19/08/2024

Atelier 00 – activité 2 : NAT - RIP

**Document de l’atelier :**

[Bloc2\_sem3-4\_Atelier-00-activite-1\_Inter-VLAN\_Routing Challenge.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-1_Inter-VLAN_Routing%20Challenge.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-2\_Découverte-NAT-RIP-01.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-2_Découverte-NAT-RIP-01.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-3-Map-a-Network-Using-CDP.docx](file:///C:\\Users\\Utilisateur\\Desktop\\Cour\\BTS%20SIO\\2e_annee\\Réseau\\Atelier\\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\\Fini\\Bloc2_sem3-4_Atelier-00-activite-3-Map-a-Network-Using-CDP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-4-Configure-CDP-and-LLDP.docx](file:///C:\\Users\\Utilisateur\\Desktop\\Cour\\BTS%20SIO\\2e_annee\\Réseau\\Atelier\\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\\Fini\\Bloc2_sem3-4_Atelier-00-activite-4-Configure-CDP-and-LLDP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-5-Configure-and-Verify-NTP.docx](file:///C:\\Users\\Utilisateur\\Desktop\\Cour\\BTS%20SIO\\2e_annee\\Réseau\\Atelier\\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\\Fini\\Bloc2_sem3-4_Atelier-00-activite-5-Configure-and-Verify-NTP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-6-reconstruction-reseau.docx](file:///C:\\Users\\Utilisateur\\Desktop\\Cour\\BTS%20SIO\\2e_annee\\Réseau\\Atelier\\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\\Fini\\Bloc2_sem3-4_Atelier-00-activite-6-reconstruction-reseau.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-7-Syslog-NTP-and-SSH-debut .pka](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-7-Syslog-NTP-and-SSH-debut%20.pka)

[Bloc2\_sem3-4\_Atelier-00-activite-8-Troubleshoot-VTP-and-DTP.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-8-Troubleshoot-VTP-and-DTP.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-9-SSH-sur-routeur-et-switch.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-9-SSH-sur-routeur-et-switch.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-10-authentification.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-10-authentification.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-11-authentification.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-11-authentification.docx)

[Bloc2\_sem3-4\_Atelier-00-activite-12-Data-Center-Exploration-Physical-Mode.docx](file:///C:\Users\Utilisateur\Desktop\Cour\BTS%20SIO\2e_annee\Réseau\Atelier\Atelier-00-1-sommaire-divers-protocoles_Adrien_Ventre\Fini\Bloc2_sem3-4_Atelier-00-activite-12-Data-Center-Exploration-Physical-Mode.docx)

Table des matières

[1. Objectifs 2](#_Toc176817473)

[2. Point de départ 2](#_Toc176817474)

[3. Première étape : Vérification de la connectivité des postes et des serveurs. 3](#_Toc176817475)

[1.1 Connectivité des postes et des serveurs vers leur passerelle 3](#_Toc176817476)

[1.2 Connectivité entre routeurs 4](#_Toc176817477)

[4. Deuxième étape : Mise en place des routes par défaut 6](#_Toc176817478)

[5. Troisième étape 7](#_Toc176817479)

[6. Explication de la mise en place du NAT 9](#_Toc176817480)

[1.1 Mise en œuvre du NAT dynamique 9](#_Toc176817481)

[1.2 Mise en œuvre du NAT statique 9](#_Toc176817482)

[1.3 Affichage des traductions actives 9](#_Toc176817483)

[7. Mise en place d’un NAT dynamique sur les routeurs terminaux RtA et RtF 10](#_Toc176817484)

[8. Quatrième étape 12](#_Toc176817485)

[9. Cinquième étape 14](#_Toc176817486)

[1.4 Partie B - Étude du fonctionnement du protocole RIP 14](#_Toc176817487)

[1.1.1 Vérifications des tables de routage 14](#_Toc176817488)

[1.1.2 Compréhension du protocole RIP 15](#_Toc176817489)

[1.1.3 Réajustement du protocole RIP, en cas de modification de la cartographie 17](#_Toc176817490)

[10. Sixième étape 22](#_Toc176817491)

[11. Septième étape 24](#_Toc176817492)

[12. Authentification OSPF 24](#_Toc176817493)

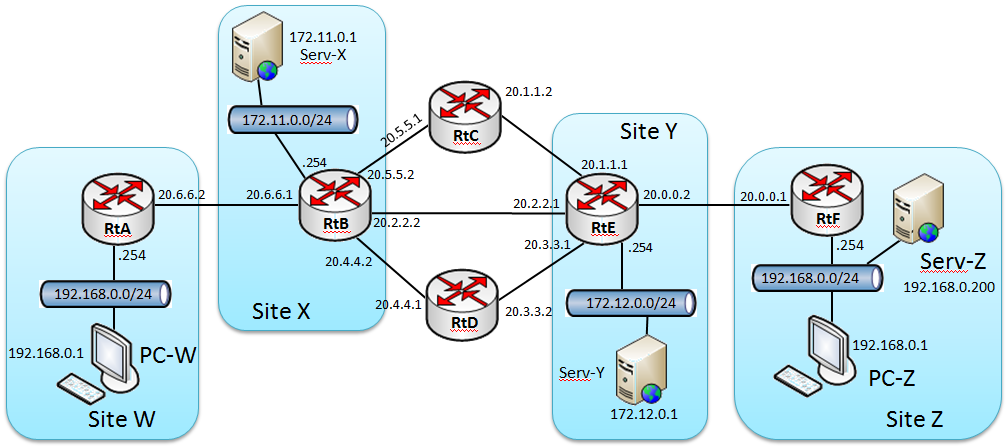
[13. Authentification EIGRP dans Packet Tracer 24](#_Toc176817494)

[14. Annex 25](#_Toc176817495)

# Objectifs

* **Mettre en place du NAT** sur deux sites distants « W » et « Z » qui communiquent via un réseau public de routeurs et qui sont dotés du même plan d’adressage en 192.168.0.0/24.
* **Mettre en place du routage dynamique** dans un réseau de routeurs et mettre en évidence la tolérance de panne.
* **Mettre en place du NAT statique** pour permettre l’accès extérieur à un serveur privé

# Point de départ



Le schéma comporte 4 sites. Les deux sites d’extrémité W et Z utilisent le même réseau 192.168.0.0/24. On peut assimiler ces deux sites à des particuliers dotés d’une « box ». Sur le site X, un réseau 172.11.0.0/24 comporte un serveur web Serv-X d’adresse 172.11.0.1. Sur le site Y, un autre serveur web (Serv-Y) est accessible à l’adresse 172.12.0.1 sur le réseau 172.12.0.0/24.

