



REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE  
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA  
RECHERCHE SCIENTIFIQUE  
ECOLE NATIONALE SUPERIEURE D'INFORMATIQUE

CS 1

## PROJET RES2

**‘Migration Ipv6 d’un réseau d’entreprise ’  
-partie 01: Mise en place du NAT-**

**REALISE PAR L'EQUIPE N° 32 :**

- **AZIZ Rezak**
- **MOHAMED ISSAM DAUD BEN  
MESSAOUD**
- **MECHOUEK Lounes**
- **FODIL Zine-eddine (CE)**

**Année 2019 / 2020**

## Table des matières

<b>I.</b>	<b>Introduction.....</b>	<b>3</b>
<b>II.</b>	<b>Définition SSII et Roles.....</b>	<b>4</b>
<b>III.</b>	<b>Mise en place de la topologie :.....</b>	<b>8</b>
1.	Plan d’adressage : .....	8
2.	Configuration des différents routeurs et machines : .....	11
<b>IV.</b>	<b>Mise en place de NAT :.....</b>	<b>13</b>
1.	Choix du NAT a utilisé .....	13
2.	Mise en place de NAT et PAT :.....	14
<b>V.</b>	<b>Tests : .....</b>	<b>17</b>
1.	Test N°01 : .....	19
2.	Test N°02 : .....	20
3.	Test N°03 : .....	21
4.	Test N°04 : .....	22
5.	Test N°05 : .....	23
6.	Test N°06 : .....	25
7.	Test N°07 : .....	26
8.	Test N°08 : .....	27
<b>VI.</b>	<b>Conclusion .....</b>	<b>29</b>

## I. Introduction

Le NAT (*Network address translation*) est une fonction implémentée sur les routeurs d'un réseau informatique. Cette fonction permet de répondre à une principale problématique :

Comment faire face à la pénurie d'adresses IP sur Internet ?

En effet les adresses IPv4 étant codées sur 32 bits, nous arrivons actuellement à la limite du nombre maximal d'adresses publiques attribuables. Bien sûr, le nouveau standard de protocole IP « IPv6 » (*que nous détaillerons par la suite*) est actuellement mis en place au niveau mondial pour résoudre ce problème de manque d'adresses. Néanmoins, le NAT reste la référence si l'on souhaite continuer à exploiter l'IPv4.

Le principe est relativement simple, il s'agit de réduire au strict minimum l'utilisation des adresses IPv4 en attribuant la plage d'adresses la plus réduite possible aux demandeurs. A partir de là, la question naturelle qui se pose est : Que se passe-t-il si l'on dispose d'un nombre important de machines à héberger sur Internet ?

C'est bien là que réside tout l'intérêt du NAT. Ce dernier peut être assimilé à un dictionnaire ; le routeur de sortie du réseau se charge de faire correspondre à chaque adresse privée du réseau une des adresses publiques fournies par son ISP en suivant l'une des méthodes de NAT (*Nat statique, Nat dynamique ou PAT*).

Notre rôle dans cette partie (en plus de la configuration des tables de routage des routeurs) a consisté dans un premier temps à définir les routeurs qui allaient assurer la fonction NAT pour chaque réseau. Nous avons ensuite déterminé le type de NAT adéquat pour chacun de ces réseaux avant d'attribuer les adresses publiques correspondant à chaque groupe d'adresses privées de chaque réseau.

## II. Définition SSII et Rôles :

### Présentation de la SSII :

**SolNet** est une entreprise de services et ingénieurs en informatique, elle a été fondée par quatre ingénieurs issus de l'Ecole Nationale Supérieure en Informatique en 2014 :

- AZIZ REZAK
- MOHAMED ISSAM DAOUD BEN MESSAOUD
- MECHOUK LOUNES
- FODIL ZINE-EDDINE

SolNet est une entreprise étendue, donc, une entreprise pilote qui prend les qualificatifs suivants :

- ✓ Entreprise maître d'œuvre
- ✓ Entreprise tête de réseau
- ✓ Entreprise chef de projet

Nous offrons plusieurs services tels : Conception, Réalisation, maintenance dans le domaine des TIC. Le principal objectif de SolNet est de répondre rigoureusement aux besoins des clients et leurs offrir la meilleure prestation.

