Correction du sujet Projet CFI (Centre de Formation Informatique)

Etape 1 :

Objectif : Mise en œuvre de RIPng et diffusion des routes connectées.

Avant toute chose, il faudra activer sur chaque routeur le routage IPv6 :

Router(config)# ipv6 unicast-routing

L'activation de RIPng se fait de manière différente en Ipv6 qu'en IPv4.

Il est nécessaire d'associer à RIP un processus, ce que nous ne faisions pas en IPv4. Cette notion de processus nous permet d'activer plusieurs instances RIP sur un routeur et donc de pouvoir le gérer comme d'autres protocoles de routage (par exemple OSPF avec ses numéros de process)

L'activation du processus se fait de la manière suivante :

Router(config)# ipv6 router rip dunkirk (dunkirk représente le nom du processus associé à RIP)

Il faut maintenant redistribuer les routes connectées et non déclarer les réseaux et interfaces par lesquelles nous diffusons les MAJ du protocole RIP comme en IPv4.

Router(config-router)# redistribute connected

Dans le cas du routeur frontière (Border Router) il peut aussi être intéressant de redistribuer les routes statiques ou routes par défaut.

Router(config-router)# redistribute static

Ensuite nous allons définir sur quelles interfaces nous devons diffuser les MAJ RIPng

Router(config-if)#ipv6 rip dunkirk enable (Dunkirk représente le nom du process)

Pour redistribuer uniquement la route par défaut, placer vous sur l'interface et entrez la commande suivante :

Router(config-if)#ipv6 rip dunkirk default-information originate (Dunkirk représente le nom du process)

A ce stade, les trois routeurs doivent être en mesure d'échanger leurs tables de routage et leurs routes connectées. Pour visualiser celle-ci :

Router# show IPv6 route

Les routes apprises par RIP apparaissent dans la table de routage avec le préfixe R comme en IPv4

Voici les configurations des 3 routeurs pour la configuration de RIP
(Nota : les parties ne concernant pas IPv6 et RIPng ont été effacées)

Border Router

```
border#sh run
Building configuration...

Current configuration : 1416 bytes
!
hostname border
!
ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
spanning-tree mode pvst
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 3001:100:100:100::254/64
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
ipv6 address 2001:2000:1999:1998::1/64
ipv6 rip dunkirk enable
ipv6 enable
clock rate 2000000
!
interface Serial0/1/0
no ip address
ipv6 address 2001:2000:1999:1997::1/64
ipv6 rip dunkirk enable
clock rate 2000000
!
interface Serial0/2/0
no ip address
ipv6 address 2002:22:66::1/64
```

```
clock rate 2000000
!
interface Serial0/3/0
ip address 64.66.68.129 255.255.255.252
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
ipv6 router rip dunkirk
redistribute static
redistribute connected
!
ip classless
```

Router Site A1

```
site_a_1#sh run
Building configuration...

version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname site_a_1
!
ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
spanning-tree mode pvst
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
encapsulation dot1Q 10
no ip address
ipv6 address 2010:70:90:25::254/64
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
no ip address
ipv6 address 2010:59:62:80::254/64
```

```
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1/0
no ip address
ipv6 address 2001:2000:1999:1997::2/64
ipv6 rip dunkirk enable
clock rate 2000000
!
interface Serial0/2/0
no ip address
ipv6 address 2001:2000:1999:1996::1/64
ipv6 rip dunkirk enable
clock rate 2000000
!
interface Serial0/3/0
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
ipv6 router rip dunkirk
redistribute connected
!
ip classless
!
```

Routeur Site A2

```
site_a_2#SH run
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname site_a_2
!
ip cef
ipv6 unicast-routing
```

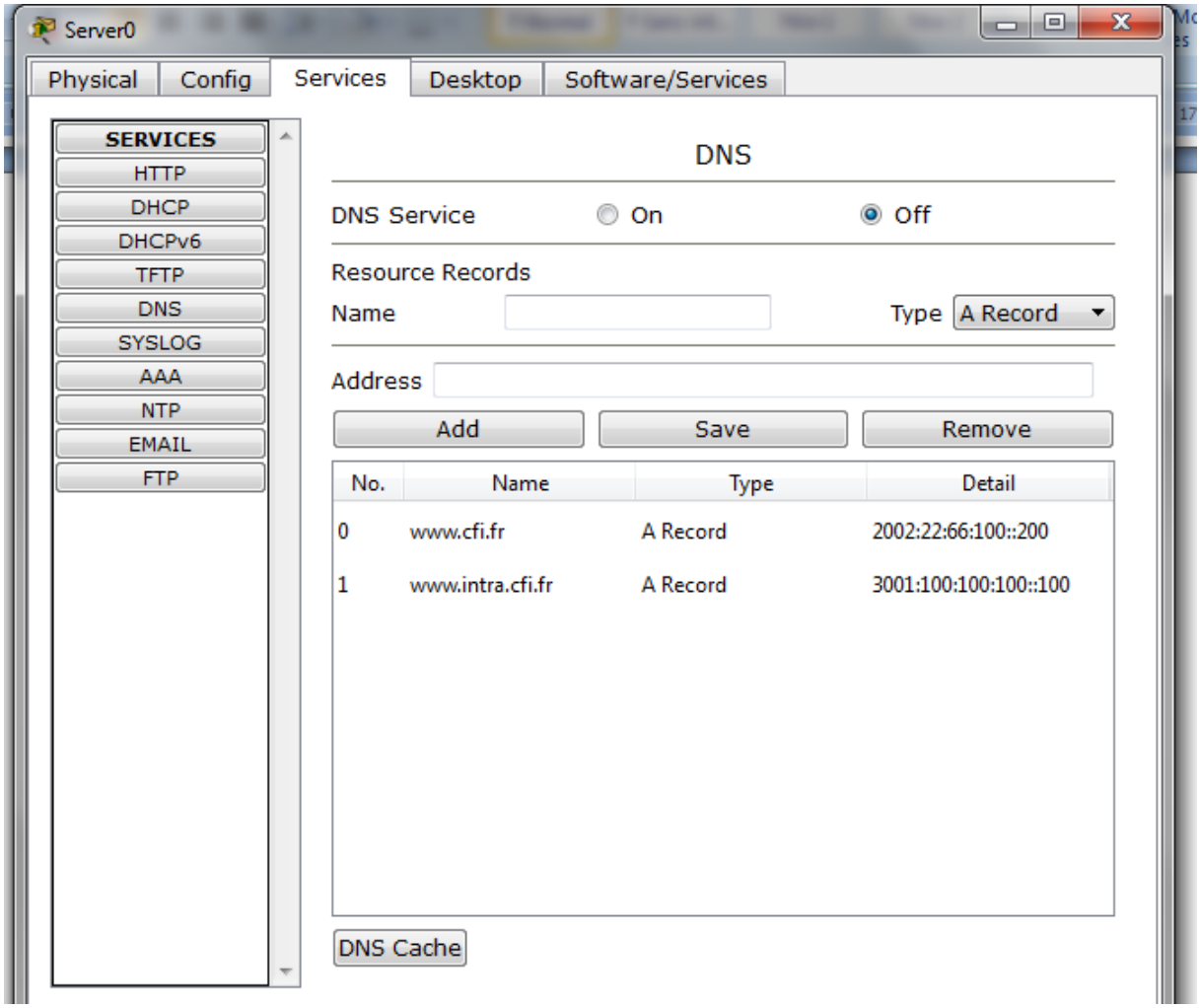
```
!
no ipv6 cef
!
spanning-tree mode pvst
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2002:22:2:66::254/64
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
ipv6 address 2001:2000:1999:1998::2/64
ipv6 rip dunkirk enable
clock rate 2000000
!
interface Serial0/1/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/2/0
no ip address
ipv6 address 2001:2000:1999:1996::2/64
ipv6 rip dunkirk enable
clock rate 2000000
!
interface Serial0/3/0
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
ipv6 router rip dunkirk
redistribute connected
!
ip classless
```

Etape 2 :

Objectif : Permettre aux hôtes du réseau d'accéder au serveur Web de l'intranet en utilisant une résolution DNS IPv6

Nota : La résolution DNS se fait en utilisant un pointeur de type AAAA pour IPv6 et A pour Ipv4. Ce type de pointeur n'existe pas encore sur Packet Tracer, mais cela fonctionne sans problème.

