

ECAM

Computer Network Labs

Routing Labs – IPv4 : Rapport

Jardinet Louis, Van Olffen Victor, Dufour Arthur
08/12/2024

Table des matières

1. Introduction	1
2. Câblage.....	2
3. Configuration.....	3
3.1 Création des VLANs	3
3.2 Vérification des connexions sur un seul routeur.....	4
3.3 Communication avec les autres routeurs	4
3.4 Routes Statiques	5
3.5 Vérification de l'interconnexion	6
4. Connexion à internet et configuration du NAT	7
4.1 Connexion depuis un autre routeur.....	7
4.2 Connexion de l'interface de notre routeur et de la passerelle par défaut.....	7
4.3 Mise en place du NAT.....	8
5. Conclusion.....	10

1. Introduction

Dans le cadre du laboratoire de Computer Networks, nous avons étudié le routage en IPv4. Nous avons créé un réseau informatique composé de trois groupes interconnectés, avec un routeur et deux ordinateurs chacun, représenté à la Figure 1.

D'abord, nous avons mis en place nos 2 sous-réseaux en configurant le routeur ainsi que des adresses IPv4. Ensuite, nous avons interconnecté notre routeur avec ceux des autres groupes. Finalement, nous avons été capable d'aller sur internet en configurant le NAT (Network Address Translation) et grâce à un fournisseur connecté par câble à notre routeur.

Au cours de ce rapport, nous allons voir en détail les différentes étapes qui nous ont permis de réaliser ce réseau, communiquer entre les machines et surfer sur internet. Nous représenterons le groupe dans le VLAN 32.