**Conséquence :**

Le protocole RIP n’est pas utilisable sur les sites terminaux W et Z, du fait de l’utilisation du même réseau IP par ces deux sites.

C’est tout l’objectif de cet atelier, qui va justement montrer comment activer le NAT ou le NAT/PAT (*Network Address Translation/ Port Address Translation*) sur les routeurs CISCO, pour masquer les adresses privées et permettre l’acheminement des requêtes vers ou depuis le réseau « public ».

Le fichier Packet Tracer de départ comporte des routeurs 1841 et des routeurs 2811 auxquels on a ajouté des modules NM4E pourvus de 4 interfaces Ethernet. Dans ce fichier, seules les interfaces ont été paramétrées selon le schéma ci-dessus.

**Tableau des réseaux de connexion entre routeurs**

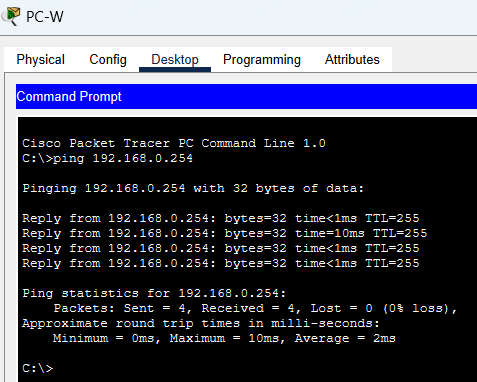
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Du routeur  vers le routeur** | **RtA** | **RtB** | **RtC** | **RtD** | **RtE** | **RtF** |
| RtA | - | 20.6.6.0/30 | - | - | - | - |
| RtB | 20.6.6.0/30 | - | 20.5.5.0/30 | 20.4.4.0/30 | 20.2.2.0/30 | - |
| RtC | - | 20.5.5.0/30 | - | - | 20.1.1.0/30 | - |
| RtD | - | 20.4.4.0/30 | - | - | 20.3.3.0/30 | - |
| RtE | - | 20.2.2.0/30 | 20.1.1.0/30 | 20.3.3.0/30 | - | 20.0.0.0/30 |
| RtF | - | - | - | - | 20.0.0.0/30 | - |

# Première étape : Vérification de la connectivité des postes et des serveurs.

## Connectivité des postes et des serveurs vers leur passerelle

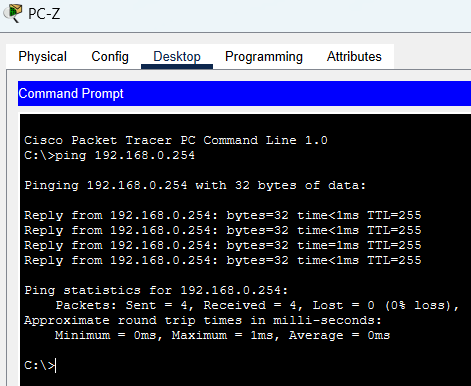
PC-W:

ping 192.168.0.254



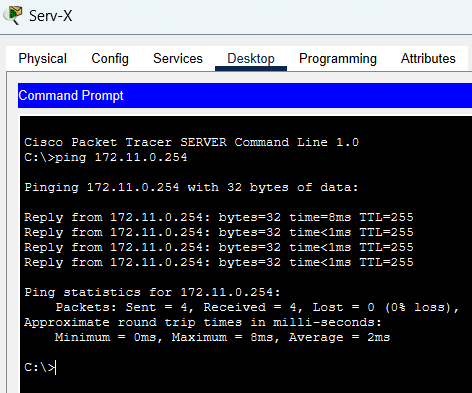
PC-Z:

ping 192.168.0.254



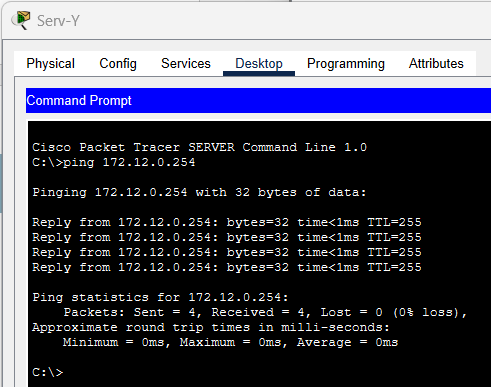
Server-X:

ping 172.11.0.254



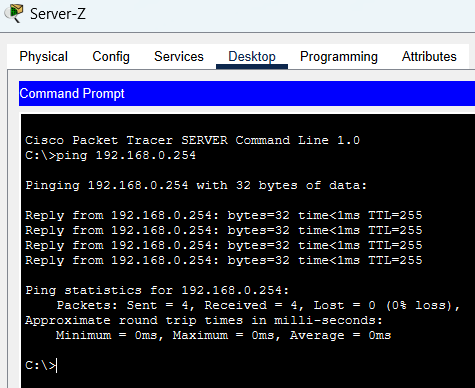
Server-Y:

ping 172.12.0.254



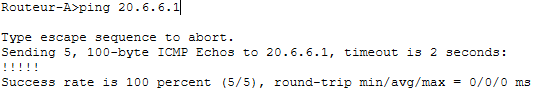
Server-Z:

ping 192.168.0.254

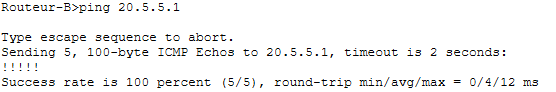


## Connectivité entre routeurs

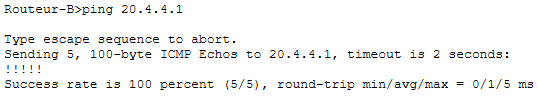
**Ping Router A à Router B : ping 20.6.6.1**

****

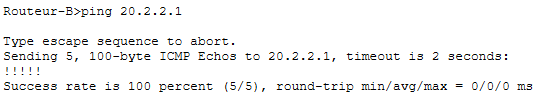
**Ping Router B à Router C : ping 20.5.5.1**

****

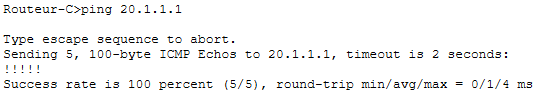
**Ping Router B à Router D : ping 20.4.4.1**