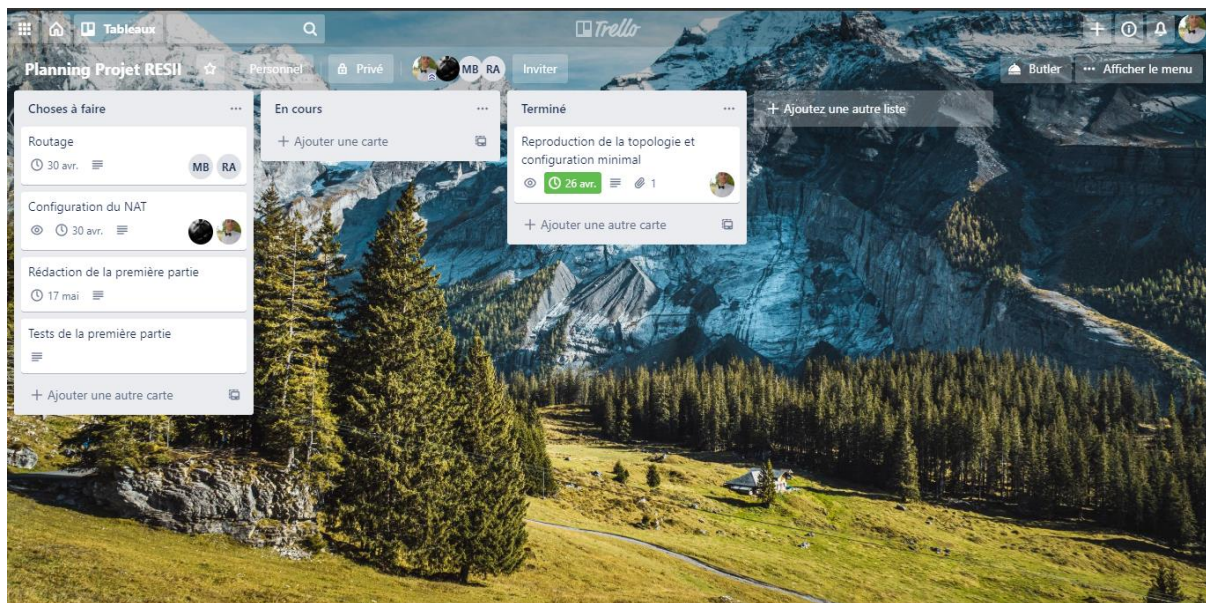


### Répartition des tâches :

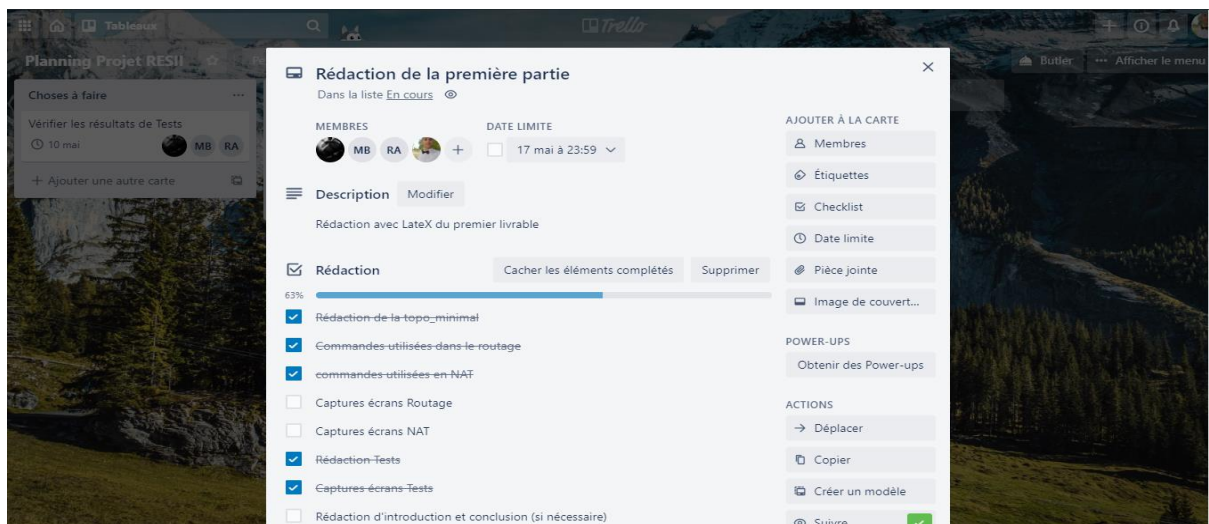
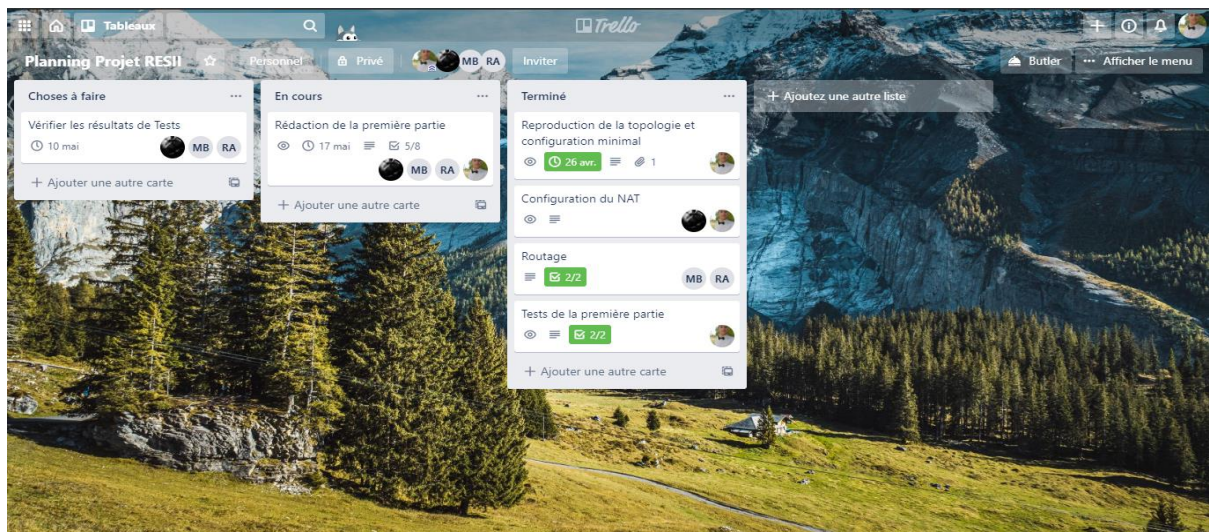
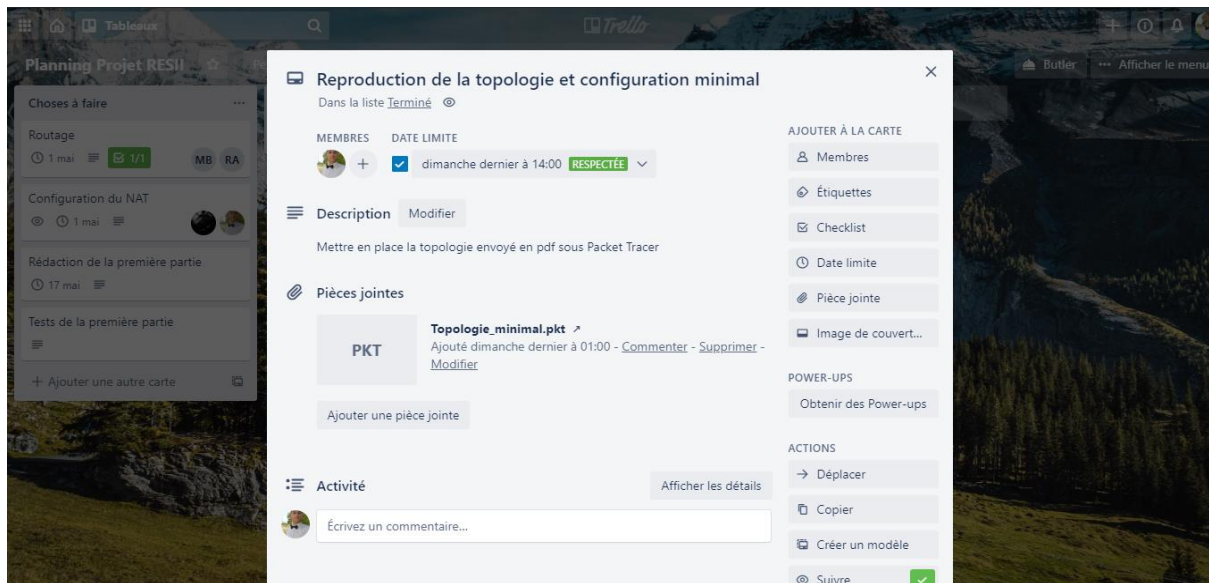
Pour le bon déroulement de projet, nous, l'équipe du projet, avons été amenés à répartir les tâches entre les membres. Nous avons utilisé Trello pour planifier les tâches hebdomadaires et Google DRIVE pour le partage des fichiers et livrables, la répartition des tâches est détaillée dans le tableau suivant :

Taches	Membres affectées
<b>Elaboration du planning et affectation des tâches</b>	Zine-eddine FODIL
<b>Etude de problème et discussion des solutions</b>	Tous les membres d'équipe
<b>Reproduction de la topologie et configuration minimal</b>	Zine-eddine FODIL
<b>Plan d'adressage et routage Ipv4</b>	Rezak AZIZ
	Issam BEN MESSAOUD
<b>Configuration du NAT</b>	Lounes MECHOUK
<b>Tests</b>	Zine-eddine FODIL
<b>Vérification des tests</b>	Rezak AZIZ, Issam BEN MESSAOUD, Lounes MECHOUK
<b>Rédaction du rapport</b>	Tous les membres de l'équipe