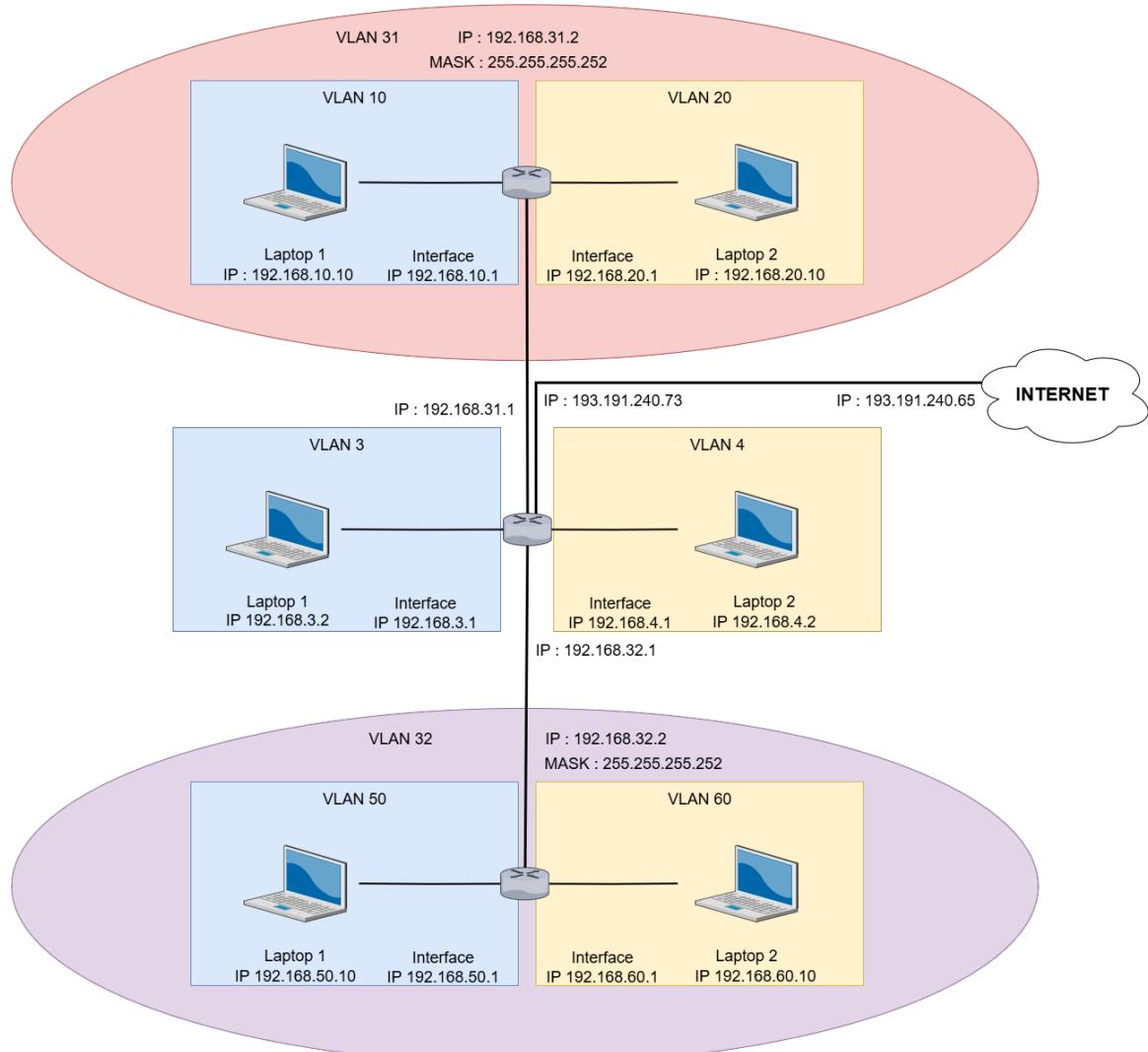


Figure 1: Vue de notre réseau informatique

2. Câblage

Notre matériel pour ce laboratoire est composé d'un routeur et de deux câbles Ethernet reliés à nos deux ordinateurs, visibles sur la Figure 2. Le routeur Cisco est composé d'un switch intégré et est connecté à un troisième ordinateur à l'aide d'un câble COM (câble bleu clair). Chaque groupe dispose de ce même matériel, ainsi que des câbles Ethernet supplémentaires pour connecter nos routeurs entre eux.

On aperçoit sur l'image ci-dessous qu'on utilise les ports FastEthernet 0, 1 et 3 de notre routeur.

Nos deux ordinateurs sont connectés aux FastEthernet 0 et 1, tandis que le FastEthernet 3 est connecté au routeur d'un autre groupe sur le réseau.