****

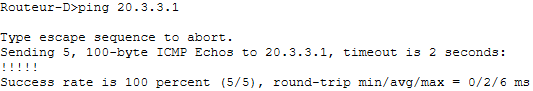
**Ping Router B à Router E : ping 20.2.2.1**

****

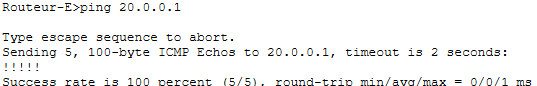
**Ping Router C à Router E : ping 20.1.1.1**

****

**Ping Router D à Router E : ping 20.3.3.1**

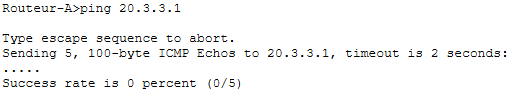
****

**Ping Router E à Router F : ping 20.0.0.1**

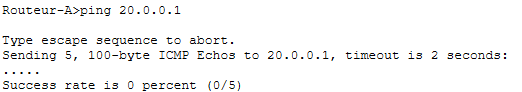
****

**Nous pouvons voir que les routeurs arriver à communiquer entre eux mais les router permettent d’aller d’un router a l’autre ne fonctionne pas.**

**Ping Router A à Router E : ping 20.3.3.1**

****

**Ping Router A à Router F : ping 20.0.0.1**

****

**Pour vérifier tout les apparie en script nous pouvons par exemple utiliser se script**

@echo off

echo Pinging Router A à Router B: ping 20.6.6.1

ping 20.6.6.1 -n 4

echo.

echo Pinging Router B à Router C: ping 20.5.5.2

ping 20.5.5.2 -n 4

echo.

echo Pinging Router B à Router D: ping 20.4.4.2

ping 20.4.4.2 -n 4

echo.

echo Pinging Router B à Router E: ping 20.2.2.1

ping 20.2.2.1 -n 4

echo.

echo Pinging Router C à Router E: ping 20.1.1.1

ping 20.1.1.1 -n 4

echo.

echo Pinging Router D à Router E: ping 20.3.3.1

ping 20.3.3.1 -n 4

echo.

echo Pinging Router E à Router F: ping 20.0.0.1

ping 20.0.0.1 -n 4

echo.

pause

# Deuxième étape : Mise en place des routes par défaut

Mettre en place les routes par défaut dans les routeurs terminaux RtA et RtF. Consultez ensuite la table de routage et vérifiez la présence de ces routes par défaut sur chaque routeur.

Pour maitre en place les routes par défaut sur les routeurs terminaux RtA et RtF il faut entre les commande suivant dans le CLI :

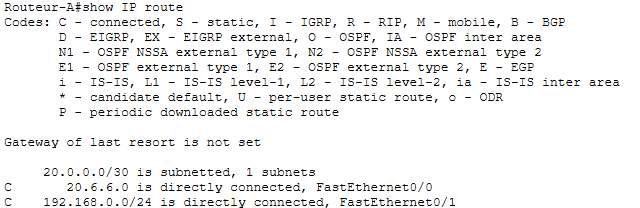
Pour RtA :

Routeur-A>en

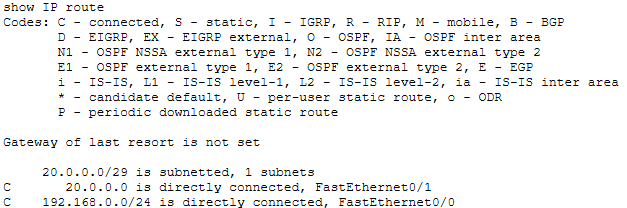
Routeur-A#conf

Routeur-A(config)#interface F0/0

Routeur-A(config-if)# ip route 20.6.6.0 255.255.255.0 20.6.6.2



Pour RtF :



# Troisième étape

Sur les routeurs terminaux RtA et RtF, mettre en place le NAT. À l’issue de cette étape, les postes clients des sites W et Z devront être capables de joindre le second routeur (RtB pour le site W et RtE pour le site Z). **Vous comprenez pourquoi** ?

Routeur-A>en

Routeur-A#conf

Routeur-A(config)#interface FastEthernet0/0

Routeur-A(config-if)#ip address 20.6.6.2 255.255.255.0

Routeur-A(config-if)#ip nat outside

Routeur-A(config-if)#exit

Routeur-A(config)#interface FastEthernet0/1

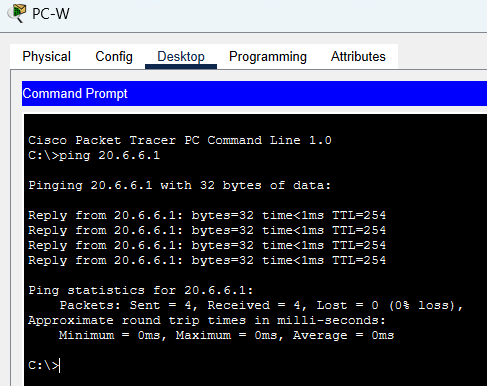
Routeur-A(config-if)#ip address 192.168.0.254 255.255.255.0

Routeur-A(config-if)#ip nat inside

Routeur-A(config-if)#exit

Routeur-A(config)#ip nat inside source static 192.168.0.254 20.6.6.2

Pour vérifier que tout fonctionne bien j’ai utilisé la commande ping de PC-W à RtB :



Routeur-F>en

Routeur-F#conf

Routeur-F(config)#interface FastEthernet0/1

Routeur-F(config-if)#ip address 20.0.0.1 255.255.255.0

Routeur-F(config-if)#ip nat outside

Routeur-F(config-if)#exit

Routeur-F(config)#interface FastEthernet0/0

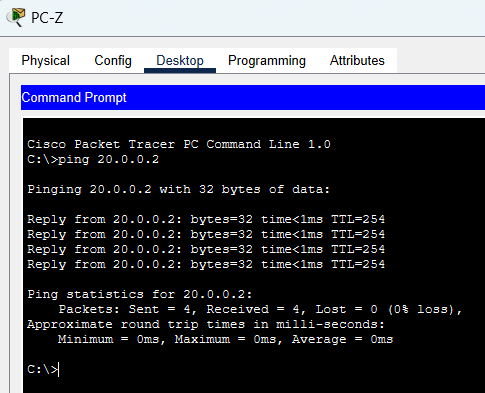
Routeur-F(config-if)#ip address 192.168.0.254 255.255.255.0

