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 02: Migration en ipv6 pour l'entreprise-

REALISE PAR L'EQUIPE N° 32 :

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

Année 2019 / 2020

Table des matières

I. Introduction

Dans un monde toujours plus connecté où de nouvelles découvertes technologiques sont faites quotidiennement, il est devenu indispensable en tant qu'entreprise d'être à l'affût des évolutions infrastructurelles et logiques touchant son système d'informations afin d'en tirer autant de bénéfices que possible.

L'une de ces dites évolutions concerne l'avènement de l'Internet des objets ainsi que du big data. En effet, le nombre d'adresses IPv4 encore attribuables est en déclin constant, ce qui a comme conséquence de compliquer la tâche des professionnels et des entreprises à maintenir leur habilité à rester flexibles et innovants -car limités par le nombre d'objets connectés *(Serveurs, Machines et autres)* pouvant être accessibles par des sources externes-.

Certes, il est toujours possible d'effectuer une gymnastique cérébrale afin de consommer le moins d'adresses IPv4 publiques que possibles, néanmoins cela deviendra de plus en plus ardu au fur et à mesure que le temps passe. Sans compter que cela représente une perte de temps et d'argent.

C'est donc là qu'est introduite la solution idéale pour toute entreprise ne souhaitant pas être ennuyée par les limitations imposées par la taille des adresses IPv4 : Concevoir ou migrer vers un réseau IPv6. En plus d'offrir une plus large plage d'adresses, l'IPv6 garantit de meilleures performances et une sécurité améliorée.

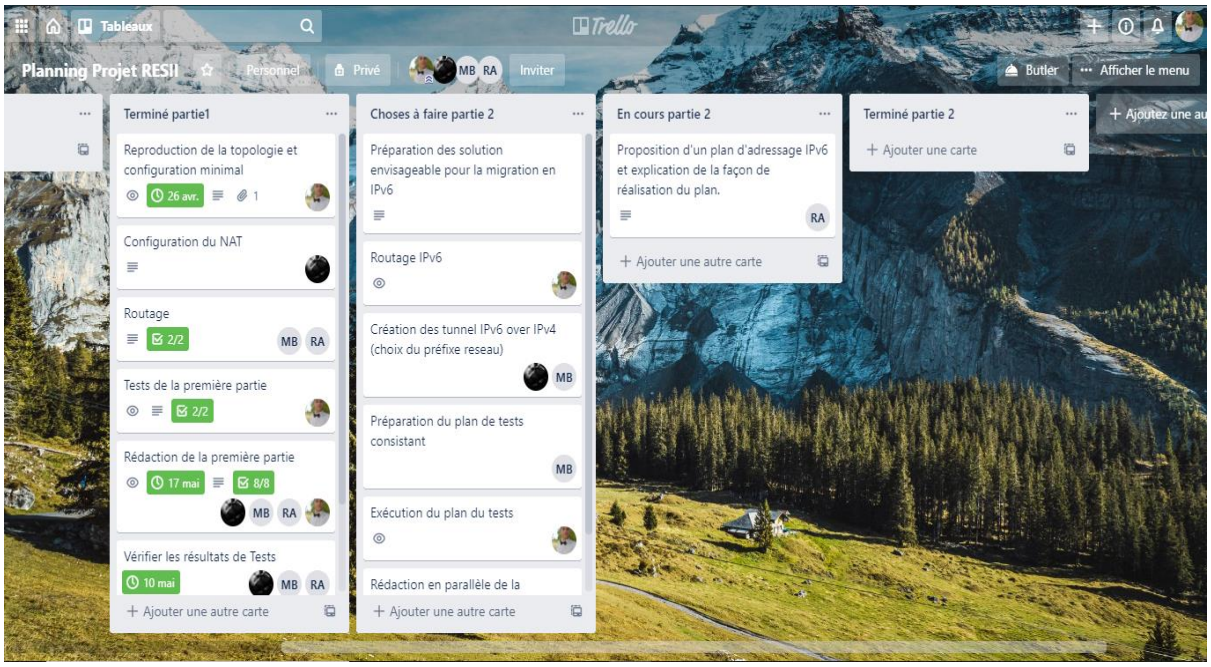
Le rapport suivant détaillera les différentes méthodes utilisées dans le processus de migration du réseau IPv4 vers un réseau IPv6. L'un des principaux axes de cette transition étant l'utilisation de tunnels « IPv6 dans IPv4 » qui permettent l'encapsulation des paquets sortants des réseaux compatibles IPv6 dans des paquets Ipv4. Ce procédé nous a permis d'assurer un passage fluide et stable entre les deux topologies.