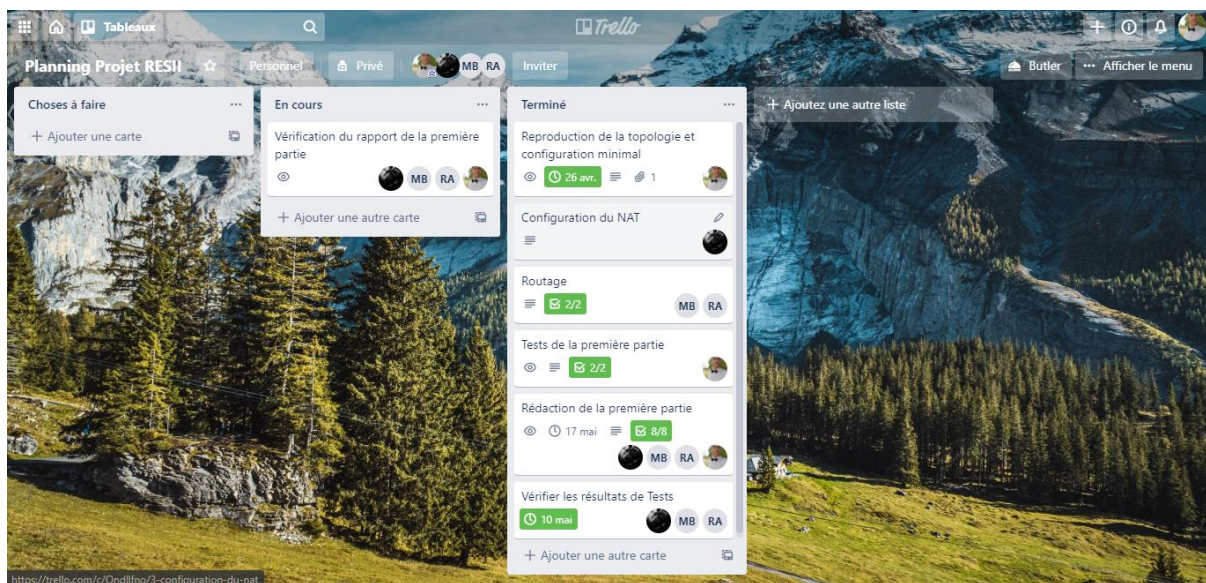
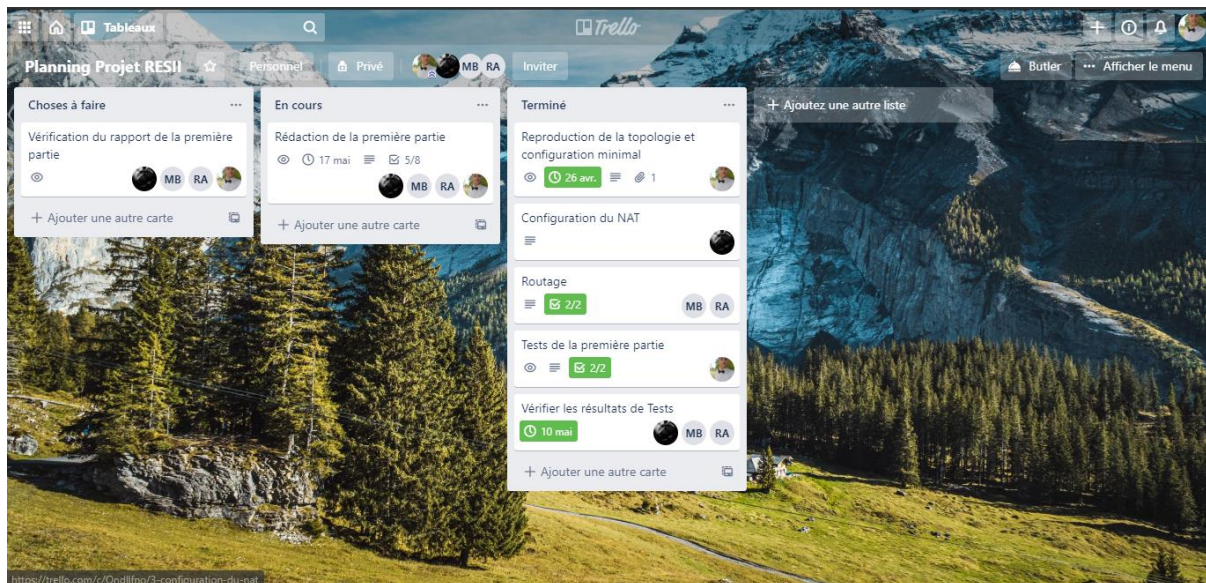
L'avancement des tâches (*définies sur Trello*) évolue chaque semaine comme le montre les captures suivantes :











Pendant la réalisation du projet nous nous avons été amenés à faire des réunions sur la plateforme MEET pour vérifier l'état d'avancement de ce dernier. Les réunions ont eu lieu aux dates suivantes :

- ✓ **Réunion 01** : Discussion du projet et première répartition des tâches ,12/04/2020
- ✓ **Réunion 02** : Vérification de la topologie minimale et préparation pour le plan d'adressage et le routage Ipv4, 28/04/2020
- ✓ **Réunion 03** : Vérification du routage et préparation pour le NAT, 05/05/2020
- ✓ **Réunion 04** : Vérification de la première partie et le livrable à remettre, 16/05/2020

### III. Mise en place de la topologie :

A partir de schéma proposé et des contraintes spécifiées, on a reproduit la topologie. Pour ce faire, nous sommes passés par les étapes suivantes :

- Reproduction de la topologie physique
- Configuration des routeurs et des machines

#### 1. Plan d'adressage :

Dans cette partie nous allons évoquer le plan d'adressage des différents sites (*site principal*, *site1*, *site2*, *site3*). Pour établir le plan d'adressage nous avons pris en considération les points suivants :

- Économiser l'utilisation des adresses IP
- Possibilités d'extensions en ajoutant d'autres sous réseaux
- Utiliser uniquement les plages d'adresses dont nous avons besoin

A partir de l'étude de la topologie nous avons les données suivantes :

Site	Net ID	Nombre de machines
Site principal	10.32.1.0/24	125+ serveurs+ le routeur interne
Site1	10.32.2.0/24	120
Site2	10.32.3.0/24	25
Site3	10.32.4.0/24	75

##### a. Site principal :

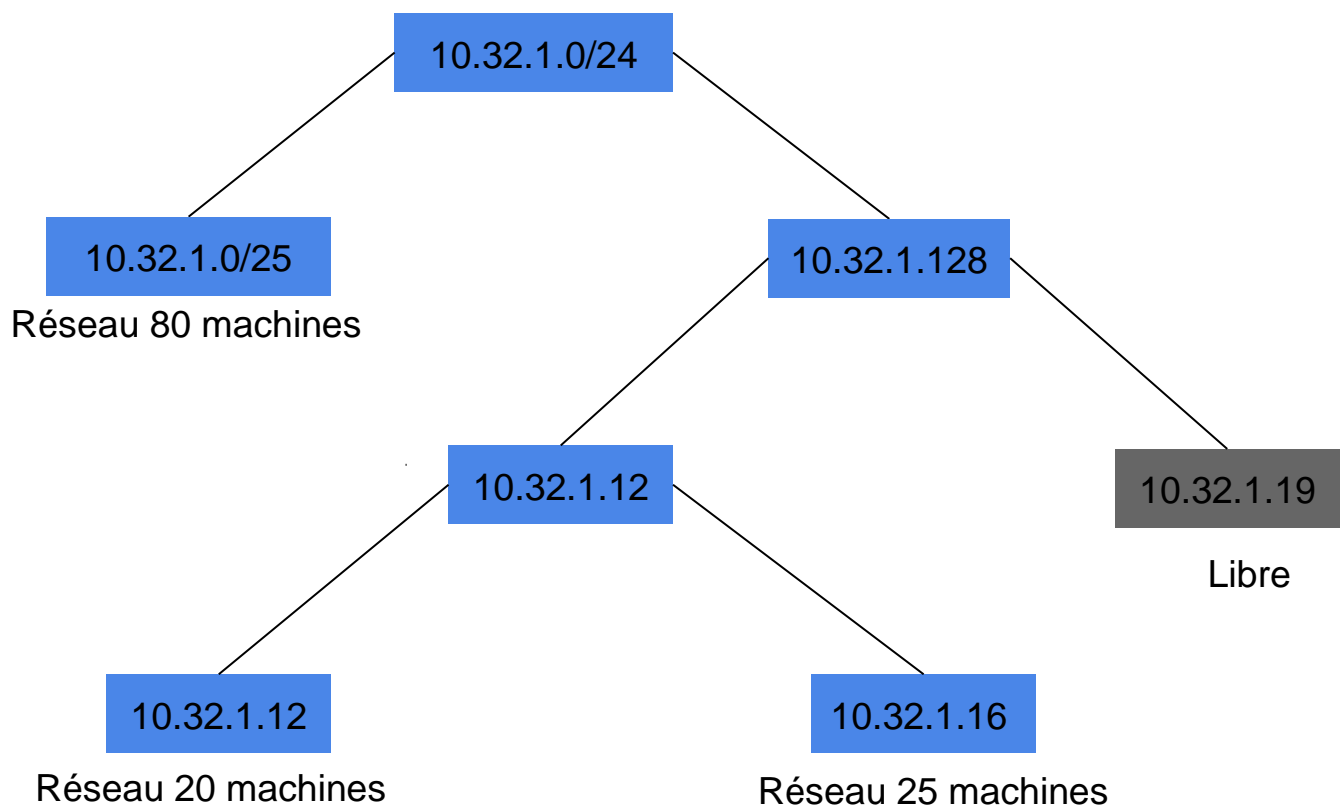
Nous avons dans ce site un routeur interne relié à un réseau contenant des serveurs et 3 autres réseaux

