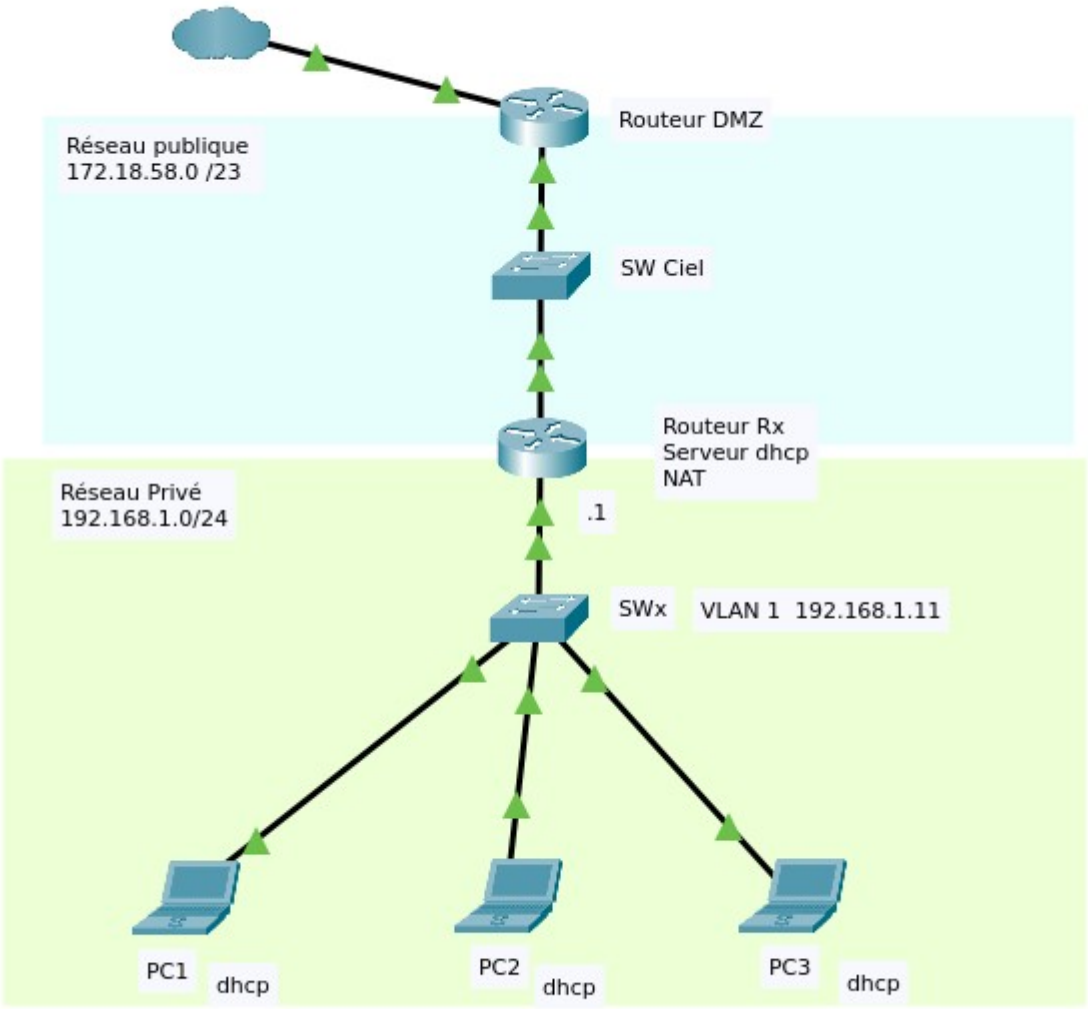
TP mise en place d’un NAT entre deux réseaux

Le NAT, ou "Network Address Translation", constitue une solution efficace aux défis de routage rencontrés lorsqu'il s'agit de connecter un réseau dit "privé" (que nous contrôlons) à un réseau "public" (dont nous ne pouvons modifier la configuration). Lorsqu'il est implémenté sur un routeur reliant ces deux types de réseaux, son rôle est de faire en sorte que toutes les requêtes provenant du réseau privé (désigné ici comme le LAN) apparaissent comme émanant directement du routeur lui-même, et non d'un dispositif interne avec un adressage différent. Le NAT est particulièrement utile pour répondre à la problématique suivante :