Sur le serveur DNS de l'architecture, vous devez activer le service DNS, puis entrer les enregistrements en saisissant le nom www.intra.cfi.fr puis l'adresse Ipv6 dans la zone Address et enfin appuyer sur le bouton Add



Ensuite, lorsque les postes auront été configurés vous pourrez atteindre le serveur Web avec son FQDN.

Nota : N'oubliez pas d'activer le service DNS sur le serveur, il est « off » par défaut

La partie adressage sur le Border routeur est détaillée dans la configuration précédente.

Etape 3 :

Objectif : Gestion du routage statique et mise en place d'une zone simulant Internet et un serveur WEB.

Le Border Router est connecté via son interface S0/2/0 au routeur du FAI. Dans notre cas il s'agit de simuler Internet.

S'agissant du Border router, nous devons implémenter une route par défaut pour pouvoir accéder à Internet. La syntaxe en Ipv4 était :

Router(config)# ip route 0.0.0.0 0.0.0.0 adresse du saut suivant ou interface de sortie.

En IPv6 la syntaxe est :

Router(config)#ipv6 route ::/0 du saut suivant ou interface de sortie.

Les :: représentent tous les bits d'adresse à zéro, le /0 tous les bits de préfixe à zéro.

Nota : Avec packet tracer, utilisez plutôt l'adresse du saut suivant, certains dysfonctionnements ont été constatés lors de l'utilisation de l'interface de sortie.

Concernant la configuration du routeur de l'ISP, il faudra aussi intégrer un routage statique pour qu'il puisse répondre aux requêtes sur le serveur WEB www.cfi.fr et insérer l'adresse dans le serveur DNS.

Voici la configuration du Routeur

ISP#sh run

```
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ISP
!
ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
spanning-tree mode pvst
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2002:22:66:100::254/64
!
```

```
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
ipv6 address 2002:22:66::2/64
clock rate 2000000
!
interface Serial0/1/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/2/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/3/0
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
ip flow-export version 9
!
ipv6 route ::/0 2002:22:66::1
!
```

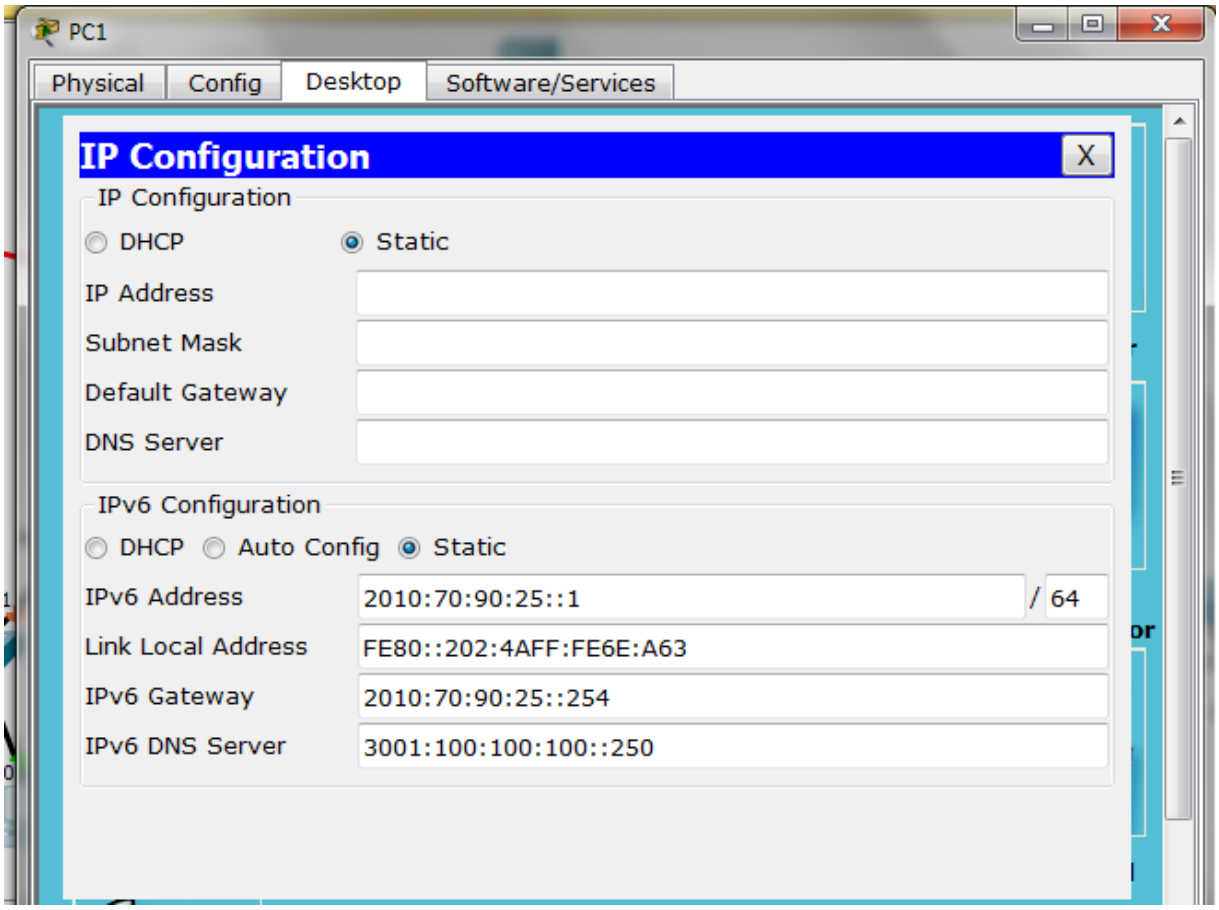
Etape 4 :

Objectif : Mise en œuvre des Vlans en Ipv6.

La gestion des Vlans au sein d'une architecture IPv6 se fait exactement de la même manière qu'en IPv4, seules les adresses différent.

Les étapes à suivre sont les suivantes :

Réaliser l'adressage Ipv6 sur les postes



A noter que nous utiliserons pour ces postes de l'adressage statique.
L'adresse de lien local (FE80 ::) est automatiquement générée en respectant le format EUI-64 modifié, vous n'avez donc pas à la gérer.

Sur le commutateur, il est nécessaire de configurer les ports connectés aux postes sur le bon Vlan.