Routeur-F(config-if)#ip nat inside

Routeur-F(config-if)#exit

Routeur-F(config)#ip nat inside source static 192.168.0.254 20.0.0.1

Pour vérifier que tout fonctionne bien j’ai utilisé la commande ping de PC-Z à RtE :



# Explication de la mise en place du NAT

Le NAT (Network Address Translation) permet de traduire des adresses IP internes non routables en adresses externes uniques et routables, facilitant ainsi l'accès à Internet tout en atténuant la pénurie d'adresses IPv4. Il existe deux types de NAT :

* **NAT statique** : Associe une adresse IP publique fixe à une adresse IP privée. Cela ne résout pas le problème de pénurie d'adresses, car chaque machine nécessite une adresse publique unique.
* **NAT dynamique** : Utilise un pool d'adresses publiques pour attribuer dynamiquement des adresses IP aux machines internes. Le NAT dynamique permet de partager un nombre limité d'adresses IP publiques entre plusieurs machines internes. Le NAT/PAT (Port Address Translation) est une variante où une seule adresse publique est utilisée, avec des ports dynamiquement attribués pour identifier chaque connexion.

## Mise en œuvre du NAT dynamique

* **Configuration des interfaces** : Définir les interfaces internes et externes avec les commandes appropriées pour indiquer quelles interfaces sont ip nat inside et ip nat outside.
* **Création d'une ACL** : Autoriser les réseaux internes à utiliser le NAT en créant une liste d'accès (ACL) qui spécifie les adresses IP internes autorisées.
* **Activation du NAT** : Utiliser la commande pour activer le NAT, en spécifiant l'interface externe et en utilisant le mot-clé overload pour activer le PAT.
* Une alternative consiste à créer un pool d'adresses pour la translation, permettant plusieurs traductions simultanées.

## Mise en œuvre du NAT statique

* Le NAT statique permet de rediriger le trafic d'un serveur interne vers une adresse IP publique. Par exemple, une commande peut être utilisée pour rediriger le trafic HTTP (port 80) d'une adresse publique vers un serveur interne.

## Affichage des traductions actives

* La commande show ip nat translations permet de visualiser les traductions NAT actives, montrant les correspondances entre les adresses IP internes et externes, ainsi que les ports utilisés.

Le NAT dynamique, en utilisant le PAT, permet de gérer efficacement les connexions sortantes d'un réseau interne vers Internet, tout en maintenant une correspondance entre les requêtes et les réponses. La commande debug ip nat peut être utilisée pour surveiller la gestion des traductions NAT.

# Mise en place d’un NAT dynamique sur les routeurs terminaux RtA et RtF

Routeur-A>en

Routeur-A#conf

Routeur-A(config)#ip nat inside source list 1 interface F0/0 overload

Routeur-A(config)#access-list 1 permit 192.168.0.0 0.0.0.255

Routeur-A(config)#interface FastEthernet0/0

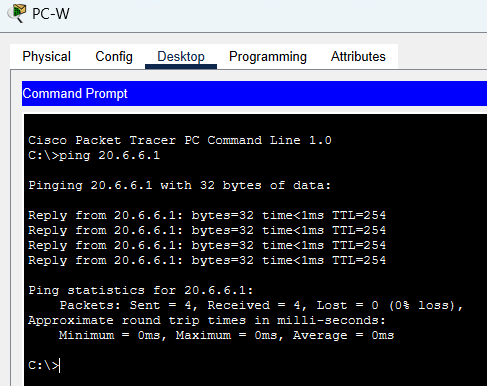
Routeur-A(config-if)#ip nat outside

Routeur-A(config-if)#exit

Routeur-A(config)#interface FastEthernet0/1

Routeur-A(config-if)#ip nat inside

Pour vérifier que tout fonctionne bien j’ai utilisé la commande ping de PC-W à RtB :



Routeur-F>en

Routeur-F#conf

Routeur-F(config)#ip nat inside source list 1 interface F0/1 overload

Routeur-F(config)#access-list 1 permit 192.168.0.0 0.0.0.255

Routeur-F(config)#interface F0/1

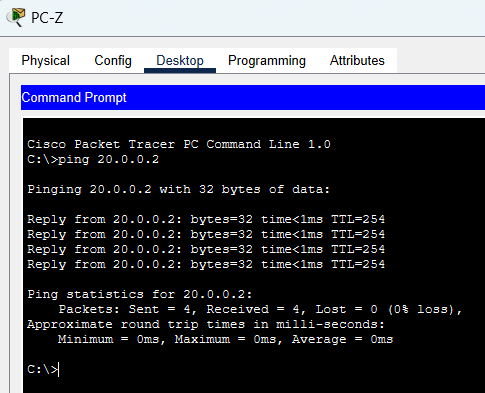
Routeur-F(config-if)#ip nat outside

Routeur-F(config-if)#exit

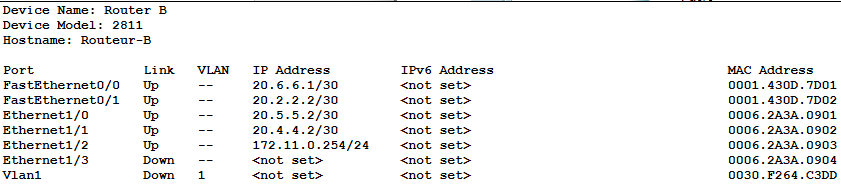
Routeur-F(config)#interface F0/0

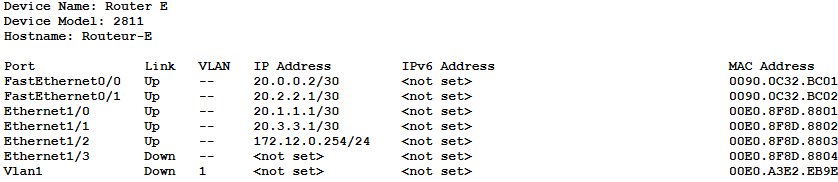
Routeur-F(config-if)#ip nat inside

Pour vérifier que tout fonctionne bien j’ai utilisé la commande ping de PC-Z à RtE :



Vérifiez, comme suggéré au début de cette étape, que PC-W et PW-Z peuvent *pinguer* respectivement RtB et RtE (sur n’importe laquelle de leurs interfaces d’ailleurs).





