

# SAÉ24: Réseau

## Groupe 13

Louis DESVERNOIS, Alexis SCHOENN, Philippe DUBOIS

24 juin 2022

### Table des matières

|          |  |          |
|----------|--|----------|
| <b>1</b> | <b>Création des VLAN et routage inter-VLAN</b> | <b>2</b> |
| 1.1      | VLANs . . . . .                                | 2        |
| 1.2      | Routage inter-VLAN . . . . .                   | 2        |
| <b>2</b> | <b>Mise en place du NAT et ACL</b>             | <b>4</b> |
| 2.1      | NAT . . . . .                                  | 4        |
| 2.2      | DHCP . . . . .                                 | 4        |
| 2.3      | ACL . . . . .                                  | 5        |

### Table des figures

|   |                           |   |
|---|---------------------------|---|
| 1 | sh ip int brief . . . . . | 3 |
|---|---------------------------|---|

### Table des codes

|   |   |   |
|---|---|---|
| 1 | Création d'un VLAN . . . . .                                | 2 |
| 2 | Résultats de "sh vlan brief" . . . . .                      | 2 |
| 3 | Configuration du port trunk . . . . .                       | 2 |
| 4 | Création des interfaces virtuelles sur le routeur . . . . . | 3 |
| 5 | Configuration du NAT . . . . .                              | 4 |
| 6 | Configuration du DHCP . . . . .                             | 4 |
| 7 | ACL présentes sur notre routeur . . . . .                   | 5 |

# 1 Création des VLAN et routage inter-VLAN

## 1.1 VLANs

Pour commencer nous avons dû créer quatre VLAN sur notre switch ainsi que de mettre en place le routage inter-VLAN. Nous avons donc d'abord créé ces VLAN avec les commandes ci-dessous.

```
Switch(config)#int range fastEthernet 0/1-4
Switch(config-if-range)#sw mode access
Switch(config-if-range)#sw access vlan 10
% Access VLAN does not exist. Creating vlan 10
```

Code 1 – Création d'un VLAN

Nous avons répété les commandes en code 1 quatre fois en utilisant quatre interfaces par VLAN ainsi que les numéros 10, 20, 30 et 40. Nous avons ensuite donné des noms à ces VLAN avec les commandes `vlan <no>` puis `name <nom>` en mode configuration.

| VLAN Name               | Status | Ports  |
|-------------------------|--------|--|
| 1 default               | active | Fa0/17, Fa0/18, Fa0/19, Fa0/20<br>Fa0/21, Fa0/22, Fa0/23, Fa0/24<br>Gig0/1, Gig0/2 |
| 10 voix                 | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4   |
| 20 users                | active | Fa0/5, Fa0/6, Fa0/7, Fa0/8   |
| 30 server               | active | Fa0/9, Fa0/10, Fa0/11, Fa0/12  |
| 40 admin                | active | Fa0/13, Fa0/14, Fa0/15, Fa0/16   |
| 1002 fddi-default       | active |  |
| 1003 token-ring-default | active |  |
| 1004 fddinet-default    | active |  |
| 1005 trnet-default      | active |  |

Code 2 – Résultats de "sh vlan brief"

## 1.2 Routage inter-VLAN

Une fois les VLAN correctement créés, nous avons besoin de configurer le routage inter-VLAN en utilisant l'encapsulation dot1Q. Pour cela, sur notre switch, nous avons choisi le port Fa0/24 comme port trunk.

```
Switch(config)#int fastEthernet 0/24
Switch(config-if)#sw mode trunk
Switch(config-if)#sw trunk allowed vlan 10,20,30,40
```

Code 3 – Configuration du port trunk

Le trunk étant activé, nous pouvons à présent créer les interfaces virtuelles sur le routeur. Nous avons besoin d'en créer quatre, une par VLAN. Au niveau de nos adresses IP, étant le groupe 13, nous pouvons utiliser les réseaux 172.113.x.0/24 avec x le numéro de VLAN. Les adresses choisies pour les gateways et les SVI seront respectivement la dernière et l'avant-dernière adresse de chaque réseau.