Switch(config-if)# switchport mode access
Switch(config-if)# switchport access Vlan 10

Il faut aussi configure le port connecté au routeur en mode Trunk

Switch(config-if)# switchport mode trunk

Enfin sur le routeur nous utiliserons les sous-interfaces avec un adressage en IPv6.

Voici la configuration des interfaces

interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
encapsulation dot1Q 10
no ip address
ipv6 address 2010:70:90:25::254/64
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
no ip address
ipv6 address 2010:59:62:80::254/64
!

A l'issue de cette configuration les différents hôtes du Site_A1 doivent être capables de se « pinguer »

```
PC>ipv6config

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::202:4AFF:FE8D:2490
   IPv6 Address.....: 2010:59:62:80::2/64
   Default Gateway.....: 2010:59:62:80::254
   DHCPv6 Client DUID.....: 00-01-00-01-91-A6-56-EE-00-02-4A-8D-24-90

PC>ping 2010:70:90:25::1

Pinging 2010:70:90:25::1 with 32 bytes of data:

Reply from 2010:70:90:25::1: bytes=32 time=0ms TTL=127
Reply from 2010:70:90:25::1: bytes=32 time=0ms TTL=127
Reply from 2010:70:90:25::1: bytes=32 time=0ms TTL=127
Reply from 2010:70:90:25::1: bytes=32 time=0ms TTL=127

Ping statistics for 2010:70:90:25::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Etape 5 :

Objectif : Mettre en place un serveur DHCPv6 sur le routeur du site A2 afin de pouvoir affecter dynamiquement les adresses aux hôtes du LAN

Nota : Packet Tracer gère l'adressage DHCPv6 EUI-64 modifié, c'est-à-dire qu'il distribue le préfixe réseau IPv6 et génère l'adresse d'hôte à partir de son adresse MAC. Si vous effectuez cette configuration sur des machines physiques utilisant Windows 7 ou supérieur, le résultat sera différent, en effet la navigation anonyme IPv6 est activée par défaut, donc l'adresse de l'hote ne correspondra pas à son adresse MAC modifiée selon le protocole EUI-64

Autre élément important, il n'est pas possible de configurer la passerelle par défaut en IPv6, que ce soit sur un routeur ou sur un serveur. En effet, l'apprentissage de cette adresse se fera via le protocole NDP (Neighbor Discovery Protocol) et l'adresse de la gateway sera l'adresse locale (en FE80 ::) de la patte du routeur connecté au LAN

Comme en Ipv4 nous devons définir un pool d'adresse avec les options nécessaires (serveur DNS…)

Voici les opérations à effectuer :

Router(config)#ipv6 dhcp pool Site_A2 (où Site_A2 représente le nom du pool)

Nous devons ensuite le pool local qui sera employé pour donner le préfixe aux clients

Router(config-dhcp)#prefix-delegation pool global_site_A2

Puis définir les options comme dans tout serveur DHCP, ici nous nous contenterons du serveur DNS

Router(config-dhcp)#dns-server 3001:100:100:100::250

Le préfixe que nous distribuerons au client sera en 64 bits.

Dans la définition du préfixe de site nous distinguerons deux parties le préfixe global et le préfixe du client.

Router(config)#ipv6 local pool global_site_A2 2002:22:2:66::/48 64

/48 représente le préfixe global, ou le préfixe de site. En règle générale un FAI attribue aux clients un préfixe de site sur 48 ou 56 bits, et le client peut ensuite le subdiviser en différents réseau pour son adressage interne. Les sous réseaux sont crées sur les 16 ou 8 bits restant.

/64 représente la longueur du préfixe qui sera attribuée à l'hôte, respectant ainsi les RFC

En IPv4, le fait d'activer un serveur DHCP sur le routeur fait que celui-ci répondra à toutes les requêtes DHCP Discover sur toutes les interfaces. En IPv6, il faut préciser l'interface sur laquelle le serveur DHCP sera activé par la commande :