Vérifiez également le contenu de la table NAT/PAT :

* Soit par la commande Cisco : show ip nat translations

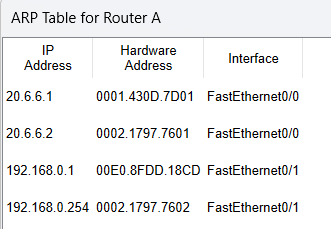


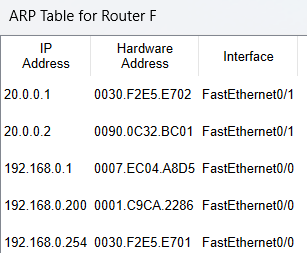


* Le mode debug fonctionne aussi (ne pas oublier de l’annuler : no debug ip nat) :



* Soit par l’interface graphique de Packet Tracer : outil loupe / clic sur Router-A / ARP Table





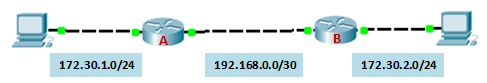
# Quatrième étape

Mettre en place le routage dynamique dans les routeurs de liaison RtB, RtC, RtD et RtE.

Le principe est que chaque routeur annonce à ses voisins les réseaux qui lui sont connectés directement et les réseaux connus par RIP. Au final, tous les routeurs connectés par RIP connaissent tous les réseaux.

Note : RIPv1 ne prenant pas en charge les masques de sous-réseau de longueur variable (on dit qu’il est *classfull*) ni l’authentification des routeurs. RIPv2 (*classless*) a été conçu pour permettre au protocole de répondre aux contraintes des réseaux actuels (découpages des réseaux IP en sous-réseaux, authentification par mot de passe…).

*Exemple de paramétrage de RIPv2 :*

**

|  |  |
| --- | --- |
| A(config)# router rip  A(config-router)# version 2  A(config-router)# network 172.30.1.0  A(config-router)# network 192.168.0.0  A(config-router)# no auto-summary  A#sh ip route  C 172.30.1.0 is directly connected, Fa0/0  R 172.30.2.0 [120/1] via 192.168.0.2, Fa0/1  C 192.168.0.0 is directly connected, Fa0/1 | B(config)# router rip  B(config-router)# version 2  B(config-router)# network 172.30.2.0  B(config-router)# network 192.168.0.0  B(config-router)# no auto-summary  B#sh ip route  R 172.30.1.0 [120/1] via 192.168.0.1, Fa0/1  C 172.30.2.0 is directly connected, Fa0/0  C 192.168.0.0 is directly connected, Fa0/1 |

Note : le « NO AUTO SUMMARY » permet de travailler avec des masques non « standards ».

**Travail à faire**

Vous devez donc, pour chaque routeur de liaison RtB, RtC, RtD et RtE activer le protocole RIPv2 et déclarer les réseaux qui lui sont directement connectés.

Routeur-B> enable

Routeur-B# configure terminal

Routeur-B(config)# router rip

Routeur-B(config-router)# version 2

Routeur-B(config-router)# network 20.6.6.0

Routeur-B(config-router)# network 172.11.0.0

Routeur-B(config-router)# no auto-summary

Routeur-B(config-router)# exit

Routeur-B(config)# exit

Routeur-C>enable

Routeur-C#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Routeur-C(config)#router rip

Routeur-C(config-router)#version 2

Routeur-C(config-router)#network 20.1.1.0

Routeur-C(config-router)#no auto-summary

Routeur-C(config-router)#exit

Routeur-C(config)#exit

Routeur-C#

Routeur-D>enable

Routeur-D#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Routeur-D(config)#router rip

Routeur-D(config-router)#version 2

Routeur-D(config-router)#network 20.3.3.0

Routeur-D(config-router)#no auto-summary

Routeur-D(config-router)#exit

Routeur-D(config)#exit

Routeur-D#

Routeur-E>enable

Routeur-E#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Routeur-E(config)#router rip

Routeur-E(config-router)#version 2

Routeur-E(config-router)#network 20.2.2.0

Routeur-E(config-router)#network 172.12.0.0

Routeur-E(config-router)#no auto-summary

Routeur-E(config-router)#exit

Routeur-E(config)#exit

Routeur-E#

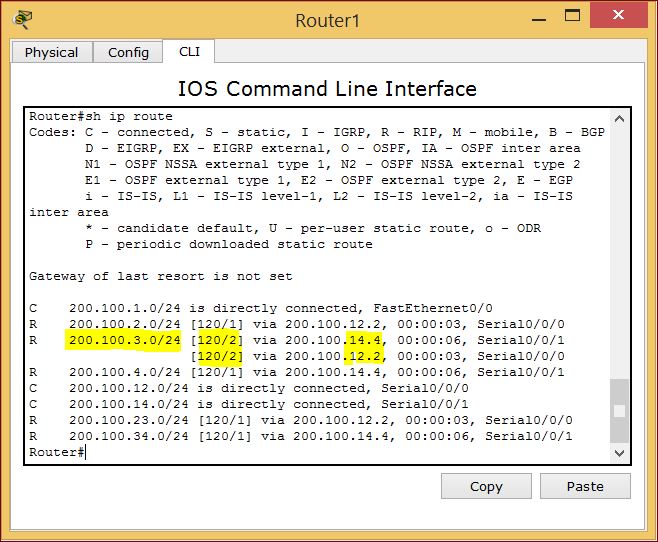
**NB** : Comme indiqué précédemment, les réseaux privés (192.168.0.0/24) ne seront pas déclarés au niveau de RIP dans notre cas de figure.

# Cinquième étape

## Partie B - Étude du fonctionnement du protocole RIP

### Vérifications des tables de routage

Prenons l’exemple d’un routeur Router1, dont la table de routage est la suivante :



Voici quelques explications sur le contenu de cette table de routage :

* Le routeur est connecté directement à 3 réseaux, via ses 3 interfaces : 1 interface ethernet et deux interfaces série. Ces lignes sont repérables par le « C » (Connected) en début de ligne.
* Le routeur a appris à connaître, via RIP, 5 autres réseaux : les réseaux des 3 autres sites, mais aussi les 2 réseaux d’interconnexion entre ces sites. Ces lignes sont repérables par le « R » (RIP) en début de ligne.
* Lorsque la route est apprise grâce à RIP, une information importante permet de connaître la « distance » pour atteindre la destination. Cette distance, appelée « métrique », correspond au nombre de routeurs à traverser (appelé également « nombre de sauts ») pour atteindre la destination.
* Lorsque plusieurs routes sont empruntables, la table de routage ne montre que les routes les plus « courtes » (autrement dit avec la métrique la plus faible).
* Lorsque deux routes de même distance sont possibles, elles sont toutes les deux affichées.
* C’est le cas pour rejoindre le réseau 200.100.3.0 : Il est joignable avec le même nombre de sauts (2), que ce soit en passant par Router2 ou par Router4.