La répartition des adresses est faite de la manière suivante :



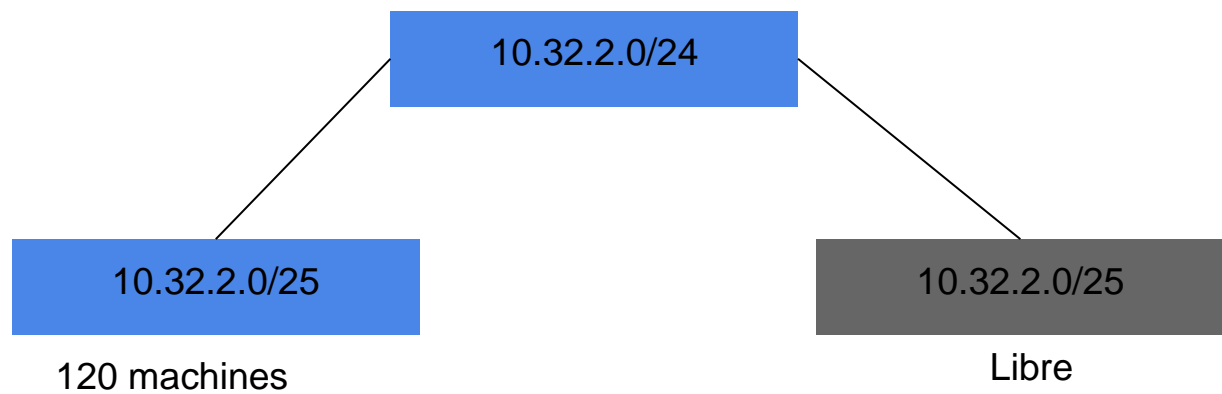
Réseaux	Net ID	Nombre de machines	Plage d'adresses
Réseau serveurs	192.168.32.0/28	4	192.168.32.2-192.168.32.15
Réseaux entre routeur site principale et routeur interne	192.168.33.0/30	2	192.168.33.1.1-192.168.33.2
Sous réseaux 1 (80 machines)	10.32.1.0/25	80	10.32.1.1-10.32.1.127
Sous réseau 2 (20 machines)	10.32.1.128/27	20	10.32.1.129-10.32.1.159
Sous réseau 3 (25 machines)	10.32.1.160/27	25	10.32.1.161-10.32.1.191

On a obtenu ces résultats a en utilisant la méthode VLSM :

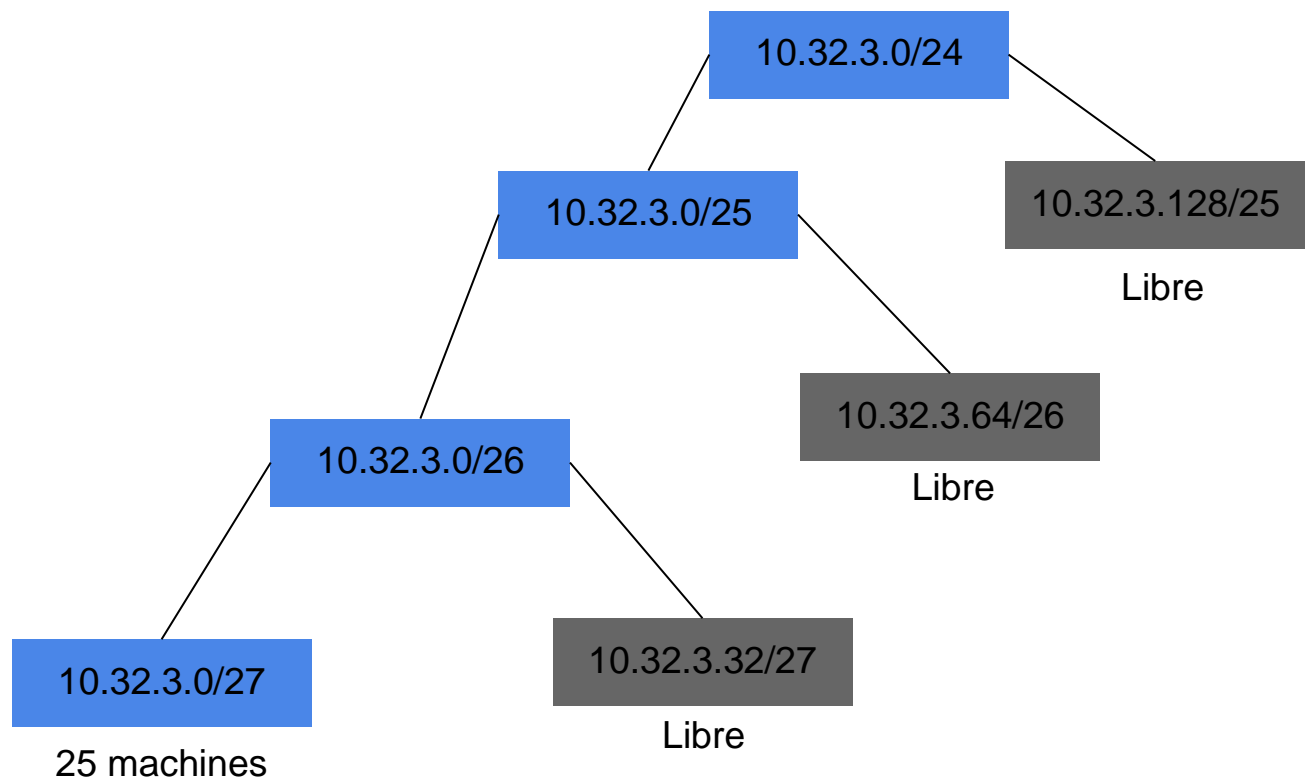


**b. Site 1 :**

Ce site est composé de 120 machines et a comme adresse 10.32.2.0/25

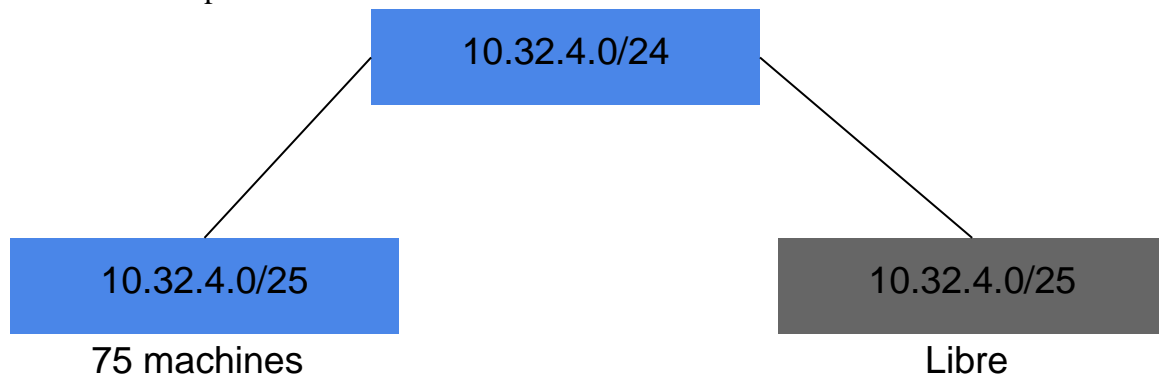
**c. Site 2 :**

Ce site est composé de 25 machines et son adresse est 10.32.3.0/27



**d. Site 3 :**

Ce site est composé de 75 machines et a comme adresse 10.32.4.0/25 :