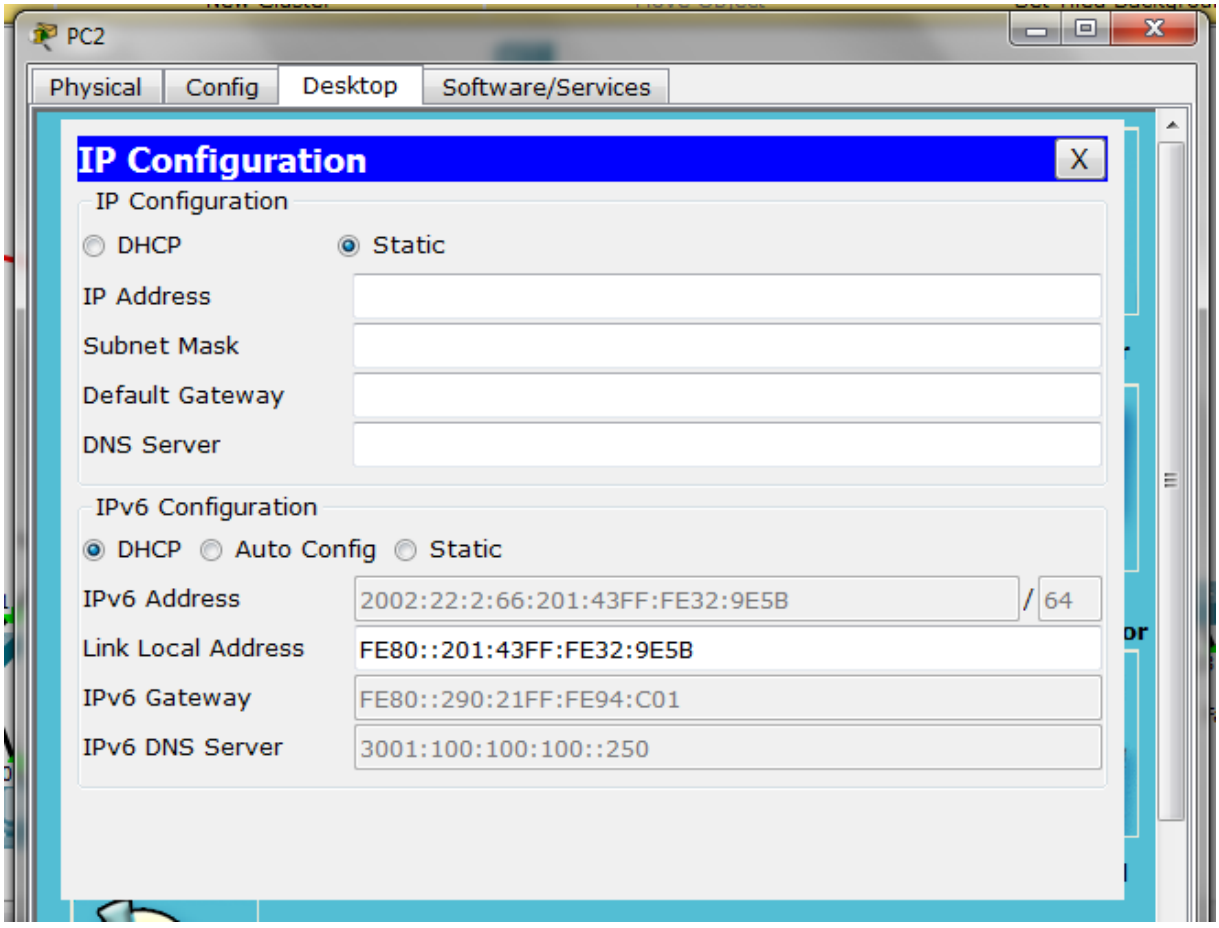
Router(config-if)# ipv6 dhcp server Site_A2 (nom du pool que nous avons crée précédemment)

Voici la configuration complète de l'interface :

interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2002:22:2:66::254/64
ipv6 dhcp server Site_A2

A noter qu'il faut aussi attribuer à l'interface une adresse IPv6 reprenant le préfixe distribué.

Concernant l'adressage des postes, il faut les passer en DHCP IPv6

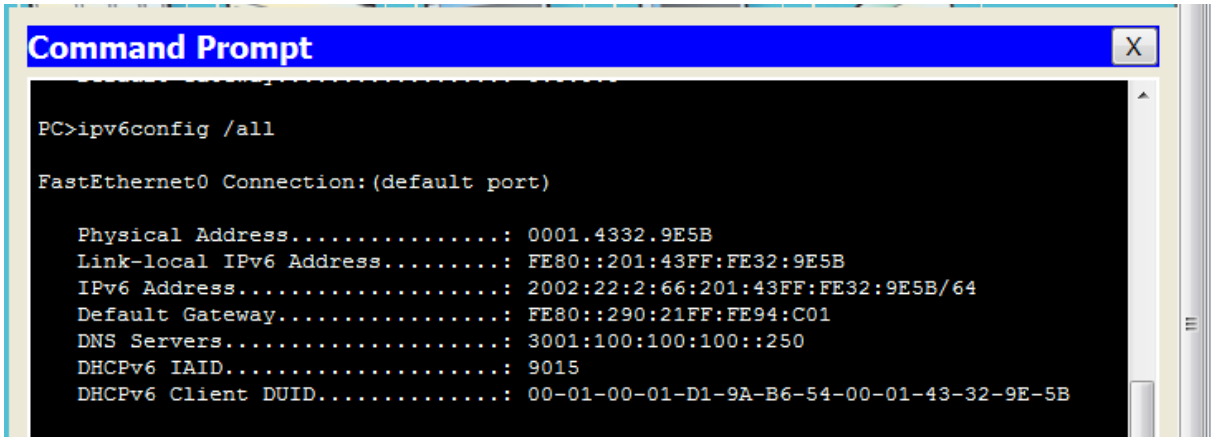


Regardons en détail la configuration obtenue par l'ordinateur.

Son adresse Ipv6 reprend bien le préfixe distribué par le routeur à savoir 2002 :22 :2 :66 ::/64
L'adresse de l'hôte est 201 :43FF :FE32 :9E5B
Cette adresse est définie en respectant le format des adresses EUI64 modifié
Le principe est d'attribuer l'adresse d'hôte en la calculant à partir de son adresse MAC

L'adresse MAC d'un Hôte est sur 48bits et se décompose en 24 bits pour l'OUI et 24 bits pour la carte.
Le préfixe distribué par le serveur DHCP v6 est 64 bits.
L'adresse d'hôte doit donc être sur 64 bits aussi.
L'adresse MAC étant sur 48 bits, il manque donc 16 bits.
Le principe est donc d'insérer FFFE entre les 24 bits de l'OUI et les 24 bits de la carte

Regardons l'adresse MAC de l'hôte



Son adresse physique est 0001.4332.9E5B

Si nous séparons l'OUI et l'adresse de la carte nous arrivons à
OUI : 0001.43
Adresse de la carte 32.9E5B

La norme EUI64 modifié, impose de modifier le bit U/L (Universal/Local) à 1 lors du calcul de l'adresse IPv6. Ce bit est à 0 (zéro) pour indiquer une adresse MAC locale (non modifiée) et est le 7ème bit du premier octet de l'OUI.

Le premier octet de notre hôte est 00, passons le 7ème bit à 1, nous arrivons donc à 0000 0010 en binaire. Convertissons-le en hexadécimal 02, puis calculons l'adresse de l'hôte
0201 :43FF :FE32 :9B5E

Les zéros non significatifs dans une adresse IPv6 peuvent être supprimés, nous arrivons donc à : 201 :43FF :FE32 :9B5E

Et nous pouvons donc vérifier l'adresse de l'hôte en rajoutant le préfixe distribué par le serveur DHCP (2002 :22 :2 :66 ::) donc son adresse est bien
2002 :22 :2 :66 :201 :43FF :FE32 :9B5E

L'adresse de lien local est calculée de la même manière en rajoutant le préfixe FE80 ::/64 devant.

Nota : Navigation anonyme

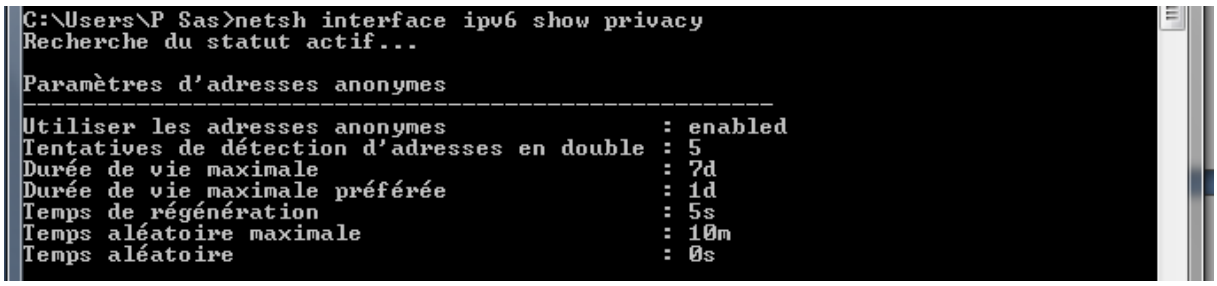
Packet Tracer reprend le fonctionnement de la norme EUI-64 modifié, mais si nous regardons sur un PC, nous constaterons que la partie hôte ne reprend pas l'adresse MAC. En effet les systèmes d'exploitation reprennent le principe de la navigation anonyme.

Il s'agit d'un principe de sécurité informatique pour éviter que l'on puisse suivre l'activité d'un ordinateur et ceci quelque soit le réseau Ipv6 auquel il est connecté.

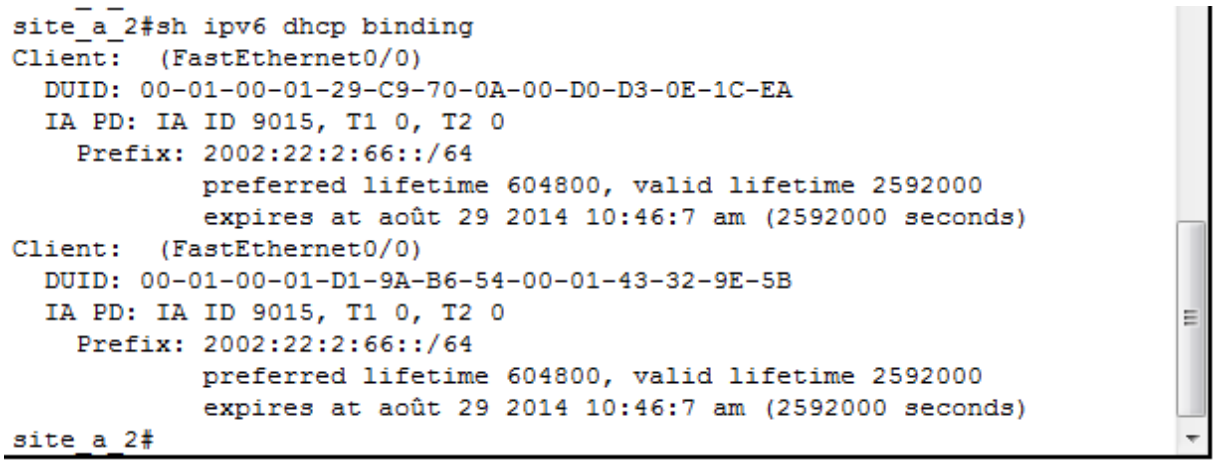
Une machine qui se connecte à un réseau IPv6 en DHCP adaptera son préfixe en fonction du serveur, mais ne changera pas d'adresse d'hôte, elle devient donc repérable en fonction de cette adresse qui n'est pas modifiée parce qu'elle est dérivée de son adresse MAC.

Cette option est activée par défaut sous Windows 7 et supérieur.

Pour visualiser celle-ci la commande à entrer est **netsh interface IPv6 show privacy**



Pour vérifier l'attribution de l'adresse IPv6 au client par le serveur DHCP, entrez la commande suivante :



Chaque client du serveur DHCP est repéré par un DUID (DHCP Unique Identifier) que nous retrouvons à la fois sur le routeur mais aussi sur le client (voir le résultat de la commande ipv6config)