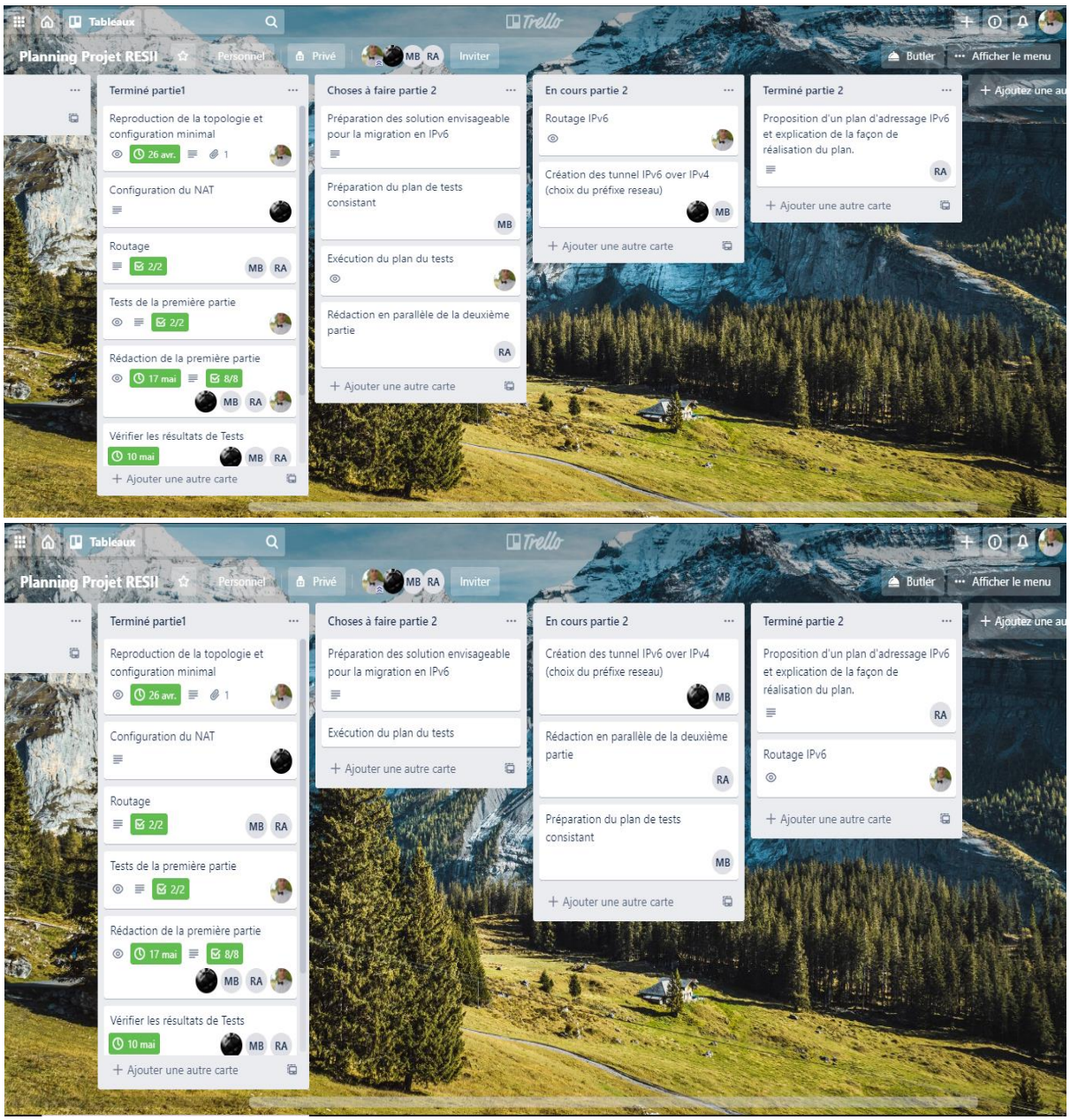
II. Répartition des tâches :

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
Elaboration du planning et affectation des tâches	Zine-eddine FODIL
Etude de problème et discussion des solutions	Tous les membres d'équipe
Préparation des solutions envisageable pour la migration en IPv6	Tous les membres d'équipe
Proposition d'un plan d'adressage IPv6 et explication de la façon de réalisation du plan.	Rezak AZIZ
Routage IPv6	Zine-eddine FODIL
Création des tunnel IPv6 over IPv4	Lounes MECHOUEK Issam BEN MESSAOUD
Préparation du plan de tests	Issam BEN MESSAOUD
Exécution du plan du tests	Zine-eddine FODIL Rezak AZIZ
Vérification des tests	Lounes MECHOUEK Issam BEN MESSAOUD
Rédaction du rapport	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 de la partie 02 ont eu lieu aux dates suivantes :

- ✓ **Réunion 01** : Discussion du la partie 02 et répartition des tâches,19/05/2020
- ✓ **Réunion 02** : Vérification du plan d'adressage et le routage Ipv6 et préparation pour les tunnels Ipv6 over Ipv4 ,26/05/2020
- ✓ **Réunion 03** : Vérification des tunnels Ipv6 over Ipv4 et discussion du plan du tests,2/06/2020
- ✓ **Réunion 04** : Vérification du plan de Tests et l'exécution des tests, 9/06/2020
- ✓ **Réunion 05** : Vérification de la deuxième partie et le livrable à remettre,10/06/2020

III. Plan d'adressage Ipv6 :

A partir de la topologie de la première partie, on va ajouter la pile Ipv6. Pour ce faire, nous sommes passés par les étapes suivantes :

- Mettre en place un plan d'adressage
- Configuration des routeurs et des machines

1. Plan d'adressage :

Sachons que la structure d'adresse Ipv6 est la suivante :

Topologie publique (préfixe global)	Topologie Privée	ID interface
48 Bits	16 Bits	64 Bits

De plus on a le préfixe global suivant : 2001 :DB8 : 32 : :/48 (avec 32 est l'identité de l'équipe)
Pour cela on utilise la structure suivante pour affecter les adresses : 2001 :DB8:32:X00Y: :/64

Avec X : le numéro du site +1

Et Y : le numéro du sous réseau (pratiquement pour le site principal)

Donc l'affectation des adresses se fait comme suit :

a. Site principale :

Adresse réseau : 2001 :DB8 :32 :1000 : :/64
Les serveurs doivent avoir des adresses stables comme suit :
Adresse sous réseau : 2001 :DB8 :32 :1001 : :/64

- WEB1 : 2001 :DB8 :32 :1001 : :2/64
- WEB2 : 2001 :DB8 :32 :1001 : :3/64
- Mail + DNS : 2001 :DB8 :32 :1001 : :4/64

Les autres sous réseau :

- Sous réseau de 25 machines :

Adresse sous réseau : 2001 :DB8 :32 :1002 : :/64

- Sous réseau de 20 machines :

Adresse sous réseau : 2001 :DB8 :32 :1003 : :/64

- Sous réseau de 80 machines :

Adresse sous réseau : 2001 :DB8 :32 :1004 : :/64

b. Site 1 :

Adresse réseau : 2001 :DB8 :32 :2000 : :/64

c. Site2 :

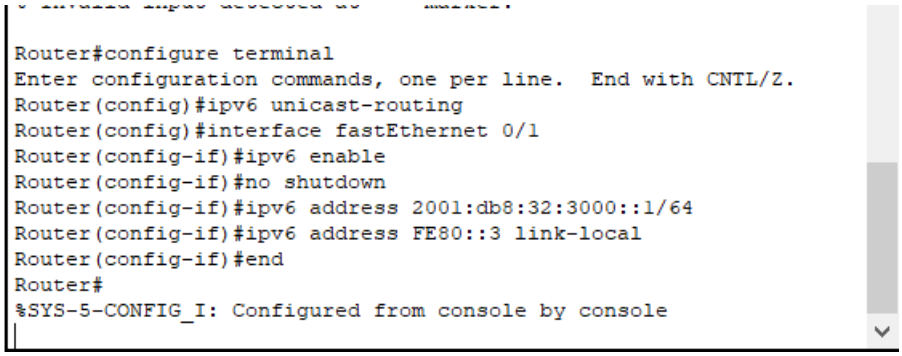
Adresse réseau : 2001 :DB8 :32 :3000 : :/64

d. Site3 :