**2. Configuration des différents routeurs et machines :**

On commence par attribuer, dans chaque routeur, une adresse IP pour chaque interface utilisée. Pour cela on donne l'exemple de l'interface Fa 0/0 au niveau de routeur CE\_Site\_Principal comme le montre la figure ci-contre :

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface
Router(config)#interface af
Router(config)#interface f
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.33.1 255.255.255.252
Router(config-if)#exit
Router(config)#exit
Router#
  
```

**Explication des commandes :**

- enable: permet d'entrer en mode configuration
- configure terminal : permet d'entrer en mode configuration globale
- interface FastEthernet 0/x : entrer en mode configuration de l'interface Fa 0/x
- ip address @ipv4 @mask : permet d'attribuer l'adresse ipv4 a l'interface Fa 0/x avec le mask @mask

Puis on configure aussi les route par défaut comme le montre la figure suivante (la capture est faite au niveau de routeur interne :

```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 f
Router(config)#ip route 0.0.0.0 0.0.0.0 fastEthernet 0/0
Router(config)#end
Router#

```

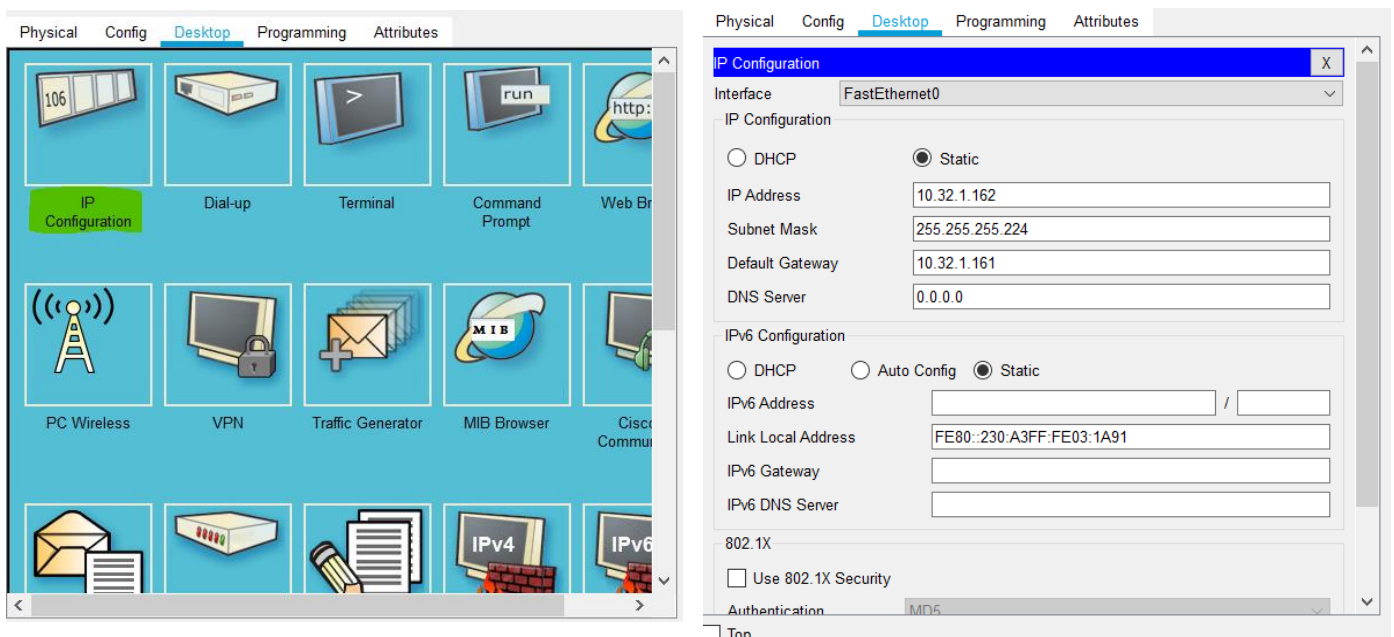
### Explication des commandes :

- `ip route 0.0.0.0 0.0.0.0 fastEthernet 0/0` : ajoute la route par défaut dans la table de routage de routeur

**On refait la même procédure pour tous les routeurs en attribuant les adresses IP adéquates.**

Pour les machines (serveur et PC) on suit les étapes suivantes pour affecter des adresses ip :

- On affecte à chaque PC une adresse ip
- On affecte une passerelle par défaut



**On refait les mêmes procédures pour tous les pc et serveur.**



## IV. Mise en place de NAT :

### 1. Choix du NAT à utiliser

Le NAT permet de traduire les adresses internes pour une ou plusieurs adresses externe (publiques). Cette fonctionnalité est réalisée par un routeur.

Il existe 3 types de Nat :

- Nat statique : à chaque adresse interne correspond une adresse publique prédéfinie. Il est utilisé pour des serveurs qui doivent être visibles et accessible de l'internet.
- Nat dynamique : à chaque adresse privée correspond une adresse prise dans un ensemble d'adresses publiques (*pool*). Cette adresse publique est attribuée dynamiquement ; lorsque toutes les adresses sont attribuées, les machines souhaitant accéder à internet doivent attendre qu'une adresse publique se libère.
- PAT : toutes les adresses internes sont traduites vers une seule adresse publique en exploitant le concept de Port.

Notre choix s'est porté sur le **PAT** dans les **différents sites de l'entreprise**. Néanmoins, en ce qui concerne les **serveurs du site principal** (*qui doivent être visibles de l'extérieur*) nous avons opté pour le **NAT statique**.

#### **Justification :**

Le PAT est utile pour économiser les adresse IP publiques. En effet ces dernières - *comme cité précédemment*- sont rares et coûtent cher.

Le NAT a été choisi pour les serveurs du site principal car ces derniers doivent être accessibles depuis l'extérieur. En d'autres termes, ils doivent avoir des adresses bien précises.

Les adresses des serveurs sont :

Serveur web1 : 192.168.32.2 correspond 11.32.0.4/29

Serveur web2 : 192.168.32.2 correspond 11.32.0.5/29

Serveur DNS mail : 192.168.32.2 correspond 11.32.0.6/29

## 2. Mise en place du NAT et du PAT :

### Attribution des adresses (*Tables NAT*) :

- Site principal  
Plage d'adresses de sortie : 11.32.0.3/29 -> 11.32.0.6/29  
Routeur : CE\_Site\_Principal

➔ Machines :  
@ Réseau : 10.32.1.0/24  
Type de NAT : PAT  
@ Sortie attribuée : 11.32.0.3/29

➔ Serveurs :  
@ Réseau : 192.168.32.0/28  
Type de NAT : Statique.

192.168.32.2/28	11.32.0.4/29
192.168.32.3/28	11.32.0.5/29
192.168.32.4/28	11.32.0.6/29

- Site 1  
@ Réseau : 10.32.2.0/24  
Type de NAT : PAT  
Routeur : CE\_Site1  
@ Sortie : 12.32.0.3/29
- Site 2  
@ Réseau : 10.32.3.0/24  
Type de NAT : PAT  
Routeur : CE\_Site2  
@ Sortie : 13.32.0.3/29
- Site 3  
@ Réseau : 10.32.4.0/24  
Type de NAT : PAT  
Routeur : CE\_Site3  
@ Sortie : 14.32.0.3/29

**Commandes de configuration NAT au niveau de chaque routeur :**

- **Routeur CE\_Site\_Principal**

**//Configuration NAT Statique**