```
site_a_2#sh ipv6 interface brief
FastEthernet0/0            [up/up]
    FE80::290:21FF:FE94:C01
    2002:22:2:66::254
FastEthernet0/1            [administratively down/down]
Serial0/0/0                [up/up]
    FE80::260:47FF:FEC9:CC33
    2001:2000:1999:1998::2
Serial0/1/0                [administratively down/down]
Serial0/2/0                [up/up]
    FE80::209:7CFF:FED6:1ED7
    2001:2000:1999:1996::2
Serial0/3/0                [administratively down/down]
Vlan1                      [administratively down/down]
```

Enfin nous pouvons remarquer que le client DHCP à pour passerelle par défaut l'adresse IPv6 locale du serveur DHCP et ceci pour l'interface qui distribue les adresses (FastEthernet 0/0 dans notre exemple) et que l'adresse du serveur DNS reprend bien celle que nous avons défini dans les options du pool DHCP.

Etape 6 :

Objectif : Cette étape sert à simuler la connexion entre les 2 sites de l'entreprise en IPv4.
Nous nous serviront ensuite de ce lien pour faire transiter du trafic IPv6 dans un tunnel IPv4.

Voici les configurations à effectuer sur les routeurs :

Sur le border routeur

interface Serial0/3/0
ip address 64.66.68.129 255.255.255.252
clock rate 2000000

N'oublions de configurer la route pour le traffic IPv4

ip route 0.0.0.0 0.0.0.0 64.66.68.130

Sur le routeur du site B

interface Serial0/0/0
ip address 64.66.68.130 255.255.255.252
clock rate 2000000

Et la route par défaut.

ip route 0.0.0.0 0.0.0.0 64.66.68.129

Vérification de la connectivité :

site_b#ping 64.66.68.129

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.66.68.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/25/67 ms

Etape 7 :

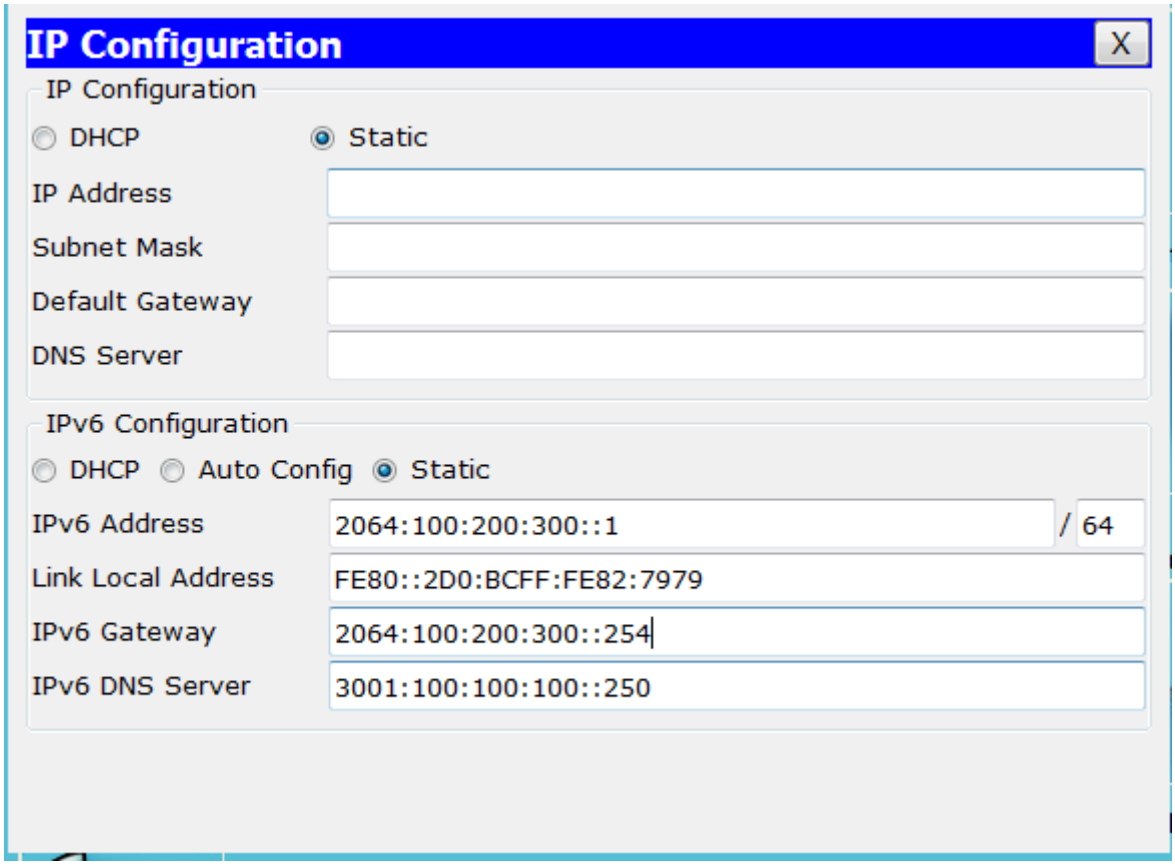
Objectif : Cette étape sert unique ment à préparer les Site B, à faire l'adressage des postes, de l'interface du routeur

Configuration du routeur :

ipv6 unicast-routing

interface FastEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2064:100:200:300::254/64

Adressage d'un poste :



Etape 8 :

Objectif : Mise en place d'un tunnel permettant l'encapsulation d'un trafic IPv6 sur un lien IPv4

Sur chacun des routeurs, nous allons définir une interface de tunnel permettant d'atteindre l'objectif.

Le plan d'adressage est fourni à savoir 2345 :1200 :2400 :3600 ::1 pour le bordeur routeur et 2345 :1200 :2400 :3600 ::2 pour le site B

La création de l'interface de tunnel doit définir la source de celui-ci (interface) et la destination (adresse IPv4 de l'autre extrémité)

Il faut aussi définir l'adresse IPv6 de l'interface Tunnel et enfin le mode transport dans le tunnel dans notre exemple ipv6ip pour encapsuler le trafic IPv6 dans un paquet Ipv4.

Configuration sur le border Routeur

