config)#end                       | On sort de la configuration du switch                      |

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret 0 Arconic31
Router(config)#end
Router#
```

## Attribution d'un nom

| Commandes           | Explications                    |
|---------------------|---------------------------------|
| Router>conf t       | On entre dans la configuration  |
| Router# hostname R1 | On attribue le nom R1 au router |

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

## Sauvegarde de la configuration

A chaque redémarrage, le routeur perd sa configuration, c'est pour cela que nous allons la sauvegarder.

| Commandes                              | Explications  |
|--|---|
| R1>En                                  | On passe en mode privilégié pour modifier la configuration                |
| R1# copy running-config startup-config | On copie la configuration actuelle du switch vers le fichier de démarrage |

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

## Récapitulatif table de routage

| Adresse de destination | Masque        | Passerelle     | Interface      |
|------------------------|---------------|----------------|----------------|
| 0.0.0.0                | 0.0.0.0       | 192.168.80.105 | 192.168.80.254 |
| 192.168.30.0           | 255.255.255.0 | 192.168.30.254 | 192.168.30.254 |
| 192.168.50.0           | 255.255.255.0 | 192.168.50.254 | 192.168.50.254 |
| 192.168.80.0           | 255.255.255.0 | 192.168.80.105 | 192.168.80.254 |

## Test de la configuration

Nous allons maintenant effectuer des tests pour voir si les paramètres sont corrects, pour cela nous allons effectuer un ping de deux postes qui sont dans le même VLAN, puis un ping entre 2 postes qui ne sont pas dans le même VLAN.

Nous allons tout d'abord effectuer sur un poste du VLAN PCS, un ping sur l'interface du VLAN BUSINESS

```

C:\Users\Andri>ping 192.168.30.254

Envoi d'une requête 'Ping' 192.168.30.254 avec 32 octets de données :
Réponse de 192.168.30.254 : octets=32 temps<1ms TTL=255
Réponse de 192.168.30.254 : octets=32 temps<1ms TTL=255
Réponse de 192.168.30.254 : octets=32 temps<1ms TTL=255
Réponse de 192.168.30.254 : octets=32 temps<1ms TTL=255

Statistiques Ping pour 192.168.30.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

```

Tout est okay !

Nous allons maintenant essayer de ping un poste derrière cette interface, c'est-à-dire un poste du réseau BUSINESS.

```

C:\Users\Andri>ping 192.168.30.2

Envoi d'une requête 'Ping' 192.168.30.2 avec 32 octets de données :
Réponse de 192.168.50.254 : Impossible de joindre le réseau de destination.
Réponse de 192.168.50.254 : Impossible de joindre le réseau de destination.
Réponse de 192.168.50.254 : Impossible de joindre le réseau de destination.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.30.2:
    Paquets : envoyés = 4, reçus = 3, perdus = 1 (perte 25%),

```

Le ping est bien bloqué !

Nous allons maintenant essayer de ping un poste du même VLAN.

```

C:\Users\Andri>PING 192.168.50.1

Envoi d'une requête 'Ping' 192.168.50.1 avec 32 octets de données :
Réponse de 192.168.50.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.50.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.50.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.50.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.50.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

```

Tout est okay !

## Mise en place du serveur DHCP

### Configuration réseau

Nous allons mettre en place les 2 cartes réseaux sur notre serveur DHCP, pour cela nous allons modifier le fichier de configuration

- Nano /etc/network/interfaces

```

auto eth0
iface eth0 inet static
    address 192.168.1.100
    netmask 255.255.255.0
    gateway 192.168.1.1

auto eth1
iface eth1 inet static
    address 192.168.80.105
    netmask 255.255.255.0
    gateway 192.168.80.254

```

Nous ajoutons une carte réseau ETH0 avec comme adresse IP : 192.168.1.100, et avec comme passerelle 192.168.1.1 qui est l'adresse du routeur de notre FAI.

Puis nous ajoutons une carte réseau ETH1 avec comme adresse ip : 192.168.80.105, et avec comme passerelle 192.168.80.254 qui est l'adresse de l'interface de notre router Cisco.

Nous pouvons maintenant redémarrer le service

- `/etc/init.d/networking restart`

Et nous vérifions que la configuration a bien été prise en compte avec la commande « ifconfig »

```

eth0      Link encap:Ethernet  HWaddr 08:00:27:76:b4:2f
          inet adr:192.168.1.100  Bcast:192.168.1.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe76:b42f/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:714 errors:0 dropped:0 overruns:0 frame:0
          TX packets:181 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:254962 (248.9 KiB)  TX bytes:23121 (22.5 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:15:a8:99
          inet adr:192.168.80.105  Bcast:192.168.80.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe15:a899/64 Scope:Lien
          adr inet6: 2a02:8435:6b0:7501:a00:27ff:fe15:a899/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:361 errors:0 dropped:6 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:97004 (94.7 KiB)  TX bytes:13616 (13.2 KiB)

```

## Installation du service

Nous allons maintenant installer le service « isc-dhcp-server »

- `Apt-get update`
- `Apt-get install isc-dhcp-server`

Puis nous allons supprimer les commentaires du fichier de la configuration et le modifier.

- `Cd /etc/dhcp`
- `cp dhcpd.conf dhcpd.back`
- `sed '/^#/d' dhcpd.back > dhcpd.conf`

- nano dhcpd.conf

