UNIVERSITÉ CÔTE D'AZUR

SAÉ 21

CONSTRUIRE UN RÉSEAU INFORMATIQUE POUR UNE PETITE STRUCTURE

Cali ALEGRE Bastien LABESTE 2B

1.Introduction :

Dans le cadre de notre formation en Réseaux et Télécommunications , nous avons été chargés de concevoir et d'implémenter le réseau informatique d'une petite entreprise. Ce projet a pour but de répondre aux besoins de commutation, de routage, de services réseaux fondamentaux et de sécurité de l'entreprise.

Ce rapport présente les étapes de la création du réseau, les choix technologiques effectués et les configurations mises en œuvre. L'objectif est de fournir à l'entreprise un réseau efficace, structuré et sécurisé, adapté à ses besoins actuels et futurs.

2. Cahier des charges :

L'objectif de ce projet est de construire un réseau d'entreprise typique d'une PME. Le réseau doit donc inclure les éléments suivants :

- Un cœur de réseau avec un multi-layer switch (MLS), capable de switcher ou router selon les besoins.

- Plusieurs VLANs pour les différents services de l'entreprise, notamment :

    - - Deux VLANs pour les groupes de travail (par exemple, RH et ingénierie).
    - - Un VLAN pour les serveurs internes.

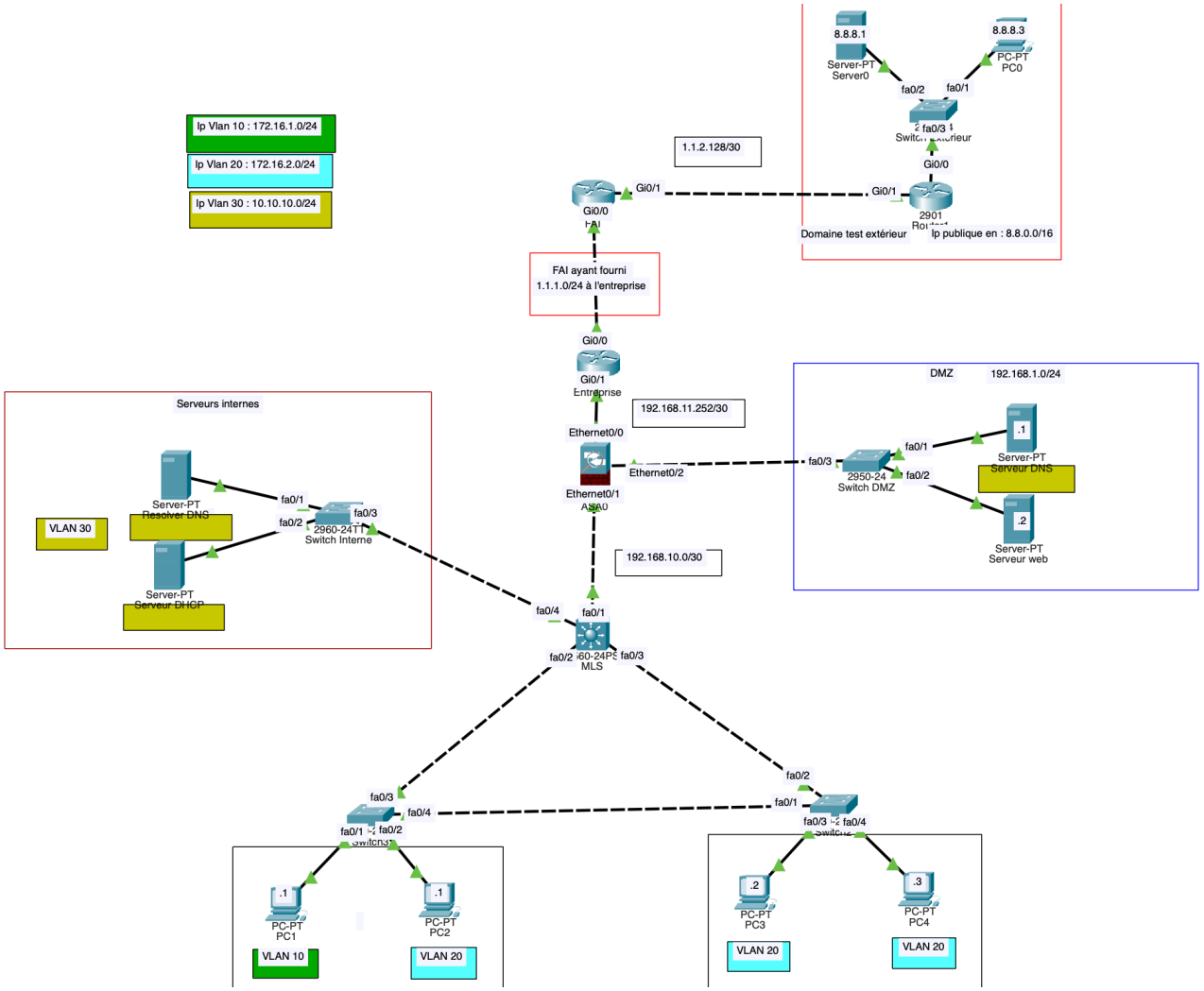
- Un pare-feu (CISCO ASA 5505) pour sécuriser les accès et les communications.