```
interface Tunnel10
no ip address
mtu 1476
ipv6 address 2345:1200:2400:3600::1/64
tunnel source Serial0/3/0
tunnel destination 64.66.68.130
tunnel mode ipv6ip
```

La commande gérant le MTU de l'interface est automatiquement ajoutée à la configuration de l'interface Tunnel.
La diminution du MTU s'explique par l'ajout de l'entête IPV4 au paquet IPv6.

Configuration sur le routeur du site B

```
interface Tunnel10
no ip address
mtu 1476
ipv6 address 2345:1200:2400:3600::2/64
tunnel source Serial0/0/0
tunnel destination 64.66.68.129
tunnel mode ipv6ip
```

Lors de la configuration vous aurez un message d'information concernant le passage à Up de l'interface tunnel10

Vous pouvez aussi le vérifier de cette manière :

```
border#show ipv6 interface brief
FastEthernet0/0            [up/up]
    FE80::204:9AFF:FEC2:AD01
    3001:100:100:100::254
FastEthernet0/1            [administratively down/down]
Serial0/0/0                [up/up]
    FE80::202:16FF:FE66:9861
    2001:2000:1999:1998::1
Serial0/1/0                [up/up]
    FE80::204:9AFF:FE66:12C9
    2001:2000:1999:1997::1
Serial0/2/0                [up/up]
    FE80::201:96FF:FE28:3433
    2002:22:66::1
Serial0/3/0                [up/up]
Tunnel10                   [up/up]
    FE80::2E0:F9FF:FEB9:34E2
    2345:1200:2400:3600::1
Vlan1                      [administratively down/down]
```

Etape 9 :

Objectif : Gestion du routage sur le Border router et sur le routeur du site B

Nous simulons un lien internet entre les deux sites. Nous ne pouvons donc pas activer de protocole de routage dynamique entre les deux routeurs, nous devons juste définir les routes statiques.

Commençons par le routeur du Site B.

Nous devons uniquement définir une route par défaut pour tous les réseaux IPv6 par l'adresse IPv6 du border routeur de l'interface Tunnel

Site_B(config)# ipv6 route ::/0 2345:1200:2400:3600::1

Sur le Border routeur la situation est plus complexe.

Il est connecté à Internet IPv6 via l'ISP

Il a donc une route par défaut :

Border(config)# ipv6 route ::/0 2002:22:66::2

Il doit aussi pouvoir atteindre le site B par le tunnel

Border(config)# ipv6 route 2064:100:200:300::/64 2345:1200:2400:3600::2

Nous ne devons pas ajouter de route sur les autres routeurs de l'architecture, la redistribution de la route se fera automatiquement via le RIPng puisque nous avions ajouté la redistribution des routes statiques dans sa configuration.

ipv6 router rip dunkirk
redistribute static
redistribute connected

Pour vérifier notre configuration nous allons procéder par étape.

Vérification de la connectivité dans le tunnel

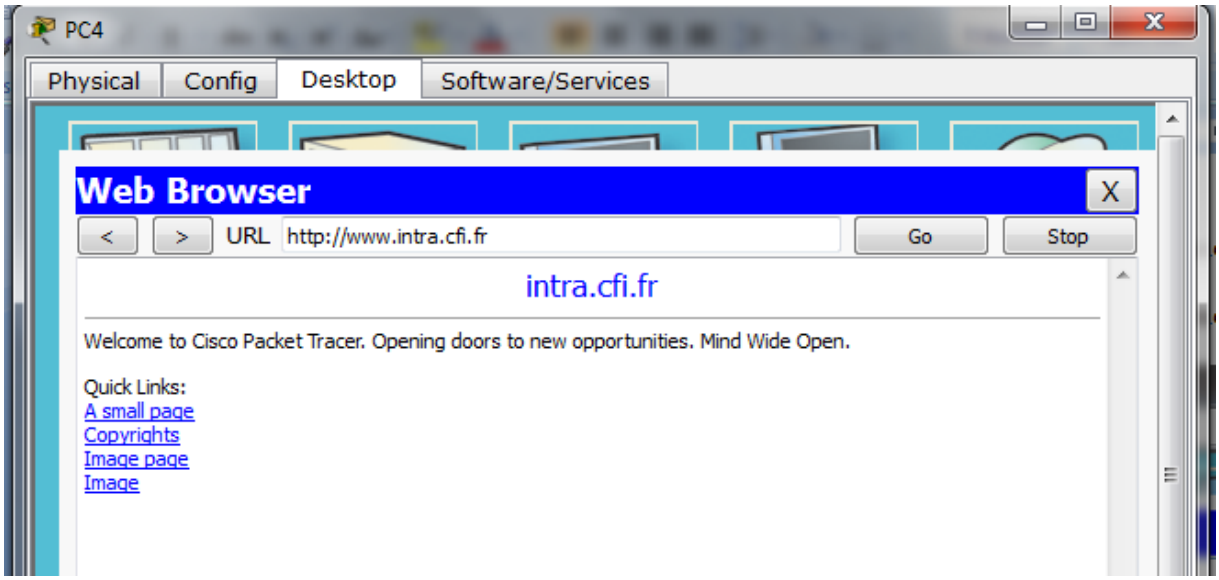
```
site_b#ping 2345:1200:2400:3600::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2345:1200:2400:3600::1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/11/21 ms

site_b#sh ipv6 int br
FastEthernet0/0            [up/up]
    FE80::202:4AFF:FE85:CE01
    2064:100:200:300::254
FastEthernet0/1            [administratively down/down]
Serial0/0/0                [up/up]
Serial0/1/0                [administratively down/down]
Serial0/2/0                [administratively down/down]
Serial0/3/0                [administratively down/down]
Tunnel10                   [up/up]
    FE80::201:64FF:FE26:1A49
    2345:1200:2400:3600::2
Vlan1                      [administratively down/down]
```

Vérifier la résolution DNS sur le site B

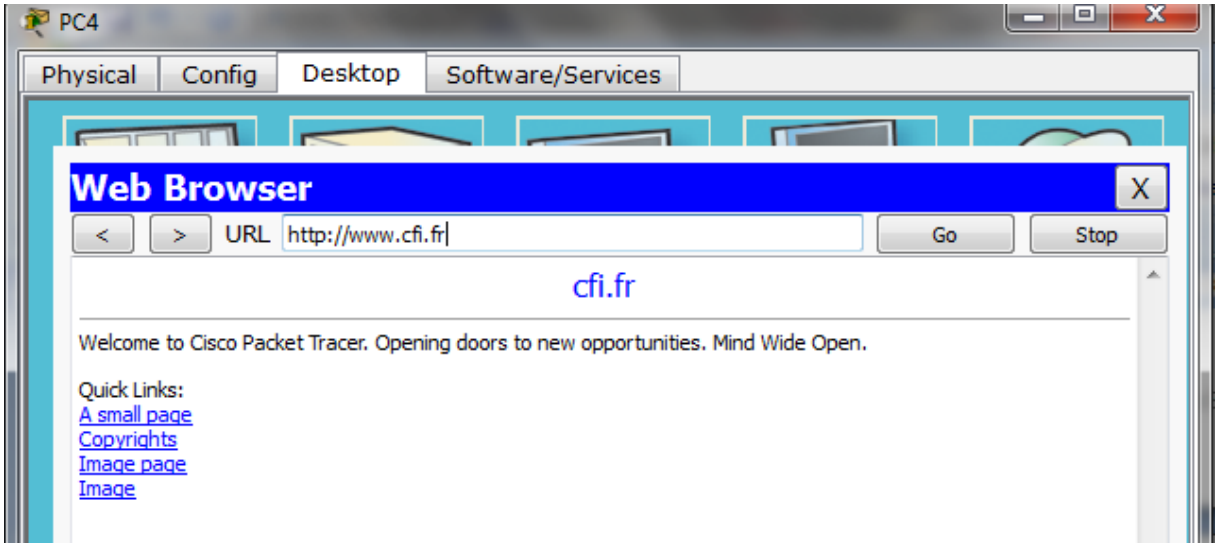
A partir d'un des postes sur le site B