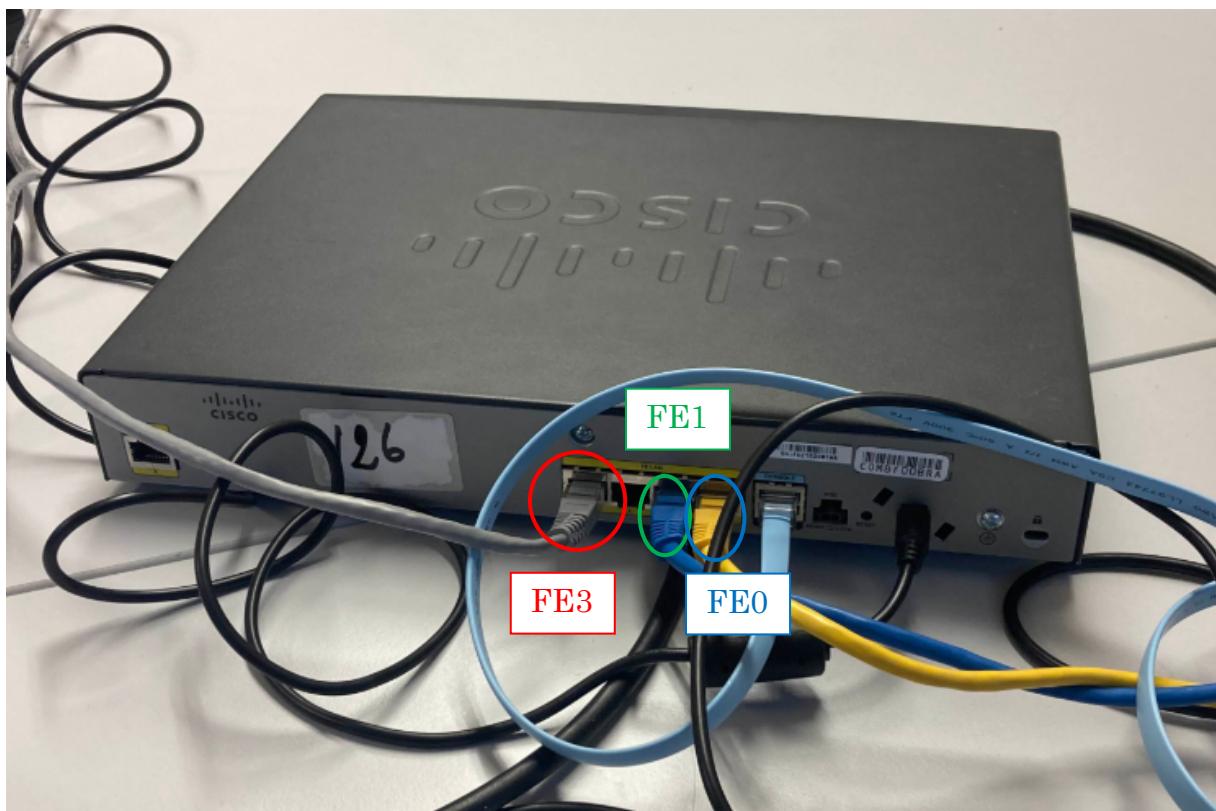


Figure 2: Câblage de notre routeur

3. Configuration

Nous ne verrons pas en détail la configuration des adresses IPv4 sur nos ordinateurs car nous avons déjà expliqué cette étape dans le dernier rapport, ainsi que la connexion au routeur en utilisant PuTTY.

Pour rappel, il existe deux types d'adresses pour les appareils connectés à un réseau : IPv4 et IPv6. Ce sont des identifiants uniques pour chaque appareil et qui leur permet de communiquer entre eux. Nous ne parlerons que des IPv4 dans ce rapport.

Pour notre groupe, nous avons choisi les adresses IPv4 suivantes :

- 192.168.50.10 (laptop 1)
- 192.168.60.10 (laptop 2)

Les passerelles par défaut associées seront :

- 192.168.50.1 (laptop 1)
- 192.168.60.1 (laptop 2)

Le masque de sous-réseau sera 255.255.255.0 pour chaque ordinateur. Les adresses des ordinateurs sur les autres routeurs sont indiquées sur la Figure 1.

Nous allons d'abord configurer notre sous-réseau et ensuite nous connecter aux autres routeurs.

3.1 Création des VLANs

Pour commencer, nous devons créer des VLANs dans lesquels nous assignerons nos passerelles par défaut. Plutôt que d'assigner directement nos adresses aux ports FastEthernet, il est nécessaire d'assigner chaque interface du routeur à un VLAN pour garantir que la communication entre les différents ports se passe via le routeur et non via le switch.

On utilise les commandes suivantes pour :

- Crée le **VLAN 5** et y assigner l'adresse du **laptop1**
- Crée le **VLAN 6** et y assigner l'adresse du **laptop2**

```
Router(config)#vlan 5
Router(config)#vlan 6
Router(config)#interface vlan 5
Router(config-if)#ip address 192.168.50.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface vlan 6
Router(config-if)#ip address 192.168.60.1 255.255.255.0
```

Ensuite, on assigne ces deux VLAN aux ports FastEthernet que nous utilisons sur nos ordinateurs (0 et 1) :

```
Router(config)#interface fa00
Router(config-if)#switchport access vlan 5
Router(config)#interface fa01
Router(config-if)#switchport access vlan 6
```

La Figure 3 nous montre le statut des interfaces ainsi que des adresses IP assignées.

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0	unassigned	YES	unset	up	up
FastEthernet1	unassigned	YES	unset	up	up
FastEthernet2	unassigned	YES	unset	down	down
FastEthernet3	unassigned	YES	unset	up	up
FastEthernet4	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	down	down
Vlan5	192.168.50.1	YES	manual	up	up
Vlan6	192.168.60.1	YES	manual	up	up

Figure 3: Visibilité des VLANs ainsi que de leurs adresses IP

Il maintenant est nécessaire de vérifier notre configuration avant d'aller plus loin.