Adresse réseau : 2001 :DB8 :32 :4000 : :/64

2. Configuration des différents routeurs et machines :

On commence par attribuer, dans chaque routeur de l'entreprise, une adresse Ipv6 pour chaque interface qui la nécessite. Pour cela on donne l'exemple de l'interface Fa 0/1 au niveau de routeur CE_Site 2 comme le montre la figure ci-contre :

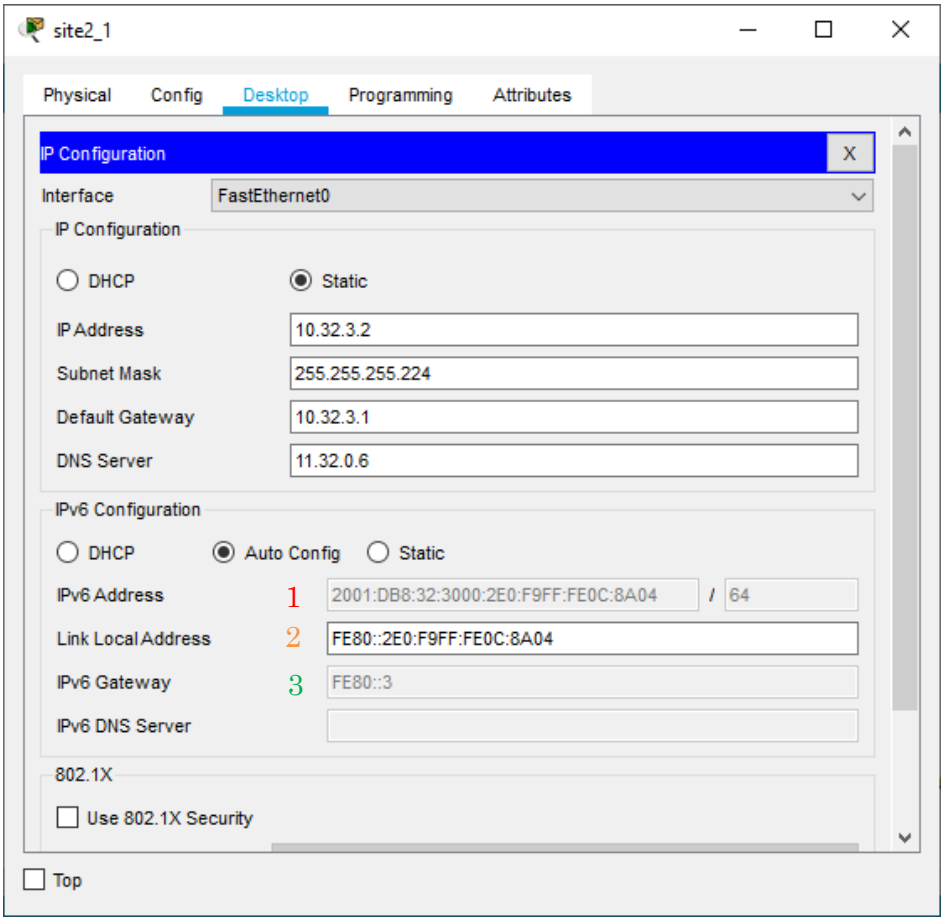


Explication des commandes :

- enable: permet d'entrer en mode configuration
- configure terminal : permet d'entrer en mode configuration globale
- ipv6 unicast-routing : activation du routage ipv6
- interface FastEthernet 0/x : entrer en mode configuration de l'interface Fa 0/x
- ipv6 enable : pour activer l'adressage ipv6 dans l'interface en question
- ipv6 address @ipv6/mask : permet d'attribuer l'adresse ipv6 a l'interface Fa 0/x avec le mask : /mask
    - ➔ La première c'est pour l'adresse global unicast (2001 :db8 :32 : 3000 : :1/64)
    - ➔ La deuxième c'est pour affecter une adresse link-local (FE80 : :3)

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

Pour les machines (serveur et PC) on active l'auto-configuration des adresses Ipv6 et ça donne le résultat suivant (pour une machine de site 2 ça donne) :



Comme le montre la figure précédente, après activation de la config automatique d'adressage Ipv6 la machine a pu obtenir les 3 adresses Ipv6, *Ipv6 global-unicast address, Ipv6 link local address, Ipv6 Gateway*

- 1/ Adresse ipv6 : la machine a pu avoir cette adresse en utilisant la méthode EUI-64 [1]et cela en tenant compte de l'adresse mac de la machine, comme dans ce cas on a :

- La machine Site2_1 a comme adresse Mac : 00E0.F90C.8A04
- La machine à solliciter le routeur CE_Site2 pour avoir le préfixe réseau 2001 :DB8 :32 :3000 ::/64 pour laquelle elle a ajouté l'extension 2E0 :F9FF :FE0C :8A04 qui est que l'adresse Mac de cette machine 00E0.F90C.8A04 avec une extension FF :FE au milieu avec un inversement du 7 -ème bit de poids fort de cette dernière.

- 2/ Adresse *Link Local :* est obtenu avec EUI -64 mais avec un préfixe qui est FE80 ::/10.
- 3/ Ipv6 Gateway (passerelle par défaut) : obtenu à partir du routeur CE_Site2.

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

[1] EUI-64: *Extend Unique Identifier* -64

IV. Création des tunnels Ipv6 over Ipv4 :

Afin de permettre la transition des paquets dans le réseau IPv6 mis en place, il est primordial d'assurer l'interconnexion des différents éléments du réseau. En exploitant le réseau IPv4 précédemment implémenté, l'option qui consiste à faire communiquer les machines de sites différents à travers des tunnels est la plus adéquate.

1. Configuration des tables de routage Ipv6 :

La configuration des tables de routage se fait en deux phase

a. Phase 01 : routes ipv6 avant la mise en place des tunnels

Ces routes, sont les routes par défaut (::/0) que les routeurs CE_Site_Principal, CE_Site 1 , CE_Site 2 , CE_Site 3 ,R_Internet_ipv6 doivent avoir , et les routes vers les sous réseaux de site principale (réseaux 25 , 20 et 80 machines).