```
PC>ping www.cfi.fr

Pinging 2002:22:66:100::200 with 32 bytes of data:

Reply from 2002:22:66:100::200: bytes=32 time=10ms TTL=125
Reply from 2002:22:66:100::200: bytes=32 time=2ms TTL=125
Reply from 2002:22:66:100::200: bytes=32 time=2ms TTL=125
Reply from 2002:22:66:100::200: bytes=32 time=2ms TTL=125

Ping statistics for 2002:22:66:100::200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 4ms

PC>ping www.intra.cfi.fr

Pinging 3001:100:100:100::100 with 32 bytes of data:

Reply from 3001:100:100:100::100: bytes=32 time=9ms TTL=126
Reply from 3001:100:100:100::100: bytes=32 time=1ms TTL=126
Reply from 3001:100:100:100::100: bytes=32 time=1ms TTL=126
Reply from 3001:100:100:100::100: bytes=32 time=1ms TTL=126

Ping statistics for 3001:100:100:100::100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 9ms, Average = 3ms
```

Vérification de la possibilité de se connecter au serveur intranet



Vérification de la possibilité de se connecter au serveur internet



Etape 10 :

Objectif : Mise en œuvre des ACLs (listes de contrôle d'accès) en IPv6

Dans notre projet, nous avons mis en œuvre des Vlans comme nous le faisons en entreprise.

Ils sont sur le site A1 et nous avons les Vlans 10 et 20

L'adressage du Vlan 10 est 2010:70:90:25::/64

L'adressage du Vlan 20 est 2010:59:62:80::/64

Nous allons maintenant définir des restrictions pour chacun des Vlans, le Vlan 10 peut uniquement consulter le site intranet de l'entreprise, le Vlan 20 lui peut consulter l'intranet mais aussi aller sur Internet, que nous simulons avec le serveur Web www.cfi.fr

Mise en œuvre des ACLs

Les principes de base des ACLs restent les mêmes, à savoir la création se fait en mode de configuration globale, ensuite nous affectons les ACLs sur les interfaces en IN ou en OUT.

Les access-lists IPv6 sont nommées et se définissent de la même manière qu'une ACL étendue nommée en IPv4

La syntaxe pour la création d'un access-list est

Router(Config)# ipv6 access-list nom de l'access-list

Ensuite nous devons définir les autorisations (permit) et les interdictions (deny)

Nous pouvons employer les mêmes abréviations qu'en IPv4 (any, host) et les mêmes opérateur 'eq, neq, lt,gt)

Les wildcards ne sont plus employés et nous définissons le préfixe à filtrer à l'aide du / et du nombre de bits à vérifier.

Dans notre projet nous allons autoriser le VLAN 10 (2010 :70 :90 :25 ::/64) à consulter le serveur Web www.intra.cfi.fr sur les ports 80 et 443, mais aussi à faire des requêtes DNS sur le serveur 3001 :100 :100 :100 ::250

L'access-list s'appellera acces-intranet

La configuration sera la suivante

```
site_a_1(config)#ipv6 access-list acces-intranet
site_a_1(config-ipv6-acl)#permit udp 2010:70:90:25::/64 host 3001:100:100:100::250 eq 53
site_a_1(config-ipv6-acl)#permit tcp 2010:70:90:25::/64 3001:100:100:100::/64 eq 80
site_a_1(config-ipv6-acl)#permit tcp 2010:70:90:25::/64 3001:100:100:100::/64 eq 443
site_a_1(config-ipv6-acl)#deny ipv6 any any
site_a_1(config-ipv6-acl)#exit
```

L'étape suivante est l'affectation de l'accès list à la sous interface la plus proche de la source, comme en IPv4, à savoir la sous-interface Fa 0/0.10

L'instruction à employer

Router(config-subif)# ipv6 traffic-filter nom de l'access-list IN (or OUT)

Configuration du routeur :

```
site_a_1(config)#interface fa0/0.10
site a 1(config-subif)#ipv6 traffic-filter acces-intranet in
```

Vérifions que l'ACL a bien été affecté à la sous-interface à l'aide de la commande Show IPv6 interface :

```
site_a_1#sh ipv6 interface
FastEthernet0/0.10 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::205:5EFF:FED9:EC01
  No Virtual link-local address(es):
  Global unicast address(es):
    2010:70:90:25::254, subnet is 2010:70:90:25::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:254
    FF02::1:FFD9:EC01
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  Input features: Access List
  Inbound access list acces-intranet
```

La dernière ligne nous indique que l'ACL acces-intranet a été affectée sur l'interface en inbound.

Il nous faut aussi vérifier l'ACL

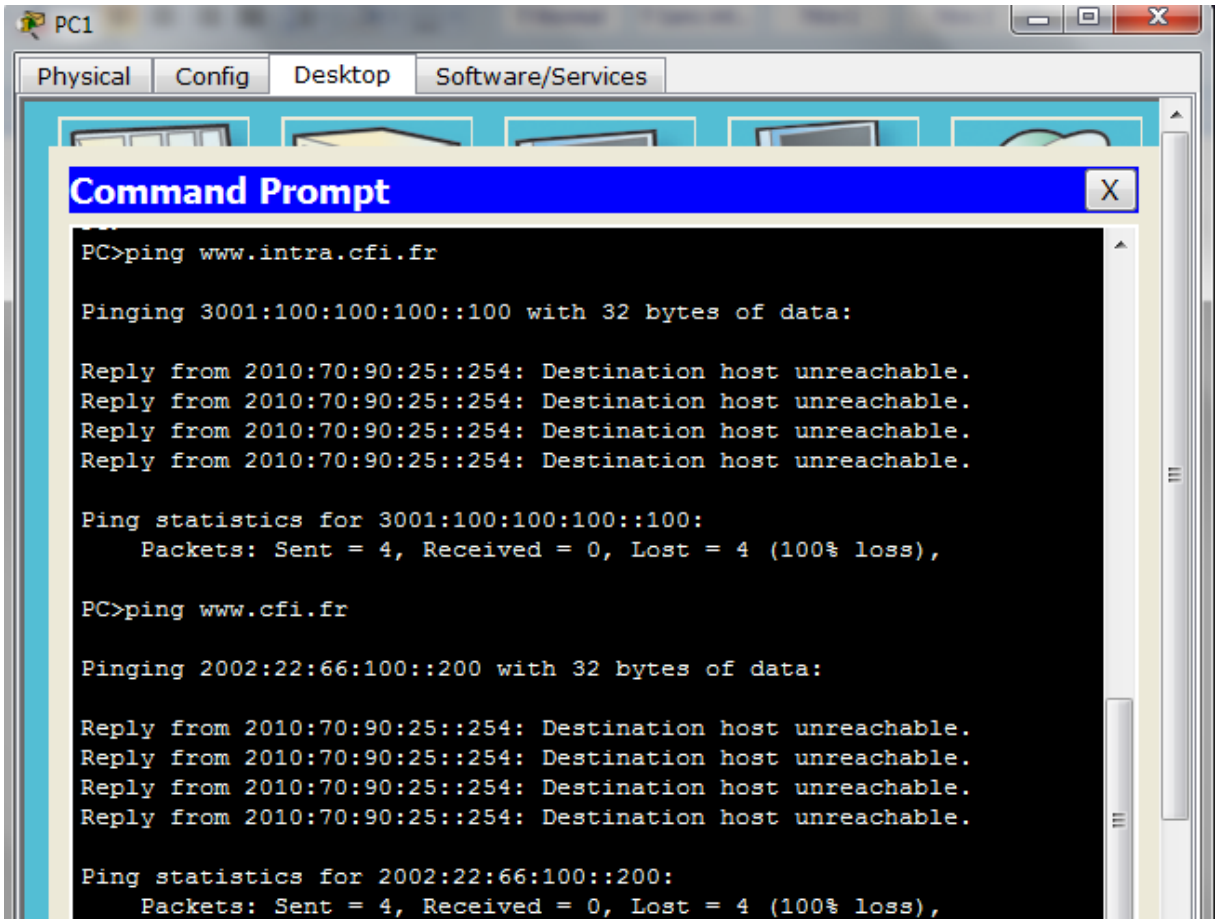
La commande est pratiquement identique à celle en IPv4 : show ipv6 access-list