3.2 Vérification des connexions sur un seul routeur

Afin de vérifier que les configurations ont été réalisées correctement, on peut envoyer un ping du laptop1 vers le laptop2, et inversement (Figure 4).

```
PS C:\Users\Dufour> ping 192.168.60.10

Pinging 192.168.60.10 with 32 bytes of data:
Reply from 192.168.60.10: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.60.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Figure 4: Ping du laptop1 vers le laptop2

Maintenant que notre routeur est fonctionnel avec les machines directement connectées, nous devons nous connecter aux routeurs des autres groupes.

3.3 Communication avec les autres routeurs

Plus tôt dans ce rapport (**2. Câblage**), nous avons mentionné que le port FastEthernet 3 de notre routeur était connecté au routeur d'un autre groupe. Si

nous voulons communiquer avec les autres ordinateurs qui se trouvent sur notre réseau, nous devons configurer ce port en suivant les mêmes étapes qu'au point **3.1** Crédit des VLANs. Nous devons donc créer un nouveau VLAN qui sera assignée au FE3, avec l'adresse IP 192.168.32.2 qui est celle du routeur connecté au nôtre :

```
Router(config)#vlan 7
Router(config-vlan)#exit
Router(config)#interface fa03
Router(config-if)#switchport access vlan 7
Router(config)#interface vlan 7
Router(config-if)#ip address 192.168.32.2 255.255.255.252
```

Une fois que nous avons configuré le VLAN 7 nous pouvons vérifier la visibilité des tous les VLANs dans notre routeur (Figure 5).

```
Router#show ip interface brief
*Feb  6 08:17:10.075: %SYS-5-CONFIG_I: Configured from console by console
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0      unassigned     YES unset  up           up
FastEthernet1      unassigned     YES unset  up           up
FastEthernet2      unassigned     YES unset  down         down
FastEthernet3      unassigned     YES unset  up           up
FastEthernet4      unassigned     YES unset  administratively down down
Vlan1              unassigned     YES unset  down         down
Vlan5              192.168.50.1   YES manual up           up
Vlan6              192.168.60.1   YES manual up           up
Vlan7              192.168.32.2   YES manual up           up
Router#
```

Figure 5: Visibilité du VLAN 7 et de son adresse IP dans les interfaces du routeur

```
Router#sh vlan-switch
-----
```

VLAN	Name	Status	Ports
1	default	active	Fa2
5	VLAN0005	active	Fa0
6	VLAN0006	active	Fa1
7	VLAN0007	active	Fa3

Figure 6 : Liaison entre chaque port et son VLAN

La connexion avec le routeur central (Figure 1) est établie mais pour pouvoir communiquer avec les ordinateurs de chaque sous-réseau, il faut spécifier des routes statiques à notre routeur.

3.4 Routes Statiques

Les routes statiques permettent d'indiquer à notre routeur par où passer pour pouvoir communiquer avec une passerelle par défaut en dehors du sous-réseau. Elle est constituée de [l'adresse de la passerelle] à atteindre suivie du [masque de sous-réseau] en passant par [l'adresse interco du prochain routeur], représenté ici par le routeur central.

Dans le routage statique, les routes sont donc fixes et définies manuellement tandis que dans le routage dynamique, des protocoles mettent automatiquement à jour les tables de routage si le réseau présente des changements.

```
Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.32.1
Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.32.1
```

Figure 7: Configuration des routes statiques

Une fois les routes statiques mises en place, les passerelles par défaut des autres groupes sont accessibles et nous pouvons vérifier les routes avec un ping vers leurs ordinateurs.

3.5 Vérification de l'interconnexion

Nous pouvons maintenant vérifier la communication avec les autres ordinateurs qui se trouvent sur notre réseau (Figure 8).

```
PS C:\Users\vanol> ping 192.168.3.1

Envoi d'une requête 'Ping' 192.168.3.1 avec 32 octets de données :
Réponse de 192.168.3.1 : octets=32 temps<1ms TTL=254

Statistiques Ping pour 192.168.3.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
PS C:\Users\vanol> ping 192.168.3.2

Envoi d'une requête 'Ping' 192.168.3.2 avec 32 octets de données :
Réponse de 192.168.3.2 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 192.168.3.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

Figure 8: Envoi de ping vers les ordinateurs sur le même réseau, mais connectés à des routeurs différents

```

Router#show ip route
Codes: L - local, C - connected, S - static, 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
      i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
      a - application route
      + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

S      192.168.3.0/24 [1/0] via 192.168.32.1
S      192.168.4.0/24 [1/0] via 192.168.32.1
S      192.168.10.0/24 [1/0] via 192.168.32.1
S      192.168.20.0/24 [1/0] via 192.168.32.1
      192.168.32.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.32.0/30 is directly connected, Vlan7
L          192.168.32.2/32 is directly connected, Vlan7
      192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.50.0/24 is directly connected, Vlan5
L          192.168.50.1/32 is directly connected, Vlan5
--More-- 

```

Figure 9 : État du routage statique entre les machines

4. Connexion à internet et configuration du NAT

La prochaine étape est d'accéder à internet grâce à une connexion par câble à un fournisseur et en configurant un NAT sur notre routeur.