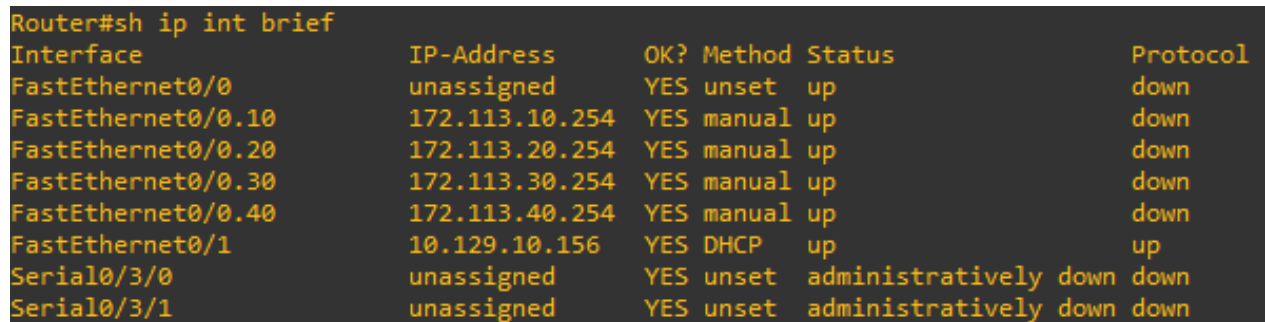
```

interface FastEthernet0/0
  no ip address
!
interface FastEthernet0/0.10
  encapsulation dot1Q 10
  ip address 172.113.10.254 255.255.255.0
!
interface FastEthernet0/0.20
  encapsulation dot1Q 20
  ip address 172.113.20.254 255.255.255.0
!
interface FastEthernet0/0.30
  encapsulation dot1Q 30
  ip address 172.113.30.254 255.255.255.0
!
interface FastEthernet0/0.40
  encapsulation dot1Q 40
  ip address 172.113.40.254 255.255.255.0

```

Code 4 – Création des interfaces virtuelles sur le routeur

Nous pouvons également en profiter pour configurer l'interface connectée à Internet en DHCP avec la commande `ip address dhcp` en mode configuration d'interface.



| Interface          | IP-Address     | OK? | Method | Status                | Protocol |
|--------------------|----------------|-----|--------|-----------------------|----------|
| FastEthernet0/0    | unassigned     | YES | unset  | up                    | down     |
| FastEthernet0/0.10 | 172.113.10.254 | YES | manual | up                    | down     |
| FastEthernet0/0.20 | 172.113.20.254 | YES | manual | up                    | down     |
| FastEthernet0/0.30 | 172.113.30.254 | YES | manual | up                    | down     |
| FastEthernet0/0.40 | 172.113.40.254 | YES | manual | up                    | down     |
| FastEthernet0/1    | 10.129.10.156  | YES | DHCP   | up                    | up       |
| Serial0/3/0        | unassigned     | YES | unset  | administratively down | down     |
| Serial0/3/1        | unassigned     | YES | unset  | administratively down | down     |

FIGURE 1 – sh ip int brief

Comme nous pouvons le voir en Figure 1, le routeur a bien récupéré une adresse IP avec DHCP et nos interfaces virtuelles ont correctement été configurées<sup>1</sup>.

1. Le protocole est en "down" sur Fa0/0 car au moment de la prise de la capture d'écran, un câble cassé était utilisé

## 2 Mise en place du NAT et ACL

### 2.1 NAT

Comme nous désirons utiliser Internet sur notre réseau, il est nécessaire de mettre en place un NAT. Pour cela, nous avons d'abord besoin de spécifier quelles interfaces se situent à l'intérieur du NAT et lesquelles sont à l'extérieur. Nous allons exécuter la commandes `ip nat inside` sur toutes les interfaces virtuelles et la commande `ip nat outside`. Ensuite, il est nécessaire de créer un ACL "permit" avec toutes les adresses source qui seront traduites par le routeur.

```
Router(config)#ip access-list standard NAT
Router(config-std-nacl)#permit 172.113.0.0 0.0.255.255
Router(config-std-nacl)#exit
Router(config)#int fastEthernet 0/0.10
Router(config-subif)#ip nat inside
Router(config-subif)#int fastEthernet 0/0.20
Router(config-subif)#ip nat inside
Router(config-subif)#int fastEthernet 0/0.30
Router(config-subif)#ip nat inside
Router(config-subif)#int fastEthernet 0/0.40
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)#ip nat inside source list NAT interface fastEthernet 0/1
```