- La configuration des routes par défaut se fait avec cette commande :

  ipv6 route ::/0 nom_interface_de_sortie (*en étant en mode config*)

- La configuration des routes vers les sous réseaux se fait de cette manière :

  CE_Site_Principal :

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ipv6 route 2001:db8:32:1001::/64 2001:db8:32:1000::1
Router(config)#ipv6 route 2001:db8:32:1002::/64 2001:db8:32:1000::1
Router(config)#ipv6 route 2001:db8:32:1003::/64 2001:db8:32:1000::1
Router(config)#ipv6 route 2001:db8:32:1004::/64 2001:db8:32:1000::1
```

[2]

- La configuration sur le routeur interne :

  Routeur_Interne :

  ipv6 route ::/0 2001 :db8 :32 :1000 ::2 (*en étant en mode config*)

b. Phase 02 : routes ipv6 durant la mise en place des tunnels

CE_Site_Principal

ipv6 route 2001:1:2:32::/64 2001:db8:5000::5
ipv6 route 2001:db8:32:2000::/64 2001:dB8:32:5002::2
ipv6 route 2001:db8:32:4000::/64 2001:dB8:32:5001::2
ipv6 route 2001:db8:32:3000::/64 2001:db8:32:5003::2

CE_Site1

ipv6 route ::/0 2001:db8:5002::1

CE_Site2

ipv6 route ::/0 2001:db8:5003::1

CE_Site3

ipv6 route ::/0 2001:db8:5001::1

R_Internet_Ipv6

ipv6 route 2001:db8::/48 2001:db8:5000::2

[2] NB : Notons que le regroupement des 4 routes est possible avec cette route 2001 :db8 :32 :1000 ::/60

2. Fonctionnement des tunnels

À la suite d'une mûre réflexion et en se basant sur les exigences du cahier des charges, il a été décidé d'implémenter 4 tunnels de type « IPv6 over IPv4 ». En effet, chaque site est relié au site principal par son propre tunnel. De plus, ce dernier est relié par un quatrième tunnel au réseau Internet IPv6. En résumé :

Nom du tunnel	Extrémités	Adresse réseau
Tunnel 0	- CE_Site_Principal : fa0/1 - R_Internet_ipv6 : fa0/0	2001:db8:32:5000::/64
Tunnel 1	- CE_Site_Principal : fa0/1 - CE_Site3 : fa0/0	2001:db8:32:5001::/64
Tunnel 2	- CE_Site_ Principal : fa0/1 - CE_Site1 : fa0/0	2001:db8:32:5002::/64
Tunnel 3	- CE_Site_Principal : fa0/1 - CE_Site2 : fa0/0	2001:db8:32:5003::/64

Le but premier de cette configuration est de se servir du routeur CE_Site_Principal comme d'une « tour de contrôle ». Tout paquet IPv6 transitant entre les sites ou étant à destination du réseau Internet ipv6 passera forcément par le tunnel le reliant au site principal.

3. Paramètres de configuration

Configuration du tunnel 0
Dans un premier temps, nous nous chargerons du routeur CE_Site_Principal.
La première étape consiste à créer l'interface tunnel 0 :

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface tunnel 0

Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up
```

Nous assignons ensuite une adresse IPv6 à cette extrémité du tunnel

```
Router(config-if)#ipv6 address 2001:DB8:32:5000::1/64
```

L'étape suivante consiste à préciser l'interface source ainsi que l'adresse IPv4 de l'interface du routeur destination du tunnel.

```
Router(config-if)#tunnel source fa0/1
Router(config-if)#tunnel destination 15.32.0.4
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
```

Finalement, il faut préciser le mode qui est d'encapsuler l'ipv6 dans de l'ipv4.

```
Router(config-if)#tunnel mode ipv6ip
Router(config-if)#exit
```

Dans un second temps, nous effectuons une configuration inverse au niveau du routeur R_Internet_Ipv6, ce qui donne :

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface tunnel 0

Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

Router(config-if)#ipv6 address 2001:DB8:32:5000::2/64
Router(config-if)#tunnel source fa0/0
Router(config-if)#tunnel destination 11.32.0.2
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

Router(config-if)#tunnel mode ipv6ip
Router(config-if)#exit
```

La configuration étant terminée, nous pouvons pinger mutuellement les extrémités du tunnel au niveau de chaque routeur.

```
Router#ping 2001:DB8:32:5000::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:32:5000::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/11 ms
```

```
Router#ping 2001:DB8:32:5000::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:32:5000::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
```

La configuration étant strictement identique au niveau de chacun des 3 autres tunnels (mis à part l'adresse réseau des tunnels) nous nous contenterons des détails du tunnel0 ci-dessus.

V. Plan de tests et son exécution :

1. Tests Ipv4

a. Plan de tests

N° Test	Description du test	Objectif	Les résultats attendus
1	Accéder à la machine client_ipv4 à partir d'une machine du site principal.	Vérifiez que le NAT fonctionne toujours correctement (entre site principal et internet ipv4) après la migration en ipv6	Accéder correctement à la machine client_ipv4.
2	Accéder à la machine client_ipv4 à partir d'une machine du site 1.	Vérifiez que le NAT fonctionne toujours correctement (entre site 1 et internet ipv4) après la migration en ipv6	Accéder correctement à la machine client_ipv4.
3	Accéder à la machine client_ipv4 à partir d'une machine du site 2.	Vérifiez que le NAT fonctionne toujours correctement (entre site 2 et internet ipv4) après la migration en ipv6	Accéder correctement à la machine client_ipv4.
4	Accéder à la machine client_ipv4 à partir d'une machine du site 3.	Vérifiez que le NAT fonctionne toujours correctement (entre site 3 et internet ipv4) après la migration en ipv6	Accéder correctement à la machine client_ipv4.
5	Accéder au serveur Web du site principal à partir de la machine client_ipv4	Vérifiez que les serveurs internes sont toujours visibles de l'extérieur après la migration en ipv6	Accéder correctement au serveur Web.

b. Exécution du plan de tests

Test N°01

Accéder à la machine client_ipv4 à partir d'une machine du site principal :

- **Commandes utilisées :**
  - ping 201.32.1.2
  - tracert 201.32.1.2
- **Résultats obtenus :**

```
C:\>ping 201.32.1.2

Pinging 201.32.1.2 with 32 bytes of data:

Reply from 201.32.1.2: bytes=32 time=13ms TTL=124
Reply from 201.32.1.2: bytes=32 time=1ms TTL=124
Reply from 201.32.1.2: bytes=32 time=11ms TTL=124
Reply from 201.32.1.2: bytes=32 time=1ms TTL=124

Ping statistics for 201.32.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 6ms
```

```
C:\>tracert 201.32.1.2

Tracing route to 201.32.1.2 over a maximum of 30 hops:

  1    1 ms      0 ms      1 ms      10.32.1.161
  2    0 ms      0 ms      0 ms      192.168.33.1
  3    0 ms      0 ms      0 ms      11.32.0.1
  4    0 ms      1 ms      11 ms     15.32.0.4
  5    0 ms      10 ms     12 ms     201.32.1.2