Une autre fonction du du NAT est de **sécuriser** une partie du réseau en la cachant à une autre partie. Cela est utile en terme de sécurité quand un réseau privé est adjacent à un réseau public et que l’on peut voir ce réseau local depuis le réseau public. Plus clairement, le routeur R2 va **changer toutes les trames IP provenant du LAN** en mettant comme **IP source** son IP sur le réseau WAN. Cela permettra de ne pas divulguer des IP du LAN à d'autres éléments du réseau et également de faire en sorte ces paquets reviennent (car l'IP source sera sur un réseau connus des autres éléments du réseau).



Le principe du NAT est simple, le routeur fait office de barrière entre le réseau outside (celui qualifié de publique) et le réseau inside (celui qui est privé). Ainsi chaque requête provenant du réseau inside vers l'outside sera cachée par le NAT du routeur.
On dit qu'une NAT est dynamique lorsque les adresses sources (ici venant du privé) sont translaté de façon dynamique (par des ports différents ou par des IP différentes si on en dispose) vers l'interfaces de sorties (ici publique). Le routeur remplie sa table NAT de façon dynamique à l'inverse du NAT statique ou les translations sont saisies et enregistrés à l'avance.

1) Configurer le serveur DHCP sur le routeur CISCO

Configurer un serveur DHCP sur le routeur Cisco pour attribuer dynamiquement des adresses IP aux clients du réseau privé.

Paramètres :

- **Réseau :** 192.168.1.0/24
- **Plage d'adresses exclues :** 192.168.1.1 - 192.168.1.15 et 192.168.1.200 - 192.168.1.254
- **Durée du bail :** 1 heure
- **Serveur DNS :** 8.8.8.8

2) Configuration du NAT

On doit indiquer quelle interface sera à l'intérieur du NAT **("inside")** et quelle interface sera à l'extérieur **("outside").**

Mettre l'interface Fa0/0 en "inside" du point de vue du NAT

```
R2(config)#interface fa0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
```

Mettre l'interface Fa0/1 en "outside" du point de vue du NAT

```
R2(config)#interface fa0/1
R2(config-if)#ip nat outside
R2(config-if)#exit
```

On va ensuite définir une liste de contrôle d'accès (ACL) numérotée **1** qui **autorise** les paquets provenant de n'importe quelle adresse IP dans le sous-réseau **192.168.1.0/24**.

```
R2(config)#access-list 1 permit 192.168.1.0   0.0.0.255
```

`0.0.0.255` → Wildcard mask, qui signifie que toutes les adresses comprises entre **192.168.1.0 et 192.168.1.255** sont concernées.

Mettre en place NAT

```
R2(config)#ip nat inside source list 1 interface fa0/1 overload
```

Explication de la commande :

1. **`ip nat inside source`** → Configure la traduction d'adresses pour les adresses sources venant de l'interface marquée comme `inside` (côté réseau privé).
2. **`list 1`** → Indique que seules les adresses correspondant à l'ACL (Access Control List) numéro **1** seront traduites.
3. **`interface fa0/1`** → Utilise l'adresse IP de l'interface **FastEthernet 0/1** (sortie vers Internet) comme adresse source pour la traduction.
4. **`overload`** → Active le **PAT (Port Address Translation)**, ce qui permet à plusieurs adresses IP privées d'être traduites en une seule adresse IP publique en différenciant les connexions grâce aux numéros de ports.

C'est une méthode couramment utilisée pour permettre à plusieurs appareils d'un réseau local d'accéder à Internet avec une seule adresse IP publique.

3) Vérifications

S'assurer que les PC du réseau privée ping bien le routeur DMZ (172.18.58.9)
Ensuite vérifier que la résolution d’adresse se fait correctement (avec la commande nslookup google.fr)
pour terminer ouvrir la page d’accueil de google.fr avec un navigateur sur un PC du réseau privé.