**Pour information :**

120 correspond à la distance administrative, non utile dans le cadre du protocole RIP, mais utile dans d’autres protocoles de routage. Cette information est alors plus importante que la métrique dans la détermination de la meilleure route à emprunter pour atteindre la destination.

### Compréhension du protocole RIP

**Examiner les échanges RIP**

Pour bien comprendre comment fonctionne le protocole RIP, le mieux est d’examiner l’échange entre routeurs :

* Ce qu’envoie un routeur comme informations
* Ce que reçoit un routeur comme informations

On pourrait capturer et étudier les trames entre les deux routeurs ; on peut aussi plus simplement activer le « debug RIP » sur un routeur, ce qui nous permettra de voir les messages RIP envoyés et reçus, toutes les 30 secondes par défaut. Pour visualiser au moins une fois les différents échanges, il faut donc patienter 30 s avant de désactiver le mode debug.

# Activer le mode debug du protocole RIP

Router# debug ip RIP

RIP protocol debugging is on



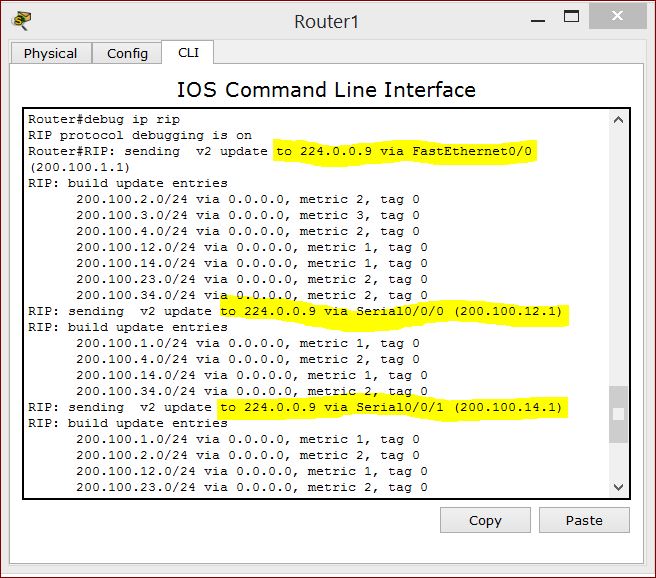
# Désactiver le mode debug du protocole RIP

Router# no debug ip RIP

RIP protocol debugging is off



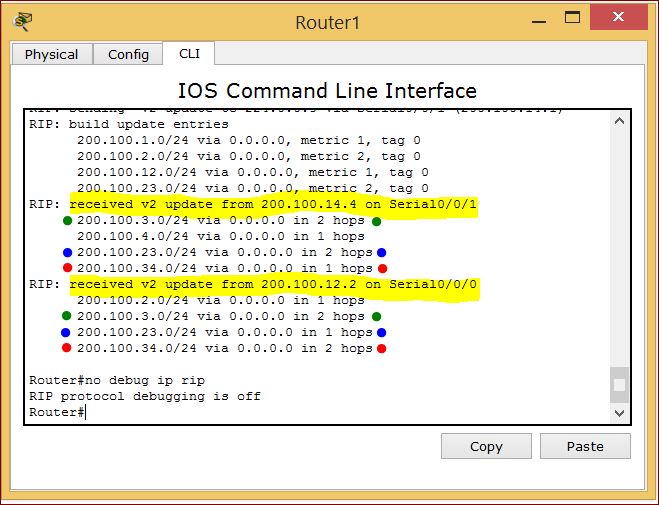
**Après avoir activé le deboggage sur le routeur 1, en exemple précédant et voici les informations transmises :**



**On peut faire les constats suivants :**

* Les informations transmises correspondent bien aux lignes de la table de routage, mais en fonction de l’interface de transmission, elles sont filtrées.
  + Par exemple, il n’est pas nécessaire de transmettre sur le site 1 que le réseau 200.100.1.0/24 est connu ; ou bien vers Router2 que le site 200.100.12.0 est connu, car on sait que le prochain routeur le connaît aussi, jusqu’à l’autre bout de la liaison.
  + De même, il est inutile de transmettre les informations reçues depuis l’interface s0/0/0 sur cette interface, car Router2 les connaît déjà : par exemple Router2 est plus près du réseau 200.100.2.0, donc inutile de lui envoyer des informations sur ce réseau, puisqu’on les a obtenues de lui.
  + Idem, sur l’interface s0/0/1, aucune information concernant le réseau 200.100.4.0 n’est envoyée, puisque la route vers ce réseau passe par ce lien.
* Le métric, autrement dit le nombre de sauts qui sera nécessaire pour l’atteindre, est transmis avec la destination. A noter que l’envoi se fait en anticipant sur le fait qu’il faut passer par Router1, donc par au moins un routeur. Aucune route n’est donc transmise avec un métric à 0.
* Le masque est bien transmis également à chaque fois (/24), parce qu’on est en RIP version 2.

**Informations reçues**



**On peut faire les constats suivants :**

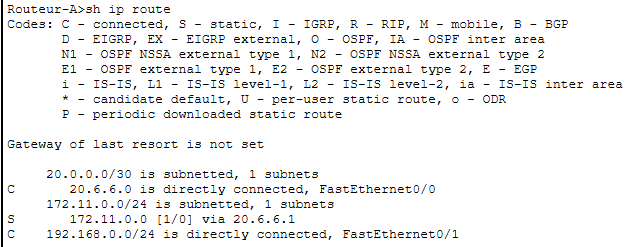
* Router1 reçoit bien des informations de ses voisins directs :
  + sur s0/0/1 depuis router4 (200.100.14.4)
  + sur s0/0/0 depuis router2 (200.100.12.2)
* Ces informations concernent parfois les mêmes réseaux (points de même couleur dans l’illustration ci-dessus). À partir de ces informations, le routeur construira sa table de routage, en ne gardant que les routes les plus directes.
* Par exemple, pour le réseau 200.1000.23.0, la route la plus directe passe par la liaison sur s0/0/0 (un saut) et c’est bien cette route qui sera conservée, comme constaté dans la table de routage observée plus haut, et non la route par la liaison sur s0/0/1, qui elle, nécessite de passer par 2 routeurs (2 sauts).