Trace complete.
```

- **Explications :**
  - Par la commande ping 201.32.1.2, on remarque que la connexion a été établie entre le pc du site principale et le client ipv4, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.
  - Par la commande tracert 201.32.1.2, 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 (10.32.1.161)
    - ➔ 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 client ipv4(201.32.1.2). Ce qui prouve que la connectivité est assurée.

Test N°02

Accéder à la machine client_ipv4 à partir d'une machine du site 1 :

- **Commandes utilisées :**
  - ping 201.32.1.2
  - tracert 201.32.1.2
- **Résultats obtenus :**

```
C:\>ping 201.32.1.2

Pinging 201.32.1.2 with 32 bytes of data:

Reply from 201.32.1.2: bytes=32 time<1ms TTL=125
Reply from 201.32.1.2: bytes=32 time<1ms TTL=125
Reply from 201.32.1.2: bytes=32 time<1ms TTL=125
Reply from 201.32.1.2: bytes=32 time=10ms TTL=125

Ping statistics for 201.32.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

```
C:\>tracert 201.32.1.2

Tracing route to 201.32.1.2 over a maximum of 30 hops:

  1    0 ms      0 ms      1 ms      10.32.2.1
  2    0 ms      0 ms      0 ms      12.32.0.1
  3    11 ms     0 ms      0 ms      15.32.0.4
  4    0 ms      1 ms      0 ms      201.32.1.2

Trace complete.
```

- **Explications :**
  - Par la commande ping 201.32.1.2, on remarque que la connexion a été établie entre le pc du site 1 et le client ipv4, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.
  - Par la commande tracert 201.32.1.2, 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 client ipv4(201.32.1.2). Ce qui prouve que la connectivité est assurée.

Test N°03

Accéder à la machine client_ipv4 à partir d'une machine du site 2 :

- **Commandes utilisées :**
  - ping 201.32.1.2
  - tracert 201.32.1.2
- **Résultats obtenus :**

```
C:\>ping 201.32.1.2

Pinging 201.32.1.2 with 32 bytes of data:

Reply from 201.32.1.2: bytes=32 time=1ms TTL=125
Reply from 201.32.1.2: bytes=32 time=1ms TTL=125
Reply from 201.32.1.2: bytes=32 time<1ms TTL=125
Reply from 201.32.1.2: bytes=32 time=12ms TTL=125

Ping statistics for 201.32.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms
```

```
C:\>tracert 201.32.1.2

Tracing route to 201.32.1.2 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      10.32.3.1
  2    0 ms      0 ms      0 ms      13.32.0.1
  3    0 ms      0 ms      0 ms      15.32.0.4
  4    1 ms      0 ms      0 ms      201.32.1.2

Trace complete.
```

- **Explications :**
  - Par la commande ping 201.32.1.2, on remarque que la connexion a été établie entre le pc du site 2 et le client ipv4, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.
  - Par la commande tracert 201.32.1.2, 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 client ipv4(201.32.1.2). Ce qui prouve que la connectivité est assurée.

Test N°04

Accéder à la machine client_ipv4 à partir d'une machine du site 3 :

- **Commandes utilisées :**
  - ping 201.32.1.2
  - tracert 201.32.1.2
- **Résultats obtenus :**

```
C:\>ping 201.32.1.2

Pinging 201.32.1.2 with 32 bytes of data:

Reply from 201.32.1.2: bytes=32 time=1ms TTL=125
Reply from 201.32.1.2: bytes=32 time=1ms TTL=125
Reply from 201.32.1.2: bytes=32 time=1ms TTL=125
Reply from 201.32.1.2: bytes=32 time<1ms TTL=125

Ping statistics for 201.32.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>tracert 201.32.1.2

Tracing route to 201.32.1.2 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      10.32.4.1
  2    0 ms      0 ms      0 ms      14.32.0.1
  3    0 ms      0 ms      0 ms      15.32.0.4
  4    0 ms      0 ms      0 ms      201.32.1.2

Trace complete.
```

- **Explications :**
  - Par la commande ping 201.32.1.2, on remarque que la connexion a été établie entre le pc du site 3 et le client ipv4, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.
  - Pour la commande tracert 201.32.1.2, 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 client ipv4(201.32.1.2). Ce qui prouve que la connectivité est assurée.

Test N°05

Accéder au serveur Web du site principal à partir de la machine client_ipv4 201.32.1.2

- **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
- **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=10ms TTL=124
Reply from 11.32.0.4: bytes=32 time<1ms TTL=124
Reply from 11.32.0.4: bytes=32 time<1ms TTL=124
Reply from 11.32.0.4: bytes=32 time<1ms 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 = 0ms, Maximum = 10ms, Average = 2ms
```

```
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      1 ms      0 ms      15.32.0.1
  3    0 ms      0 ms      4 ms      11.32.0.4
  4    1 ms      0 ms      0 ms      11.32.0.4
  5    0 ms      0 ms      0 ms      11.32.0.4