- Un routeur de bordure (entreprise) pour l'interconnexion avec le fournisseur d'accès à Internet (FAI).

- Des services de base comme DHCP et DNS pour faciliter la gestion du réseau.

Les équipements doivent être configurés de manière à assurer une connectivité interne fluide et une sécurité optimale pour les accès externes.

3. Schéma global du réseau :



4. Plan d’adressage :

Voici les détails du plan d'adressage pour le réseau de l'entreprise :

VLAN 10 (Service RH) :

- Adresse réseau : 172.16.1.0/24
- Passerelle : 172.16.1.254
- Plage d’adresses disponibles : 172.16.1.2 - 172.16.1.254

VLAN 20 (Service Ingénierie) :

- Adresse réseau : 172.16.2.0/24
- Passerelle : 172.16.2.254
- Plage d’adresses disponibles : 172.16.2.2 - 172.16.2.254

VLAN 30 (Serveurs Internes) :

- Adresse réseau : 10.0.0.0/24
- Passerelle : 10.0.0.254
- Plage d’adresses disponibles : 10.0.0.2 - 10.0.0.254

Réseau entre le MLS et l'ASA :

- Adresse réseau : 192.168.10.0/30
- Passerelle (MLS) : 192.168.10.1
- Adresse ASA : 192.168.10.2

Réseau entre l'ASA et le routeur entreprise :

- Adresse réseau : 192.168.11.252/30
- Passerelle (ASA) : 192.168.11.253
- Adresse routeur : 192.168.11.254

DMZ :

- Adresse réseau : 192.168.1.0/24
- Passerelle : 192.168.1.254

- Serveur Web : 192.168.1.2

- Serveur DNS : 192.168.1.1

FAI :

- Adresse réseau : 1.1.1.0/24

- Adresse attribuée à l'entreprise : 1.1.1.1 - 1.1.1.254

- Adresse externe du serveur web de la DMZ : 1.1.1.253

Réseau public de test :

- Adresse réseau : 8.8.0.0/16

- Serveur Web : 8.8.8.1

- Client : 8.8.8.3

Interconnexion entre le réseau 8.8.0.0/16 et 1.1.1.0/24 :

- Adresse réseau : 1.1.2.128/30

- Adresse routeur côté FAI : 1.1.2.130

- Adresse routeur externe: 1.1.2.129

Réseau entre l'le routeur FAI et le routeur entreprise :

- Adresse réseau : 1.1.1.0/24

-Adresse routeur entreprise : 1.1.1.2

- Adresse routeur FAI : 1.1.1.1

5. Étape 1 : Construction du cœur de réseau :

5.1. Configuration des switches et du MLS :

Configuration générale du MLS (Multi-Layer Switch) :

hostname MLS : Définit le nom d'hôte du switch à "MLS".

ip routing : Active le routage IP sur le switch, permettant ainsi le routage entre VLANs.

spanning-tree vlan 10,20,30 priority 4096 : Définit la priorité STP à 4096 pour les VLANs 10, 20, et 30, ce qui rend ce switch plus prioritaire pour devenir le root bridge pour ces VLANs.

Configuration des interfaces :

Interface FastEthernet0/1

no switchport : Convertit l'interface en port routé.

ip address 192.168.10.1 255.255.255.252 : Assigne l'adresse IP 192.168.10.1 avec un masque de sous-réseau /30.

no shutdown : Active l'interface.

Interfaces FastEthernet0/2 à 0/4

switchport trunk allowed vlan 10,20,30 : Permet uniquement les VLANs 10, 20, et 30 sur ce trunk.

switchport trunk encapsulation dot1q : Utilise l'encapsulation IEEE 802.1Q pour le trunking.

switchport mode trunk : Configure l'interface en mode trunk.

no shutdown : Active l'interface.

Configuration des interfaces VLAN

Interface Vlan10

ip address 172.16.1.254 255.255.255.0 : Assigne l'adresse IP 172.16.1.254 avec un masque de sous-réseau /24.

ip helper-address 10.10.10.1 : Configure une adresse IP de l'assistant pour le relais DHCP.