```
ddns-update-style none;

default-lease-time 600;
max-lease-time 7200;

log-facility local7;

#Réseau BUSINESS
subnet 192.168.30.0 netmask 255.255.255.0 {
    range 192.168.30.1 192.168.30.200;
    option subnet-mask 255.255.255.0;
    option routers 192.168.30.254;
}

#Réseau PCS
subnet 192.168.50.0 netmask 255.255.255.0 {
    range 192.168.50.1 192.168.50.200;
    option subnet-mask 255.255.255.0;
    option routers 192.168.50.254;
}

#Serveur
subnet 192.168.80.0 netmask 255.255.255.0{
}
subnet 192.168.1.0 netmask 255.255.255.0{
}
```

Nous déclarons dans cette configuration :

- Le réseau BUSINESS avec comme tranche d'ip de 192.168.30.1 à 192.168.30.200 et nous indiquons l'adresse du routeur 192.168.30.254.
- Le réseau PCS avec comme tranche d'ip de 192.168.50.1 à 192.168.50.200 et nous indiquons l'adresse du routeur 192.168.50.254.
- Et nous indiquons le réseau des 2 cartes réseaux de notre serveur DHCP (obligatoire pour lancer le service DHCP)

Puis nous configurons le fichier isc-dhcp-server pour indiquer la carte réseau de notre serveur DHCP.

- Nano /etc/default/isc-dhcp-server

```
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="eth1"
```

Puis nous redémarrons le service réseau

- /etc/init.d/networking restart



## Ajout des routes sur le routeur Debian

Le DHCP n'est pas encore accessible pour les postes des 2 VLANS, avec le Routeur Debian ne connaît pas encore le chemin pour accéder aux sous-réseaux, pour cela nous allons modifier le fichier des interfaces et ajouter les routes avec les commandes :

- `ip route add 192.168.30.0/24 via 192.168.80.254 dev eth1`
- `ip route add 192.168.50.0/24 via 192.168.80.254 dev eth1`

## Test du DHCP

Nous allons maintenant tester le DHCP, pour cela nous branchons un ordinateur sur une des interfaces du VLAN BUSINESS sur notre switch, c'est-à-dire une des interfaces entre 1 et 16.

Puis nous tapons la commande :

- `Ipconfig /release`
- `Ipconfig /renew`

Ce qui nous permet de forcer le DHCP.

```
Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . . :
Adresse IPv6 de liaison locale. . . . . : fe80::7d93:10d1:dd42:1e2b%14
Adresse IPv4. . . . . : 192.168.30.1
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.30.254
```

## Activation du routage et du NAT

Nous allons maintenant mettre en place le routage et le NAT sur le serveur Debian qui occupe aussi le serveur DHCP pour ainsi permettre aux postes du Réseau BUSINESS et du Réseau PCS d'avoir accès à internet.

### Activation du routage

- `Nano /etc/sysctl.conf`

Puis nous allons décommenter la ligne « `net.ipv4.ip_forward=1` »

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Et on met à jour les paramètres avec

- `Sysctl -p /etc/sysctl.conf`

```
root@srv-ar-deb:/etc/dhcp# sysctl -p /etc/sysctl.conf
net.ipv4.ip_forward = 1
root@srv-ar-deb:/etc/dhcp#
```

### Activation du nat

Puis nous activons le nat avec la commande :

- iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

### Automatiser le montage du NAT

Pour aller plus loin dans l'activation du nat nous pouvons automatiser cette règle pour éviter de devoir l'écrire à chaque fois que le routeur est redémarré. Pour cela nous allons écrire la commande :

- iptables-save > /etc/iptables\_rules.save

iptables\_rules.save = correspond à un nom que nous avons donné , ce nom n'est pas obligatoire, nous pouvons aussi appeler ce fichier : rulesiptables.save

Après avoir entré cette commande, nous allons ajouter dans le fichier /etc/network/interfaces la ligne de commande :

- post-up iptables-restore < /etc/iptables\_rules.save

Cette commande permet à chaque fois de charger les règles du fichier « iptables\_rules.save »

```
post-up iptables-restore < /etc/iptables_rules.save
```

| Adresse de destination | Masque        | Passerelle     | Interface      |
|------------------------|---------------|----------------|----------------|
| 0.0.0.0                | 0.0.0.0       | 192.168.1.1    | 192.168.1.100  |
| 192.168.1.0            | 255.255.255.0 | 192.168.1.100  | 192.168.1.100  |
| 192.168.80.0           | 255.255.255.0 | 192.168.80.105 | 192.168.80.105 |