```
enable //entrer en mode configuration
configure terminal //mode configuration globale
interface fa0/0 //Accès à l'interface fast ethernet0/0.
ip nat inside //fa0/0 débouche sur le réseau interne.
exit

interface fa0/1 //Accès à l'interface fast ethernet0/1.
ip nat outside //fa0/1 est du côté du réseau externe.
exit

ip nat inside source static 192.168.32.2 11.32.0.4 //NAT du premier serveur.
ip nat inside source static 192.168.32.3 11.32.0.5 //NAT du 2e serveur.
ip nat inside source static 192.168.32.4 11.32.0.6 //NAT du 3e serveur.
```

**//NAT Statique configuré avec succès****//Configuration PAT**

```
enable //entrer en mode configuration
configure terminal //mode configuration globale

interface fa0/0 //Accès à l'interface fast ethernet0/0.
ip nat inside //fa0/0 débouche sur le réseau interne.
exit

interface fa0/1 //Accès à l'interface fast ethernet0/1.
ip nat outside //fa0/1 est du côté du réseau externe.
exit
```

```
//Création d'une access-list pour le réseau.
access-list 1 permit 10.32.1.0 0.0.0.255
```

```
ip nat inside source list 1 interface fa0/1 overload
//Définition du PAT sur l'interface fa0/1 (interface de sortie).
```

**//PAT configuré avec succès**

- **Routeur CE\_Site1**

```
enable
configure terminal

interface fa0/1
ip nat inside
exit

interface fa0/0
ip nat outside
exit

access-list 1 permit 10.32.2.0 0.0.0.255
ip nat inside source list 1 interface fa0/0 overload
```

- **Routeur CE\_Site2**

```
enable
configure terminal

interface fa0/1
ip nat inside
exit

interface fa0/0
ip nat outside
exit

access-list 1 permit 10.32.3.0 0.0.0.255
ip nat inside source list 1 interface fa0/0 overload
```



- **Routeur CE\_Site3**

```
enable
configure terminal

interface fa0/1
ip nat inside
exit

interface fa0/0
ip nat outside
exit

access-list 1 permit 10.32.4.0 0.0.0.255
ip nat inside source list 1 interface fa0/0 overload
```

## Captures d'écran de la table NAT de chaque routeur

- **Routeur CE\_Site\_Principal :**

```
Router#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside
-----
icmp 11.32.0.2:1        10.32.1.162:1     11.32.0.1:1
11.32.0.1:1
icmp 11.32.0.2:2        10.32.1.162:2     11.32.0.1:2
11.32.0.1:2
icmp 11.32.0.2:3        10.32.1.162:3     11.32.0.1:3
11.32.0.1:3
icmp 11.32.0.2:4        10.32.1.162:4     11.32.0.1:4
11.32.0.1:4
---  11.32.0.4           192.168.32.2      ---
---  11.32.0.5           192.168.32.3      ---
---  11.32.0.6           192.168.32.4      ---
```

- **Routeur CE\_Site1 :**

```
Router#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside
global
icmp 12.32.0.2:1        10.32.2.2:1       12.32.0.1:1
12.32.0.1:1
icmp 12.32.0.2:2        10.32.2.2:2       12.32.0.1:2
12.32.0.1:2
icmp 12.32.0.2:3        10.32.2.2:3       12.32.0.1:3
12.32.0.1:3
icmp 12.32.0.2:4        10.32.2.2:4       12.32.0.1:4
12.32.0.1:4
```

- **Routeur CE\_Site2 :**

```
Router#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside
global
icmp 13.32.0.2:1        10.32.3.2:1       13.32.0.1:1
13.32.0.1:1
icmp 13.32.0.2:2        10.32.3.2:2       13.32.0.1:2
13.32.0.1:2
icmp 13.32.0.2:3        10.32.3.2:3       13.32.0.1:3
13.32.0.1:3
icmp 13.32.0.2:4        10.32.3.2:4       13.32.0.1:4
13.32.0.1:4
```

- **Routeur CE\_Site3 :**

```
Router#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside
global
icmp 14.32.0.2:1        10.32.4.2:1       14.32.0.1:1
14.32.0.1:1
icmp 14.32.0.2:2        10.32.4.2:2       14.32.0.1:2
14.32.0.1:2
icmp 14.32.0.2:3        10.32.4.2:3       14.32.0.1:3
14.32.0.1:3
icmp 14.32.0.2:4        10.32.4.2:4       14.32.0.1:4
14.32.0.1:4
```

## V. Tests :

Pour s'assurer de la fiabilité de la topologie mise en place et du bon fonctionnement du NAT, on procède à une série de tests.

Il est à noter que les serveurs du site principal ont comme adresses publiques :

Serveur web1 : 11.32.0.4/29

Serveur web2 : 11.32.0.5/29

Serveur DNS mail : 11.32.0.6/29

### 1. Test N°01 :

Accéder au serveur 201.32.1.3 à partir d'une machine du site principal :

#### a. Commandes utilisées :

- ping 201.32.1.3
- tracert 201.32.1.3

#### b. Résultats obtenus :

```
C:\>ping 201.32.1.3

Pinging 201.32.1.3 with 32 bytes of data:

Reply from 201.32.1.3: bytes=32 time=13ms TTL=124
Reply from 201.32.1.3: bytes=32 time=13ms TTL=124
Reply from 201.32.1.3: bytes=32 time=16ms TTL=124
Reply from 201.32.1.3: bytes=32 time=12ms TTL=124

Ping statistics for 201.32.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 16ms, Average = 13ms
```

```
C:\>tracert 201.32.1.3

Tracing route to 201.32.1.3 over a maximum of 30 hops:

  0  1 ms    0 ms    0 ms    10.32.1.129
  1  0 ms    11 ms   0 ms    192.168.33.1
  2  11 ms   4 ms    12 ms   11.32.0.1
  3  13 ms   11 ms   30 ms   15.32.0.4
  4  14 ms   22 ms   13 ms   201.32.1.3

Trace complete.
```

**c. Explications :**

- Par la commande ping 201.32.1.3, on remarque que la connexion a été établie entre le pc du site principale et le serveur, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.
- Par la commande tracert 201.32.1.3, on s'assure bien que la connexion a été établie.

De plus on s'assure que le chemin suivi par les paquets est correct

- Les paquets passent par l'interface d'entrée du routeur interne (10.32.0.129)
- Puis l'interface d'entrée de CE\_site\_principal (192.168.33.1)
- Puis l'interface d'entrée de R1\_ISP (11.32.0.1)
- Puis l'interface d'entrée de R\_internet\_ipv6(15.32.0.4)
- Et puis le serveur web ipv4(201.32.1.3). Ce qui prouve que la connectivité est assurée

**2. Test N°02 :**

Accéder au serveur 201.32.1.3 à partir d'une machine du site 1 :

**a. Commandes utilisées :**

- ping 201.32.1.3
- tracert 201.32.1.3

**b. Résultats obtenus :**