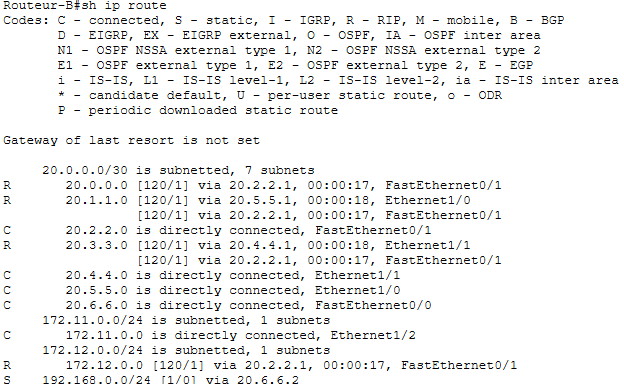
### Réajustement du protocole RIP, en cas de modification de la cartographie

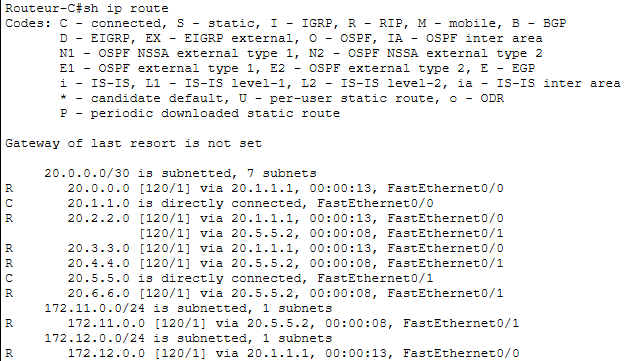
**Travail à faire**

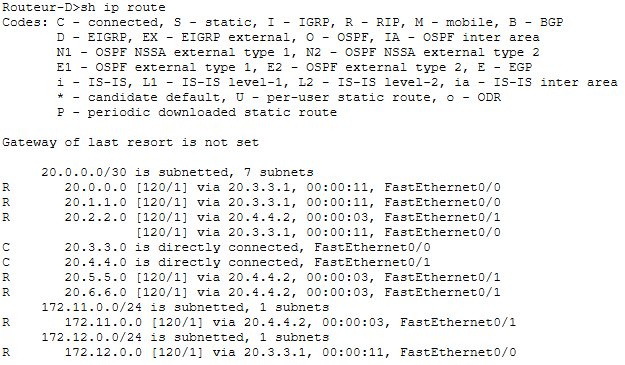
À l’aide de commandes vous mettrez en évidence le comportement du protocole RIP et en coupant une des connexions vous montrerez la tolérance de panne permise par notre architecture en comparant les tables de routages des différents routeurs.

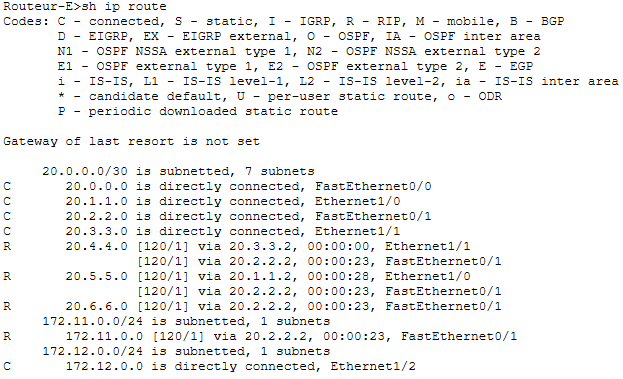
Pour bien vérifier que le router soin mis en place je suis aller voir les tables routes pour vérifier que les routeurs avaient resus les route des autres routeurs.

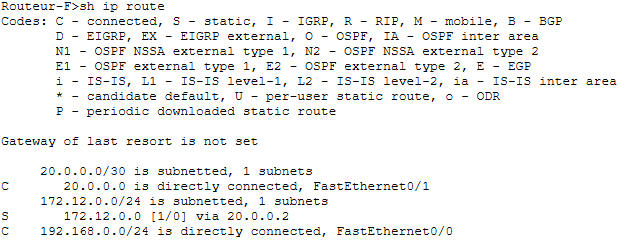












On peut voir que tous les routeurs on bien resus des router des différents routeurs.

Pour vérifier que tous c’est route fonctionne, il suffit de fait un test ping pour vérifier le bon fonctionnement des routes.





Comme nous pouvons le voir les routes fonctionne bien car PC-W a pu communiquer avec le routeur le plus éloigner. Comme pour PC-Z.

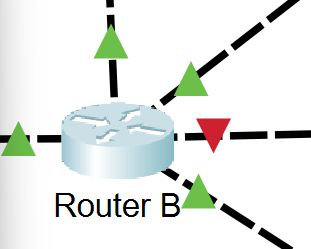
Maintenant, pour vérifier la tolérance de panne, je vais couper l’interface F0/1 pour voir si l’acheminement des paquets arrive encore à destination.

Routeur-B>en

Routeur-B#conf

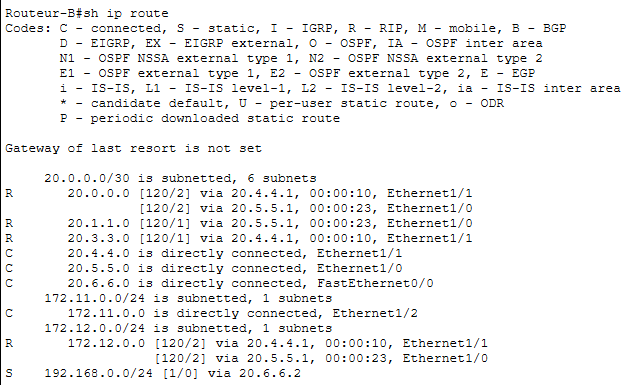
Routeur-B(config)#interface f0/1

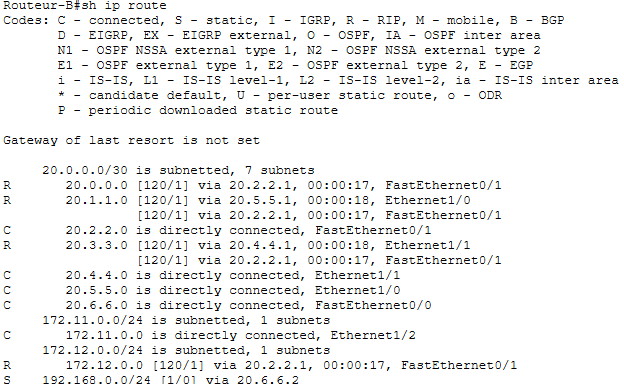
Routeur-B(config-if)#shutdown



Après un nouveau test de ping, PC-W et PC-Z arrivent à acheminer leurs paquets.