4.1 Connexion depuis un autre routeur

Nous avons d'abord configuré internet en passant par le routeur de l'autre groupe. Pour cela, il suffisait de configurer une route statique vers internet : 0.0.0.0/0

```

Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.32.1

```

Figure 10 : Configuration de la route vers internet

L'autre groupe s'occupait de la connexion entre son routeur et internet. Nous avons ensuite échangé les rôles et récupéré cette connexion sur notre routeur.

4.2 Connexion de l'interface de notre routeur et de la passerelle par défaut

Pour pouvoir raccorder notre routeur à internet, nous avons d'abord raccordé l'interface fastEthernet4 à un autre routeur qui aura le rôle d'Internet Service Provider (ISP). Nous devons donc configurer cette interface avec l'adresse 193.191.240.73 et avec un masque 255.255.255.0.

```
Router(config)#interface fa04  
Router(config-if)#ip address 193.191.240.73 255.255.255.0
```

Ensuite, nous avons configuré la passerelle par défaut. C'est la passerelle que vont emprunter les paquets dont le destinataire n'est pas dans la table de routage du routeur. Nous devons donc la reconfigurer, car ce n'est plus le routeur de l'autre groupe, ce dernier n'étant pas connecté à internet.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 193.191.240.65
```

De cette façon, tous les paquets à destination d'un réseau internet 0.0.0.0/0 passeront par la passerelle 193.191.240.65.

4.3 Mise en place du NAT

Finalement, afin d'accéder à Internet, nous devons configurer un NAT (Network Address Translation) qui va gérer les communications entre notre réseau local privé et un réseau public (Internet).

En effet, nous ne pouvons pas directement accéder à internet avec une adresse IP privée. Elles sont réservées à une utilisation locale sur un réseau privé et ne sont donc pas routables sur Internet.

À l'origine, chaque machine recevait une adresse IPv4 publique unique, mais avec la croissance exponentielle des objets connectés à internet, nous sommes rapidement tombés à cours d'adresses IPv4. Pour remédier à ce problème, le NAT a été créé. Lorsqu'ils passent par du réseau interne vers le réseau externe, le NAT va donc modifier les adresses IP privées des paquets en adresses IP publiques. De cette manière, plusieurs machines peuvent partager une seule adresse IP publique pour se connecter à internet.

Lorsqu'on travaille avec du NAT, il est nécessaire de définir quels sont les réseaux internes et externes avec les commandes « **ip nat inside** » et « **ip nat outside** »

```
Router(config)#int vlan5  
Router(config-if)#ip nat inside  
Router(config-if)#exit  
Router(config)#int vlan6  
Router(config-if)#ip nat inside  
Router(config-if)#exit  
Router(config)#int vlan7  
Router(config-if)#ip nat inside  
Router(config-if)#exit
```

Figure 11: Configuration du NAT pour les réseaux internes

```

Router(config)#int fast 4
Router(config-if)#ip nat out
Router(config-if)#ip nat outside

```

Figure 12: Configuration du NAT pour le réseau externe

Finalement, pour mettre en place la traduction des adresses privées en adresses publiques, il reste à effectuer les commandes :

```

Router(config)#access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)#ip nat inside source list 1 interface FastEthernet4 overload

```

La première commande crée une ACL (Access Control List) avec le numéro 1. Elle sert à définir une règle qui autorise le trafic venant de la plage d'adresses IP 192.168.0.0/16. Comme tous nos réseaux sont dans cette range d'adresses, tous les appareils que nous avons connectés pourront accéder à Internet.

La deuxième commande configure le NAT avec la surcharge (overload) :

- **source list 1** : fait référence à l'ACL créée précédemment qui autorise le trafic de la plage d'adresses IP 192.168.0.0/16.
- **interface fastEthernet4** : spécifie que l'adresse IP publique de l'interface FastEthernet4 du routeur sera utilisée pour le trafic qui sort vers Internet.
- **overload** : permet de traduire plusieurs adresses privées en une seule adresse publique en utilisant des ports logiques différents pour distinguer les connexions.

Cette configuration permet donc à tous les appareils du réseau interne de partager une seule adresse IP publique pour accéder à Internet.

Il ne nous reste donc plus qu'à vérifier que tout fonctionne via un ping vers google.com dont l'adresse IP est 8.8.8.8. On peut ensuite effectuer la commande tracert afin de visualiser par quels réseaux passent les paquets envoyés à google.com (Figure 13 et Figure 14).