```
site_a_1#sh ipv6 access-list
IPv6 access list acces-intranet
    permit udp 2010:70:90:25::/64 host 3001:100:100:100::250 eq domain (4 match(es))
    permit tcp 2010:70:90:25::/64 3001:100:100:100::/64 eq www (5 match(es))
    permit tcp 2010:70:90:25::/64 3001:100:100:100::/64 eq 443
    deny ipv6 any any (8 match(es))
```

Comme en IPv4, nous pouvons connaitre les lignes de l'ACL qui ont été employées (Match(es))

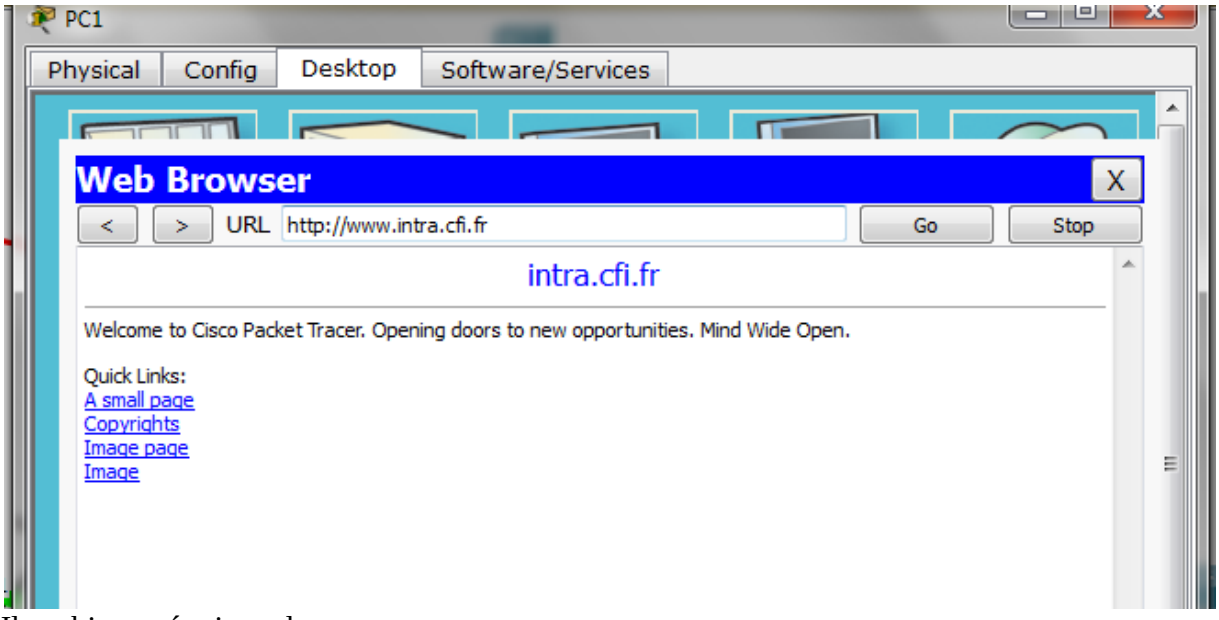
Vérifions maintenant que notre ACL fonctionne correctement.

Tout d'abord la résolution DNS



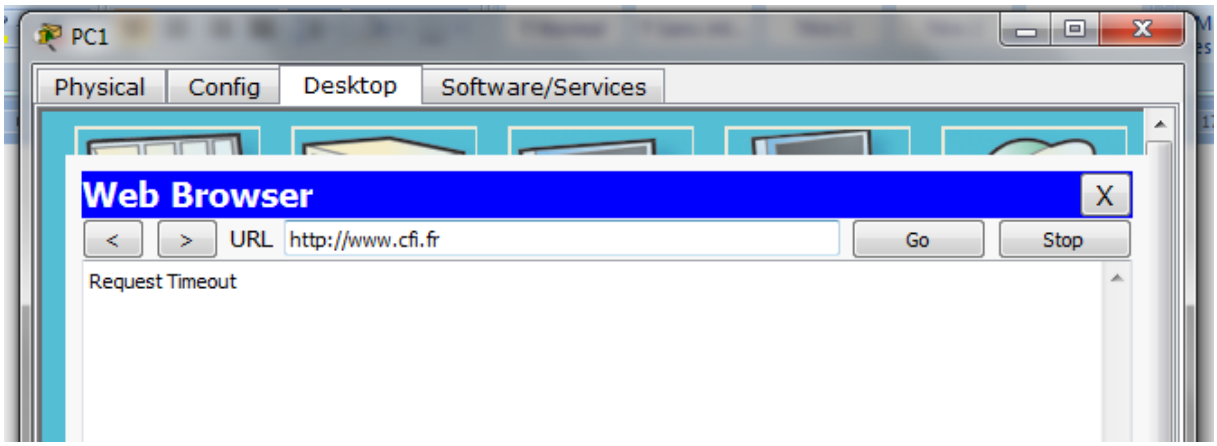
La résolution fonctionne bien, mais les hôtes ne répondent pas, le protocole ICMP n'ayant pas été autorisé dans l'ACL

Vérifions l'accès à l'intranet



Il est bien opérationnel

Maintenant l'accès à Internet



Il est bien refusé, donc notre access-list est bien opérationnelle.