Sur les deux images on peut voir les tables de routage du routeur B avec des différences entre la première et la deuxième :

On voit qu’il y a un sous-réseau en moins pour 20.0.0.0/30, Première image il y en a 7 sous-réseaux et Deuxième image il y en a 6 sous-réseaux.

Deplus il y a des routes manquantes ou supplémentaires, dans la première image il y a 20.2.2.0/30 est présent, mais absent dans la deuxième. Dans la deuxième image il y a 192.168.0.0/24 est ajouté, mais absent dans la première.

Également la distances administratives/métriques et différentes entre les deux images car il y a plus de router à traverser.

# Sixième étape

Mettre en place une redirection de port sur RtF, permettant d’atteindre Serv-Z depuis tout le réseau et notamment PC-W, en invoquant l’adresse publique de RtF.

**Travail à faire**

1. Mettre en place la redirection nécessaire pour atteindre Serv-Z depuis l’extérieur du site Z.

Routeur-F>en

Routeur-F#conf

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

Routeur-F(config)#access-list 100 permit tcp any host 20.0.0.1 eq 80

Routeur-F(config)#ip nat inside source static tcp 192.168.0.200 80 20.0.0.1 80

Routeur-F(config)#interface f0/1

Routeur-F(config-if)#ip nat outside

Routeur-F(config-if)#exit

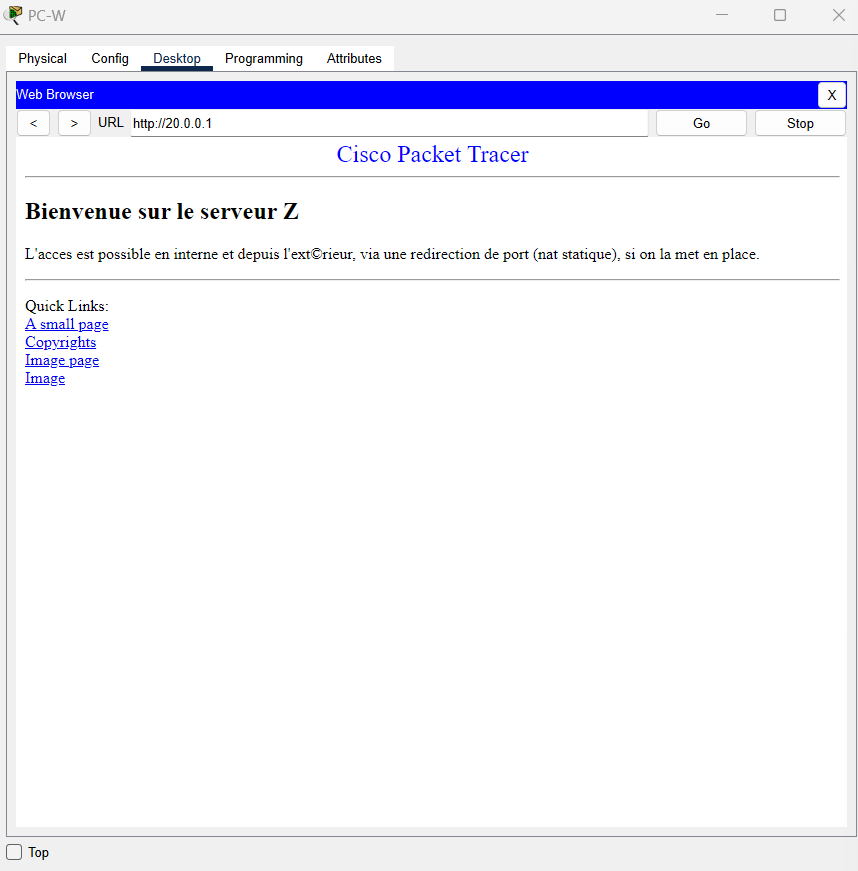
Routeur-F(config)#interface F0/0

Routeur-F(config-if)#ip nat inside

Routeur-F(config-if)#exit

Routeur-F(config)#

1. Vérifier ensuite que l’accès HTTP fonctionne, par exemple depuis PC-W,



**NB** : Vous utilisez bien sûr le NAT statique comme indiqué plus haut, pour le port n° 80.

# Septième étape

Afin que les mises à jour des tables de routage de chacun des routeurs puissent se faire de manière sécurisée, il sera nécessaire d’implémenter l’authentification réciproque des routeurs.

**Travail à faire**

Faire une recherche des commandes que vous auriez utilisées sur Rtb, Rtc,Rtd, Rte afin de satisfaire à cette demande. Elles ne sont pas supportées par Packet Tracer. Bien entendu, la réponse tiendra compte du contexte proposé.

D’apprés mais rechercher ces commandes activent l'authentification sur l'interface spécifiée pour OSPF, en utilisant un mot de passe (clé) partagé. Le mot de passe doit être identique sur toutes les interfaces des routeurs participant à l'aire OSPF pour assurer une communication sécurisée.

Pour EIGRP, l'authentification est réalisée en utilisant une clé MD5. Le routeur stocke le mot de passe dans une chaîne de clés, qui est ensuite appliquée à l'interface où EIGRP est activé. Cette configuration garantit que seuls les routeurs authentifiés peuvent échanger des informations de routage EIGRP.

# Authentification OSPF

Router(config)# interface F0/0

Router(config-if)# ip ospf authentication

Router(config-if)# ip ospf authentication-key secretpassword

Router(config-if)# exit

Router(config)# router ospf 1

Router(config-router)# area 0 authentication

# Authentification EIGRP dans Packet Tracer

Router(config)# key chain EIGRP\_AUTH

Router(config-keychain)# key 1

Router(config-keychain-key)# key-string secretpassword

Router(config-keychain-key)# exit

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ip authentication mode eigrp 1 md5

Router(config-if)# ip authentication key-chain eigrp 1 EIGRP\_AUTH

# Annex

Après avoir vérifié tous les réseaux, j’ai découvert que le routeur A avait un port mal configuré sur son adresse IP, qui était 20.6.6.1, alors que, selon la logique de toutes les topologies réseau, elle aurait dû être 20.6.6.2. Une fois l'erreur corrigée, j’ai pu obtenir une vérification de Packet Tracer à 100 %. De plus, j’ai pu accéder à la page web qui s’est affichée comme mentionné plus haut.