```

PS C:\Users\vanol> ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=2 ms TTL=57
Réponse de 8.8.8.8 : octets=32 temps=2 ms TTL=57
Réponse de 8.8.8.8 : octets=32 temps=2 ms TTL=57
Réponse de 8.8.8.8 : octets=32 temps=3 ms TTL=57

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

```

Figure 13 : Ping vers google.com

```

PS C:\Users\Dufour> tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

 1      1 ms      1 ms      1 ms  192.168.50.1
 2      1 ms      1 ms      1 ms  193.191.240.65
 3     52 ms      1 ms      1 ms  hevinci_brueve_01_bll.bsr.belnet.net [193.191.5.1]
 4      2 ms      8 ms      2 ms  r1.brueve.belnet.net [193.191.5.197]
 5      8 ms      2 ms      2 ms  10.28.17.201
 6      4 ms      4 ms      4 ms  72.14.213.200
 7      3 ms      3 ms      3 ms  142.251.253.185
 8      3 ms      3 ms      3 ms  142.251.246.111
 9      3 ms      2 ms      3 ms  dns.google [8.8.8.8]

Trace complete.

```

Figure 14: Routage des paquets vers google.com

On remarque donc qu'ils passent bien par la passerelle par défaut 193.191.240.65 configurée précédemment.

On constate ci-dessous que le NAT a bien fonctionné et que notre machine a maintenant l'adresse IPv4 publique 193.191.240.73.

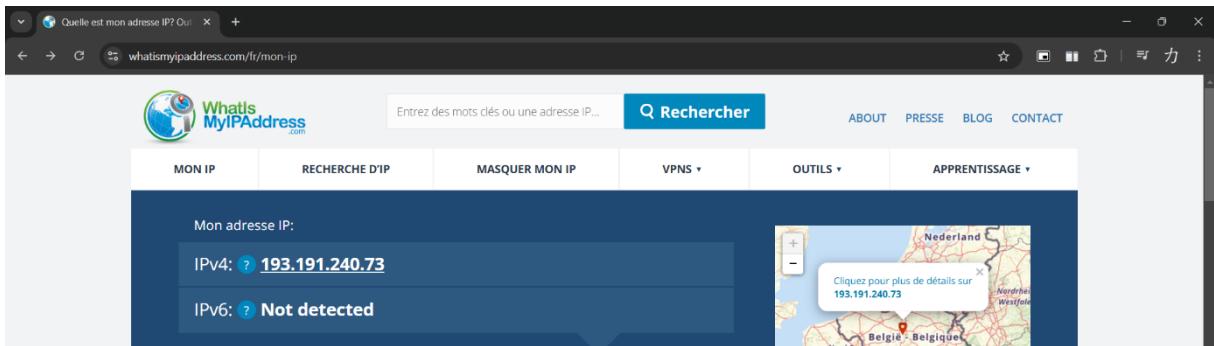


Figure 15 : Adresse IPV4 publique de notre machine

5. Conclusion

En résumé, au cours de ce laboratoire, nous avons configuré un routeur en IPv4. Nous avons établi une communication entre deux ports de ce routeur via un routage statique en configurant les deux interfaces avec des adresses IPv4 distinctes dans des VLANs différents.

L'utilisation des routes statiques nous a ensuite permis de nous connecter aux autres routeurs sur notre réseau et d'établir une connexion à internet. Nous avons également configuré la connexion d'un réseau local à internet en utilisant le NAT.

La configuration du réseau mise en place lors de ce labo est une structure de réseaux couramment retrouvée en entreprise, où plusieurs appareils sont reliés à un routeur central pour accéder à internet. Ce laboratoire nous a permis d'acquérir des compétences pratiques dans la gestion d'un réseau IPv4.