Code 5 – Configuration du NAT

Une fois les commandes en code 5 sont exécutées et que les interfaces des PC sont correctement configurées, nous devrions être capables de nous connecter à Internet sur notre réseau.

### 2.2 DHCP

Maintenant que notre NAT est mis en place, il serait intéressant de configurer le DHCP dans notre réseau. Pour cela, nous allons utiliser notre Switch, qui est capable d'agir en tant que serveur DHCP.

```
Switch(config)#ip dhcp excluded-address 172.113.20.254
Switch(config)#ip dhcp excluded-address 172.113.40.254
Switch(dhcp-config)#ip dhcp pool vlan20
Switch(dhcp-config)#network 172.113.20.0 255.255.255.0
Switch(dhcp-config)#default-router 172.113.20.254
Switch(dhcp-config)#ip dhcp pool vlan40
Switch(dhcp-config)#network 172.113.40.0 255.255.255.0
Switch(dhcp-config)#default-router 172.113.40.254
```

Code 6 – Configuration du DHCP

Les VLAN 10 et 30 ne sont pas configurés, car ceux-ci ne doivent pas utiliser le DHCP, en effet le DHCP du PABX présent sur le VLAN 10 entre en conflit et les serveurs du VLAN 30 sont configurés en statique.

## 2.3 ACL

Nous avons dû implémenter des ACL pour limiter les actions des utilisateurs des différents VLAN. Voici toutes les ACL que nous avons mis en place :

- ACL pour bloquer un site de commerce sur le VLAN users
- ACL pour bloquer l'accès au serveur FTP pour tous les utilisateurs
- ACL pour empêcher les utilisateurs la connexion aux utilisateurs du VLAN admin
- ACL pour que le VLAN voix ai uniquement accès a son opérateur public ayant l'IP 10.129.10.20

```
Router#sh access-list
Standard IP access list NAT
  10 permit 172.113.0.0, wildcard bits 0.0.255.255 (6034 matches)
Extended IP access list cdiscount
  10 deny ip host 204.74.99.103 172.113.20.0 0.0.0.255 (33 matches)
  20 permit ip any any (235882 matches)
Extended IP access list no-ftp
  10 permit tcp 172.113.40.0 0.0.0.255 host 172.113.30.1 eq ftp (60 matches)
  20 deny tcp any host 172.113.30.1 eq ftp (47 matches)
  30 permit ip any any (6159 matches)
Extended IP access list userBlockAdmin
  10 permit icmp 172.113.40.0 0.0.0.255 172.113.20.0 0.0.0.255 (33 matches)
  20 deny icmp 172.113.20.0 0.0.0.255 any echo
  30 permit icmp 172.113.20.0 0.0.0.255 any echo-reply
  40 permit tcp 172.113.20.0 0.0.0.255 any established
  50 deny tcp 172.119.20.0 0.0.0.255 any
  60 permit ip any any (2108 matches)
Extended IP access list voix-no-internet
  10 permit ip 172.113.10.0 0.0.0.255 host 10.129.10.20 (49912 matches)
  20 deny ip any any (5607 matches)
```

Code 7 – ACL présentes sur notre routeur

Les ACL présentées en code 7 sont ensuite appliquées en entrée ou en sorties sur les différentes interfaces avec les commandes `ip access-group <nom_acl> in` et `ip access-group <nom_acl> out` en mode configuration d'interfaces. Nous les avons appliquées comme suit.

- ACL `cdiscount` en *out* sur Fa0/0.20
- ACL `no-ftp` en *out* sur Fa0/0.30
- ACL `userBlockAdmin` en *in* sur Fa0/0.40
- ACL `voix-no-internet` en *in* sur Fa0/0.10