```
C:\>ping 201.32.1.3

Pinging 201.32.1.3 with 32 bytes of data:

Reply from 201.32.1.3: bytes=32 time<1ms TTL=125
Reply from 201.32.1.3: bytes=32 time=14ms TTL=125
Reply from 201.32.1.3: bytes=32 time=14ms TTL=125
Reply from 201.32.1.3: bytes=32 time=12ms TTL=125

Ping statistics for 201.32.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 10ms
```

```
C:\>tracert 201.32.1.3

Tracing route to 201.32.1.3 over a maximum of 30 hops:

  1  1 ms      0 ms      0 ms      10.32.2.1
  2  10 ms     0 ms      0 ms      12.32.0.1
  3   3 ms     16 ms     18 ms     15.32.0.4
  4  11 ms     16 ms      0 ms     201.32.1.3

Trace complete.
```



**c. Explications :**

- Par la commande ping 201.32.1.3, on remarque que la connexion a été établie entre le pc du site principal et le serveur, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.
- Par la commande tracert 201.32.1.3, on s'assure bien que la connexion a été établie. De plus on s'assure que le chemin suivi par les paquets est correct
  - Les paquets passent par l'interface d'entrée de CE\_site\_1 (10.32.2.1)
  - Puis l'interface d'entrée de R2\_ISP (12.32.0.1)
  - Puis l'interface d'entrée de R\_internet\_ipv6(15.32.0.4)
  - Et puis le serveur web ipv4(201.32.1.3). Ce qui prouve que la connectivité est assurée

**3. Test N°03 :**

Accéder au serveur 201.32.1.3 à partir d'une machine du site 2 :

**a. Commandes utilisées :**

- ping 201.32.1.3
- tracert 201.32.1.3

**b. Résultats obtenus:**

```
C:\>ping 201.32.1.3

Pinging 201.32.1.3 with 32 bytes of data:

Reply from 201.32.1.3: bytes=32 time=11ms TTL=125
Reply from 201.32.1.3: bytes=32 time=10ms TTL=125
Reply from 201.32.1.3: bytes=32 time=11ms TTL=125
Reply from 201.32.1.3: bytes=32 time<1ms TTL=125

Ping statistics for 201.32.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 8ms
```

```
C:\>tracert 201.32.1.3

Tracing route to 201.32.1.3 over a maximum of 30 hops:

  0  1 ms    0 ms    0 ms    10.32.3.1
  1  0 ms    0 ms    12 ms   13.32.0.1
  2  14 ms   12 ms   14 ms   15.32.0.4
  3  11 ms   11 ms   11 ms   201.32.1.3

Trace complete.
```

**c. Explications :**

- Par la commande ping 201.32.1.3, on remarque que la connexion a été établie entre le pc de site principal et le serveur, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.
- Par la commande tracert 201.32.1.3, on s'assure bien que la connexion a été établie. De plus on s'assure que le chemin suivi par les paquets est correct
  - Les paquets passent par l'interface d'entrée de CE\_site\_2 (10.32.3.1)
  - Puis l'interface d'entrée de R3\_ISP (13.32.0.1)
  - Puis l'interface d'entrée de R\_internet\_ipv6(15.32.0.4)
  - Et puis le serveur web ipv4(201.32.1.3). Ce qui prouve que la connectivité est assurée

**4. Test N°04 :**

Accéder au serveur 201.32.1.3 à partir d'une machine du site 3

**a. Commandes utilisées :**

- ping 201.32.1.3
- tracert 201.32.1.3

**b. Résultats obtenus :**

```
C:\>ping 201.32.1.3

Pinging 201.32.1.3 with 32 bytes of data:

Reply from 201.32.1.3: bytes=32 time<1ms TTL=125
Reply from 201.32.1.3: bytes=32 time=12ms TTL=125
Reply from 201.32.1.3: bytes=32 time<1ms TTL=125
Reply from 201.32.1.3: bytes=32 time=11ms TTL=125

Ping statistics for 201.32.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 5ms
```

```
C:\>tracert 201.32.1.3

Tracing route to 201.32.1.3 over a maximum of 30 hops:

  1  1 ms    0 ms    0 ms    10.32.4.1
  2  0 ms    0 ms    6 ms    14.32.0.1
  3  11 ms   13 ms    0 ms    15.32.0.4
  4  15 ms   11 ms   10 ms    201.32.1.3

Trace complete.
```

**c. Explications :**

- Par la commande ping 201.32.1.3, on remarque que la connexion a été établie entre le pc du site principal et le serveur, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.
- Pour la commande tracert 201.32.1.3, on s'assure que la connexion a bien été établie. De plus on s'assure que le chemin suivi par les paquets est correct
  - Les paquets passent par l'interface d'entrée de CE\_site\_3 (10.32.4.1)
  - Puis l'interface d'entrée de R4\_ISP (14.32.0.1)
  - Puis l'interface d'entrée de R\_internet\_ipv6(15.32.0.4)
  - Et puis le serveur web ipv4(201.32.1.3). Ce qui prouve que la connectivité est assurée

**5. Test N°05 :**

Accéder au serveur Web du site principal à partir de la machine client 201.32.1.2

**a. Commandes utilisées :**

- ping 11.32.0.4
- tracert 11.32.0.4

On a utilisé l'adresse publique 11.32.0.4 qui substitue 192.168.32.2

**b. Résultats obtenus :**

```
C:\>ping 11.32.0.4

Pinging 11.32.0.4 with 32 bytes of data:

Reply from 11.32.0.4: bytes=32 time=1ms TTL=124
Reply from 11.32.0.4: bytes=32 time=4ms TTL=124
Reply from 11.32.0.4: bytes=32 time=12ms TTL=124
Reply from 11.32.0.4: bytes=32 time=13ms TTL=124

Ping statistics for 11.32.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 7ms
```

```
C:\>tracert 11.32.0.4

Tracing route to 11.32.0.4 over a maximum of 30 hops:

  1  1 ms      0 ms      0 ms      201.32.1.1
  2  0 ms      11 ms     15 ms     15.32.0.1
  3  12 ms     16 ms     11 ms     11.32.0.4
  4  15 ms     13 ms     13 ms     11.32.0.4
  5  25 ms     24 ms     16 ms     11.32.0.4

Trace complete.
```

**c. Explications :**

- Pour accéder au serveur web du site principal on doit accéder à l'adresse publique de ce dernier (11.32.0.4 pour web1, 11.32.0.5 pour web2, 11.32.0.6 pour ftp/DNS) car un NAT statique est mis en place.
- Par la commande ping 11.32.0.4, on remarque que la connexion a été établie entre le serveur web du site principal et la machine client de internet\_ipv4, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.
- Pour la commande tracert 11.32.0.4, on s'assure que la connectivité a bien été établie. De plus on s'assure que le chemin suivi par les paquets est correct

- Les paquets passent par l'interface d'entrée de R\_internet\_ipv6(201.32.1.1)
- Puis l'interface d'entrée de R1\_ISP (15.32.0.1)
- Puis l'interface d'entrée de CE\_SITE\_PRINCIPALE (11.32.0.4), à ce niveau l'adresse 11.32.0.4 sera remplacée par l'adresse privée du serveur web c'est à dire 192.168.32.2 et le fait de voir 3 adresses IP identiques est dû au fait que l'adresse 192.168.32.2 est remplacée par 11.32.0.4 au retour
- Donc le paquet passe par le routeur interne puis arrive au serveur web



## 6. Test N°06 :

Accéder au serveur Web du site principal à partir de site1

### a. Commandes utilisées :

- ping 11.32.0.4
- tracert 11.32.0.4

On a utilisé l'adresse publique 11.32.0.4 qui substitue 192.168.32.2

### b. Résultats obtenus :