Trace complete.
```

- **Explications :**
  - Par la commande ping 11.32.0.4, on remarque que la connexion a été établie entre le pc client ipv4 et le serveur web1, 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.

2. Tests Ipv6

a. Plan de tests

N° Test	Description du test	Objectif	Les résultats attendus
1	Accéder à une machine de site 2 à partir de site 1	Vérifiez le bon fonctionnement du tunneling ipv6 over ipv4 et le respect de la contrainte de passer par le site principal	Succès du requête 'tracert' et les paquets passent par CE_site1, la 2ème extrémité du tunnel reliant CE_site1 et CE_site_principal puis la 2ème extrémité du tunnel reliant CE_site_principal et CE_site2.
2	Accéder à une machine de site 3 à partir de site 1.	Vérifiez le bon fonctionnement du tunneling ipv6 over ipv4 et le respect de la contrainte de passer par le site principal.	Succès du requête 'tracert' et les paquets passent par CE_site1, la 2ème extrémité du tunnel reliant CE_site1 et CE_site_principal puis la 2ème extrémité du tunnel reliant CE_site_principal et CE_site3.
3	Accéder au serveur web ipv6 à partir de site 1.	Vérifiez le bon fonctionnement du tunneling ipv6 over ipv4 et le respect de la contrainte de passer par le site principal.	Succès du requête 'tracert' et les paquets passent par CE_site1, la 2ème extrémité du tunnel reliant CE_site1 et CE_site_principal puis la 2ème extrémité du tunnel reliant CE_site_principal et R_internet_ipv6.
4	Accéder à une machine de site 3 à partir de site 2.	Vérifiez le bon fonctionnement du tunneling ipv6 over ipv4 et le respect de la contrainte de passer par le site principal.	Succès du requête 'tracert' et les paquets passent par CE_site2, la 2ème extrémité du tunnel reliant CE_site2 et CE_site_principal puis la 2ème extrémité du tunnel reliant CE_site_principal et CE_site3.
5	Accéder au serveur web ipv6 à partir de site 2.	Vérifiez le bon fonctionnement du tunneling ipv6 over ipv4 et le respect de la contrainte de passer par le site principal.	Succès du requête 'tracert' et les paquets passent par CE_site2, la 2ème extrémité du tunnel reliant CE_site2 et CE_site_principal puis la 2ème extrémité du tunnel reliant CE_site_principal et R_internet_ipv6.
6	Accéder au serveur web ipv6 à partir de site 3.	Vérifiez le bon fonctionnement du tunneling ipv6 over ipv4 et le respect de la contrainte de passer par le site principal.	Succès du requête 'tracert' et les paquets passent par CE_site3, la 2ème extrémité du tunnel reliant CE_site3 et CE_site_principal puis la 2ème extrémité du tunnel reliant CE_site_principal et R_internet_ipv6.
7	Accéder au serveur WEB1 à partir de site 1.	Vérifiez que les serveurs internes sont visibles de l'extérieur en ipv6.	Accéder correctement au serveur Web1.
8	Accéder au serveur WEB1 à partir de site 2.	Vérifiez que les serveurs internes sont visibles de l'extérieur en ipv6.	Accéder correctement au serveur Web1.
9	Accéder au serveur WEB1 à partir de site 3.	Vérifiez le bon fonctionnement du tunneling ipv6 over ipv4.	Succès du 'ping ' entre la machine du site 3 et le site principal.
10	Accéder au site principal à partir de la machine client_ipv6.	Vérifiez le bon fonctionnement du tunneling ipv6 over ipv4.	Succès du 'ping ' entre la machine client_ipv6 et le site principal.
11	Accéder à une machine de sous réseau 80 machines à partir de S/R 25 machines	Vérifier le bon fonctionnement de l'adressage ipv6 intra-site (i.e. inter sous réseau)	Succès du 'ping' entre la machine de S/R 80 et la machine de S/R 25.

b. Exécution du plan de tests

Test N°01

Accéder à une machine de site 2 à partir de site 1

- **Commandes utilisées :**
  - tracert 2001 :DB8 :32 :3000 :2E0 :F9FF :FE0C :8A04
- **Résultats obtenus :**

```
C:\>tracert 2001:DB8:32:3000:2E0:F9FF:FE0C:8A04

Tracing route to 2001:DB8:32:3000:2E0:F9FF:FE0C:8A04 over a maximum
of 30 hops:

  1    1 ms     0 ms     0 ms     2001:DB8:32:2000::1
  2    0 ms     0 ms     0 ms     2001:DB8:32:5002::1
  3   10 ms    11 ms    11 ms     2001:DB8:32:5003::2
  4   10 ms    11 ms    10 ms     2001:DB8:32:3000:2E0:F9FF:FE0C:
8A04

Trace complete.
```

- **Explications :**
  - Avec tracert 2001 :DB8 :32 :3000 :2E0 :F9FF :FE0C :8A04 , on s'assure que la connectivité a bien été établie. De plus on s'assure que le chemin suivi par les paquets est correct (la contrainte de passer par le site principale)
    - ➔ Les paquets passent par l'interface d'entrée 2001 : DB8 :32 :2000 ::1 (CE_site1)
    - ➔ Puis par l'arrivé du tunnel (Tunnel2) qui a comme adresse ipv6 2001 :DB8 :32 :5002 ::1 dans CE_Site_Principal
    - ➔ Puis le paquet est envoyé vers la destination du tunnel (Tunnel3) qui a comme adresse ipv6 2001 :DB8 :32 :5003 ::2 dans CE_Site2
    - ➔ Et puis la machine de site2 qui a comme adresse ipv6 2001 :DB8 :32 :3000 :2E0 :F9FF :FE0C :8A04 Ce qui prouve que la connectivité est assurée.

Test N°02

Accéder à une machine de site 3 à partir de site 1

- **Commandes utilisées :**
  - tracert 2001 :DB8 :32 :4000 :250 :FFF :FEE6 :4D40
- **Résultats obtenus :**

```
C:\>tracert 2001:DB8:32:4000:250:FFF:FEE6:4D40

Tracing route to 2001:DB8:32:4000:250:FFF:FEE6:4D40 over a maximum
of 30 hops:

  1    1 ms      0 ms      0 ms      2001:DB8:32:2000::1
  2    0 ms     10 ms      0 ms      2001:DB8:32:5002::1
  3   13 ms     11 ms     11 ms      2001:DB8:32:5001::2
  4   10 ms     10 ms     13 ms
2001:DB8:32:4000:250:FFF:FEE6:4D40

Trace complete.
```

- **Explications :**
  - Avec tracert 2001 :DB8 :32 :4000 :250 :FFF :FEE6 :4D40, on s'assure que la connectivité a bien été établie. De plus on s'assure que le chemin suivi par les paquets est correct (la contrainte de passer par le site principale)

    ➔ Les paquets passent par l'interface d'entrée
    2001 : DB8 :32 :2000 ::1 (CE_site1)

    ➔ Puis par l'arrivé du tunnel (Tunnel2) qui a comme adresse ipv6 2001 :DB8 :32 :5002 ::1 dans CE_Site_Principal

    ➔ Puis le paquet est envoyé vers la destination du tunnel (Tunnel1) qui a comme adresse ipv6 2001 :DB8 :32 :5001 ::2 dans CE_Site3

    ➔ Et puis la machine de site3 qui a comme adresse ipv6 2001 :DB8 :32 :4000 :250 :FFF :FEE6 :4D40 .Ce qui prouve que la connectivité est assurée.

Test N°03

Accéder au serveur web ipv6 à partir de site 1

- **Commandes utilisées :**
  - tracert 2001 :1 :2 :32 ::3
- **Résultats obtenus :**

```
C:\>tracert 2001:1:2:32::3

Tracing route to 2001:1:2:32::3 over a maximum of 30 hops:

  1    2 ms      0 ms      0 ms      2001:DB8:32:1002::1
  2    0 ms      0 ms      6 ms      2001:DB8:32:1000::2
  3    0 ms      0 ms      18 ms     2001:DB8:32:5000::5
  4    1 ms      15 ms     13 ms     2001:1:2:32::3

Trace complete.
```

- **Explications :**
  - Avec tracert 2001 :1 :2 :32 ::3 , on s'assure que la connectivité a bien été établie. De plus on s'assure que le chemin suivi par les paquets est correct (la contrainte de passer par le site principale)

    ➔ Les paquets passent par l'interface d'entrée 2001 : DB8 :32 :2000 ::1 (CE_site1)

    ➔ Puis par l'arrivé du tunnel (Tunnel2) qui a comme adresse ipv6 2001 :DB8 :32 :5002 ::1 dans CE_Site_Principal

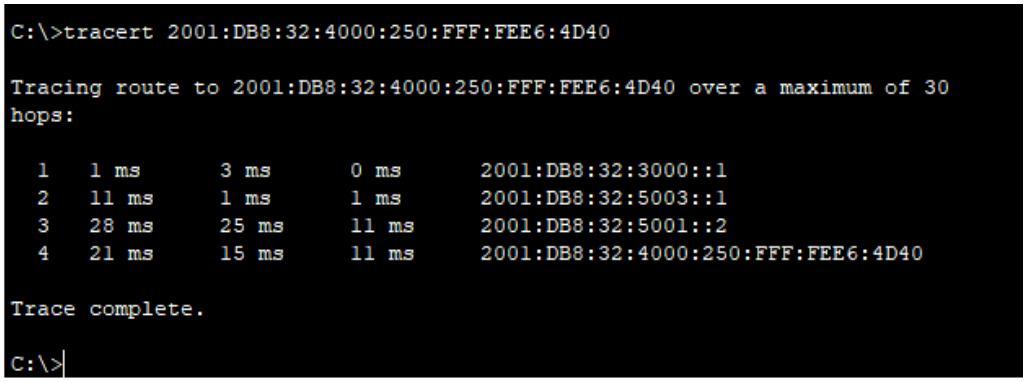
    ➔ Puis le paquet est envoyé vers la destination du tunnel (Tunnel0) qui a comme adresse ipv6 2001 :DB8 :32 :5000 ::5 dans CE_Site3

    ➔ Et puis le serveur web ipv6 qui a comme adresse ipv6 2001 :1 :2 :32 ::3 .Ce qui prouve que la connectivité est assurée.

Test N°04

Accéder au site 3 à partir de site 2

- **Commandes utilisées :**
  - tracert 2001 :DB8 :32 :4000 :250 :FFF :FEE6 :4D40
- **Résultats obtenus :**



- **Explications :**

  L'objectif de la commandes tracert 2001 :DB8 :32 :4000 :250 :FFF :FEE6 :4D40 est de s'assurer de la connectivité ainsi que la contrainte de passage par site principale a été bien effectué, donc le bon acheminement des paquets.

  ➔ Les paquets passent par l'interface d'entrée 2001 :DB8 :32 :3000 ::1 (CE_Site2)

  ➔ Comme le réseau de l'ISP est en ipv4, on doit utiliser le tunnel ipv6ip(Tunnel 3) vers l'adresse 5001 :DB8 :32 :5003 ::1 dans CE_site_principal

  ➔ Le paquet ensuite utilise le tunnel 1 vers l'adresse 5001 :DB8 :32 :5001 ::2

  ➔ Puis la machine de site 3 qui a l'adresse 2001 :DB8 :32 :4000 :250 :FFF :FEE6 :4D40

Test N°05

Accéder à internet ipv6 à partir de site 2

- **Commandes utilisées :**
  - tracert 2001 :1 :2 :32 ::3
- **Résultats obtenus :**

```
C:\>tracert 2001:1:2:32::3

Tracing route to 2001:1:2:32::3 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      2001:DB8:32:3000::1
  2    10 ms     12 ms     10 ms     2001:DB8:32:5003::1
  3    11 ms     14 ms     12 ms     2001:DB8:32:5000::5
  4    13 ms     10 ms     14 ms     2001:1:2:32::3

Trace complete.
```

- **Explications :**
  L'objectif de la commandes tracert 2001 :1 :2 :32 ::3 est de s'assurer de la connectivité ainsi que la contrainte de passage par site principale a été bien effectué, donc le bon acheminement des paquets.
  - ➔ Les paquets passent par l'interface d'entrée 2001 :DB8 :32 :3000 ::1 (CE_Site2)
  - ➔ Comme le réseau de l'ISP est en ipv4, on doit utiliser le tunnel ipv6ip (Tunnel 3) vers l'adresse 5001 :DB8 :32 :5003 ::1 dans CE_site_principal
  - ➔ Le paquet ensuite utilise le tunnel 1 vers l'adresse 5001 :DB8 :32 :5000::5
  - ➔ Puis la machine de site 3 qui a l'adresse 2001 :1 :2 :32 ::3

Test N°06

Accéder à internet ipv6 à partir de site 3

- **Commandes utilisées :**
  - tracert 2001 :1 :2 :32 ::3
- **Résultats obtenus :**

```
C:\>tracert 2001:1:2:32::3

Tracing route to 2001:1:2:32::3 over a maximum of 30 hops:

  1    1 ms      0 ms      1 ms      2001:DB8:32:4000::1
  2    12 ms     12 ms     10 ms     2001:DB8:32:5001::1
  3    13 ms     12 ms     25 ms     2001:DB8:32:5000::5
  4    15 ms     12 ms     12 ms     2001:1:2:32::3

Trace complete.
```

- **Explications :**
  L'objectif de la commandes tracert 2001 :1 :2 :32 ::3 est de s'assurer de la connectivité ainsi que la contrainte de passage par site principale a été bien effectué, donc le bon acheminement des paquets.
  - ➔ Les paquets passent par l'interface d'entrée 2001 :DB8 :32 :4000 ::1 (CE_Site3)
  - ➔ Comme le réseau de l'ISP est en ipv4, on doit utiliser le tunnel ipv6ip (Tunnel 1) vers l'adresse 5001 :DB8 :32 :5001 ::1 dans CE_site_principal
  - ➔ Le paquet ensuite utilise le tunnel 0 vers l'adresse 5001 :DB8 :32 :5000 ::5
  - ➔ Puis la machine de site 3 qui a l'adresse 2001 :1 :2 :32 ::3

Test N°07

Accéder au serveur WEB1 à partir de site 1

- **Commandes utilisées :**
  - Ping 2001 :DB8 :32 :1001 :260 :47FF :FE8E :B016
- **Résultats obtenus :**

```
C:\>ping 2001:DB8:32:1001:260:47FF:FE8E:B016

Pinging 2001:DB8:32:1001:260:47FF:FE8E:B016 with 32 bytes of data:

Reply from 2001:DB8:32:1001:260:47FF:FE8E:B016: bytes=32 time=23ms
TTL=125
Reply from 2001:DB8:32:1001:260:47FF:FE8E:B016: bytes=32 time=13ms
TTL=125
Reply from 2001:DB8:32:1001:260:47FF:FE8E:B016: bytes=32 time=12ms
TTL=125
Reply from 2001:DB8:32:1001:260:47FF:FE8E:B016: bytes=32 time=11ms
TTL=125

Ping statistics for 2001:DB8:32:1001:260:47FF:FE8E:B016:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 23ms, Average = 14ms
```

- **Explications :**
  - Par la commande
    ping 2001 :DB8 :32 :1001 :260 :47FF :FE8E :B016 , on remarque que la connexion a été établie entre le pc du site 1 et le serveur WEB1, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.

Test N°08

Accéder au serveur WEB1 à partir de site 2

- **Commandes utilisées :**
  - Ping 2001 :DB8 :32 :1001 :260 :47FF :FE8E :B016
- **Résultats obtenus :**

```
C:\>ping 2001:DB8:32:1001:260:47FF:FE8E:B016

Pinging 2001:DB8:32:1001:260:47FF:FE8E:B016 with 32 bytes of data:

Reply from 2001:DB8:32:1001:260:47FF:FE8E:B016: bytes=32 time=10ms
TTL=125
Reply from 2001:DB8:32:1001:260:47FF:FE8E:B016: bytes=32 time=12ms
TTL=125
Reply from 2001:DB8:32:1001:260:47FF:FE8E:B016: bytes=32 time=10ms
TTL=125
Reply from 2001:DB8:32:1001:260:47FF:FE8E:B016: bytes=32 time=11ms
TTL=125

Ping statistics for 2001:DB8:32:1001:260:47FF:FE8E:B016:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 12ms, Average = 10ms
```

- **Explications :**
  - Par la commande
    ping 2001 :DB8 :32 :1001 :260 :47FF :FE8E :B016 , on remarque que la connexion a été établie entre le pc du site 2 et le serveur WEB1, en effet 4 paquets ont été envoyés et le serveur les a reçus correctement.

Test N°09

Accéder au serveur web1 à partir de site 3

- **Commandes utilisées :**
  - tracert 2001 :db8 :32 :1001::2
- **Résultats obtenus :**

```
C:\>tracert 2001:DB8:32:1001::2

Tracing route to 2001:DB8:32:1001::2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      2001:DB8:32:4000::1
  2    13 ms     11 ms     10 ms     2001:DB8:32:5001::1
  3    0 ms      13 ms     19 ms     2001:DB8:32:1000::1
  4    11 ms     10 ms     15 ms     2001:DB8:32:1001::2

Trace complete.
```

- **Explications :**

  L'objectif de la commandes tracert 2001 :db8 :32 :1001::2 est de s'assurer de la connectivité ainsi que la contrainte de passage par site principale a été bien effectué, donc le bon acheminement des paquets.

  ➔ Les paquets passent par l'interface d'entrée 2001 :DB8 :32 :4000 ::1 (CE_Site3)

  ➔ Comme le réseau de l'ISP est en ipv4, on doit utiliser le tunnel ipv6ip (Tunnel 1) vers l'adresse 2001 :DB8 :32 :5001 ::1 dans CE_site_principal

  ➔ Le paquet ensuite passe vers le routeur interne via 2001 :DB8 :32 :1000 ::1

  ➔ Puis la serveur web1 qui a l'adresse 2001 :DB8 :32 :1001 ::2

Test N°10

Accéder serveur web1 à partir de client ipv6

- **Commandes utilisées :**
  - Ping 2001 :1 :2 :32 ::3
- **Résultats obtenus :**

```
C:\>ping 2001:DB8:32:1001::2

Pinging 2001:DB8:32:1001::2 with 32 bytes of data:

Reply from 2001:DB8:32:1001::2: bytes=32 time=10ms TTL=125
Reply from 2001:DB8:32:1001::2: bytes=32 time=10ms TTL=125
Reply from 2001:DB8:32:1001::2: bytes=32 time=14ms TTL=125
Reply from 2001:DB8:32:1001::2: bytes=32 time=12ms TTL=125

Ping statistics for 2001:DB8:32:1001::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 14ms, Average = 11ms
```

- **Explications :**

  L'objectif de la commandes ping 2001 :1 :2 :32 ::3 est de s'assurer de la connectivité entre client ipv6 et serveur web1.

  On remarque que la connectivité a été bien établie. En effet pour les quatre paquets envoyés on a reçu quatre.

Test N°11

Accéder à une machine de sous réseau 80 machines à partir de S/R 25 machines

- **Commandes utilisées :**
  - Ping 2001 :DB8 :32 :1004 :201 :C7FF :FEB5 :95DB
- **Résultats obtenus :**

```
C:\>ping 2001:DB8:32:1004:201:C7FF:FEB5:95CB

Pinging 2001:DB8:32:1004:201:C7FF:FEB5:95CB with 32 bytes of data:

Reply from 2001:DB8:32:1004:201:C7FF:FEB5:95CB: bytes=32 time=3ms
TTL=127
Reply from 2001:DB8:32:1004:201:C7FF:FEB5:95CB: bytes=32 time<1ms
TTL=127
Reply from 2001:DB8:32:1004:201:C7FF:FEB5:95CB: bytes=32 time=15ms
TTL=127
Reply from 2001:DB8:32:1004:201:C7FF:FEB5:95CB: bytes=32 time=1ms
TTL=127

Ping statistics for 2001:DB8:32:1004:201:C7FF:FEB5:95CB:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 4ms
```

- **Explications :**

  L'objectif de la commandes ping est de s'assurer de la connectivité à l'intérieur de site principale.

  On remarque que la connectivité a été bien établie, pour les 4 paquet envoyé 4 sont reçus.

VI. Conclusion

En guise de point final à notre travail, nous tenions à vous remercier pour la confiance placée en nous pour la prise en charge de votre réseau et son évolution. Ce fut un projet très enrichissant pour nous au niveau individuel et en tant qu'équipe. Nous espérons que vous serez autant satisfaits du résultat obtenu que les personnes qui ont œuvré à sa réalisation.