```
C:\>ping 11.32.0.4

Pinging 11.32.0.4 with 32 bytes of data:

Reply from 11.32.0.4: bytes=32 time<1ms TTL=123
Reply from 11.32.0.4: bytes=32 time=13ms TTL=123
Reply from 11.32.0.4: bytes=32 time=19ms TTL=123
Reply from 11.32.0.4: bytes=32 time=12ms TTL=123

Ping statistics for 11.32.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 11ms
```

```
C:\>tracert 11.32.0.4

Tracing route to 11.32.0.4 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    10.32.2.1
  1  0 ms    0 ms    1 ms    12.32.0.1
  2  11 ms   10 ms   12 ms   15.32.0.1
  3  13 ms   18 ms   18 ms   11.32.0.4
  4  15 ms   10 ms   23 ms   11.32.0.4
  5  25 ms   14 ms   25 ms   11.32.0.4

Trace complete.
```

### c. Explications :

- Pour accéder au serveur web du site principal on doit accéder à l'adresse publique de ce dernier (11.32.0.4 pour web1, 11.32.0.5 pour web2, 11.32.0.6 pour ftp/DNS) car un NAT statique est mis en place,
- Par la commande ping 11.32.0.4, on remarque que la connexion a été établie entre le serveur web de site principal et la machine client du site 1, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.
- Pour la commande tracert 11.32.0.4, on s'assure bien que la connexion a été établie. De plus on s'assure que le chemin suivi par les paquets est correct
  - Les paquets passent par l'interface d'entrée de CE\_SITE\_1(10.32.2.1)
  - Puis l'interface d'entrée de R2\_ISP (12.32.0.1)

- Puis l'interface d'entrée de R1\_ISP (15.32.0.1)
- Puis l'interface d'entrée de CE\_SITE\_PRINCIPALE (11.32.0.4), à ce niveau l'adresse 11.32.0.4 sera remplacée par l'adresse privée du serveur web c'est à dire 192.168.32.2 et le fait de voir 3 adresses IP identiques est dû au fait que l'adresse 192.168.32.2 est remplacée par 11.32.0.4 au retour
- Donc le paquet passe par le routeur interne puis arrive au serveur web

## 7. Test N°07 :

Accéder au serveur Web du site principal à partir de site 3

### a. Commandes utilisées :

- ping 11.32.0.4
- tracer 11.32.0.4

On a utilisé l'adresse publique 11.32.0.4 qui substitue 192.168.32.2

### b. Résultats obtenus :

```
C:\>ping 11.32.0.4

Pinging 11.32.0.4 with 32 bytes of data:

Reply from 11.32.0.4: bytes=32 time=12ms TTL=123
Reply from 11.32.0.4: bytes=32 time=12ms TTL=123
Reply from 11.32.0.4: bytes=32 time=14ms TTL=123
Reply from 11.32.0.4: bytes=32 time=13ms TTL=123

Ping statistics for 11.32.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 14ms, Average = 12ms
```

```
C:\>tracert 11.32.0.4

Tracing route to 11.32.0.4 over a maximum of 30 hops:

  1  1 ms    0 ms    0 ms    10.32.3.1
  2  0 ms    0 ms    3 ms    13.32.0.1
  3  10 ms   12 ms   12 ms   15.32.0.1
  4  11 ms   15 ms   11 ms   11.32.0.4
  5  14 ms    0 ms   24 ms   11.32.0.4
  6  14 ms   14 ms   13 ms   11.32.0.4

Trace complete.
```

**c. Explications :**

- Pour accéder au serveur web du site principal on doit accéder à l'adresse publique de ce dernier (11.32.0.4 pour web1, 11.32.0.5 pour web2, 11.32.0.6 pour ftp/DNS) car un NAT statique est mis en place,
- Par la commande ping 11.32.0.4, on remarque que la connexion a été établie entre le serveur web du site principal et la machine client du site 2, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.
- Pour la commande tracert 11.32.0.4, on s'assure que la connectivité a bien été établie. De plus on s'assure que le chemin suivi par les paquets est correct
  - Les paquets passe par l'interface d'entrée de CE\_SITE\_2(10.32.3.1)
  - Puis l'interface d'entrée de R3\_ISP (13.32.0.1)
  - Puis l'interface d'entrée de R1\_ISP (15.32.0.1)
  - Puis l'interface d'entrée de CE\_SITE\_PRINCIPALE (11.32.0.4), à ce niveau l'adresse 11.32.0.4 sera remplacée par l'adresse privée du serveur web c'est à dire 192.168.32.2 et le fait de voir 3 adresses IP identiques est dû au fait que l'adresse 192.168.32.2 est remplacée par 11.32.0.4 au retour
  - Donc le paquet passe par le routeur interne puis arrive au serveur web

**8. Test N°08 :**

Accéder au serveur Web du site principal à partir de site 4

**a. Commandes utilisées :**

- ping 11.32.0.4
- tracert 11.32.0.4

On a utilisé l'adresse publique 11.32.0.4 qui substitue 192.168.32.2

**b. Résultats obtenus :**

```
C:\>tracert 11.32.0.4

Tracing route to 11.32.0.4 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    10.32.4.1
  2  0 ms    0 ms    0 ms    14.32.0.1
  3  11 ms   11 ms   13 ms   15.32.0.1
  4  16 ms   20 ms   12 ms   11.32.0.4
  5  16 ms   27 ms   12 ms   11.32.0.4
  6  14 ms   12 ms   12 ms   11.32.0.4

Trace complete.
```

```
C:\>ping 11.32.0.4

Pinging 11.32.0.4 with 32 bytes of data:

Reply from 11.32.0.4: bytes=32 time=15ms TTL=123
Reply from 11.32.0.4: bytes=32 time=16ms TTL=123
Reply from 11.32.0.4: bytes=32 time=13ms TTL=123
Reply from 11.32.0.4: bytes=32 time=11ms TTL=123

Ping statistics for 11.32.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 16ms, Average = 13ms
```

### c. Explications :

- Pour accéder au serveur web du site principal on doit accéder à l'adresse publique de ce dernier (11.32.0.4 pour web1, 11.32.0.5 pour web2, 11.32.0.6 pour ftp/DNS) car un NAT statique est mis en place, et l'accès avec HTTP (utilise TCP) donne les résultats précédents (avec et sans DNS).
- Par la commande ping 11.32.0.4, on remarque que la connectivité a été établie entre le serveur web de site principal et la machine client de site 4, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.
- Pour la commande tracert 11.32.0.4, on s'assure que la connectivité a bien été établie.

De plus on s'assure que le chemin suivi par les paquets est correct

- Les paquets passent par l'interface d'entrée de CE\_SITE\_4(10.32.5.1)
- Puis l'interface d'entrée de R4\_ISP (14.32.0.1)
- Puis l'interface d'entrée de R1\_ISP (15.32.0.1)
- Puis l'interface d'entrée de CE\_SITE\_PRINCIPALE (11.32.0.4), à ce niveau l'adresse 11.32.0.4 sera remplacée par l'adresse privée de serveur web c'est à dire 192.168.32.2 et le fait de voir 3 adresses IP identiques est dû au fait que l'adresse 192.168.32.2 est remplacée par 11.32.0.4 au retour
- Donc le paquet passe par le routeur interne puis arrive au serveur web

## **VI. Conclusion**

En conclusion de cette première partie, nous pouvons affirmer en s'appuyant sur les résultats des tests de connectivités effectués par nos soins que le NAT a été correctement implémenté sur l'ensemble des réseaux ce qui permet la communication entre sites et la connexion à Internet.