Interface Vlan20

ip address 172.16.2.254 255.255.255.0 : Assigne l'adresse IP 172.16.2.254 avec un masque de sous-réseau /24.

ip helper-address 10.10.10.1 : Configure une adresse IP de l'assistant pour le relais DHCP.

Interface Vlan30

ip address 10.10.10.254 255.255.255.0 : Assigne l'adresse IP 10.10.10.254 avec un masque de sous-réseau /24.

ip helper-address 10.10.10.1 : Configure une adresse IP de l'assistant pour le relais DHCP.

Configuration des routes et autres paramètres IP :

ip default-gateway 10.10.10.254 : Définit la passerelle par défaut pour le switch.

ip route 0.0.0.0 0.0.0.0 192.168.10.2 : Ajoute une route par défaut pointant vers 192.168.10.2.

Configuration d'un switch d'accès (Switch 3) :

hostname Switch : Définit le nom d'hôte du switch à "Switch".

Configuration des interfaces :

Interface FastEthernet0/1

switchport access vlan 10 : Configure l'interface en mode accès pour le VLAN 10.

switchport mode access : Force l'interface en mode accès.

no shutdown : Active l'interface.

Interface FastEthernet0/2

switchport access vlan 20 : Configure l'interface en mode accès pour le VLAN 20.

switchport mode access : Force l'interface en mode accès.

no shutdown : Active l'interface.

Interface FastEthernet0/3 et 0/4

switchport trunk allowed vlan 10,20,30 : Permet uniquement les VLANs 10, 20, et 30 sur ce trunk.

switchport mode trunk : Configure l'interface en mode trunk.

no shutdown : Active l'interface.

5.2. Résumé du déroulement de la étape 1 :

Nous avons commencé par construire le cœur du réseau avec les trois switches qui desservent les VLANs et le MLS. Nous avons attribué des adresses IP statiques aux Pc et testé leur connectivité avec des pings, confirmant que tout fonctionnait correctement.

Puis, nous avons configuré le MLS en activant le routage IP et en définissant la priorité STP pour les VLANs 10, 20 et 30, s'assurant ainsi que le MLS devienne le root bridge pour ces VLANs. Les interfaces du MLS ont été configurées avec des adresses IP et les trunks nécessaires ont été mis en place pour permettre la communication entre les VLANs.

Ensuite, nous avons configuré les switches d'accès en assignant les ports aux VLANs appropriés et en activant les trunks là où nécessaire. Nous avons vérifié la configuration STP pour nous assurer que le MLS était bien le switch racine pour les VLANs 10 et 20.

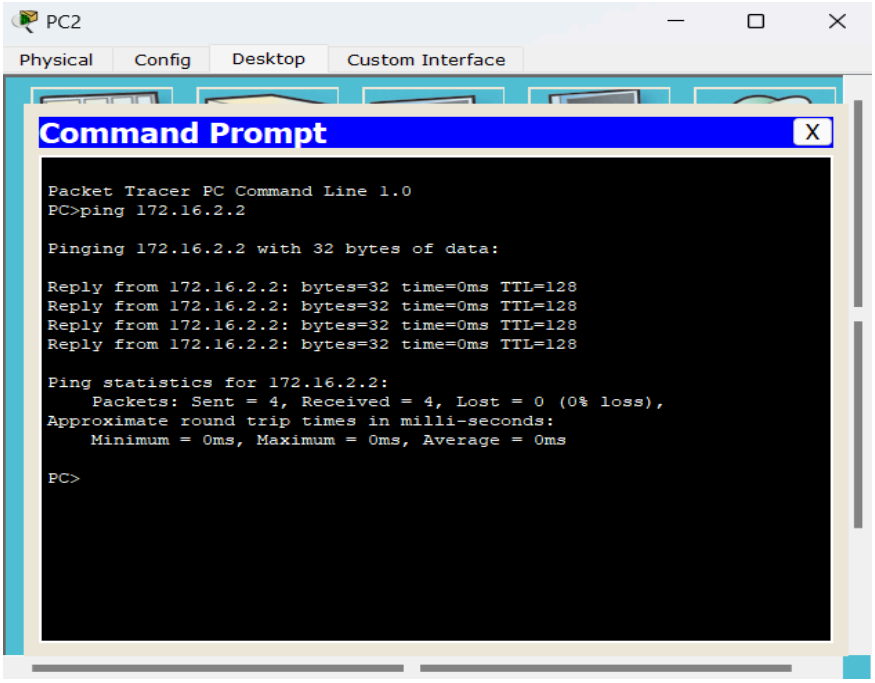
Nous avons rencontré un problème avec les pings entre les VLANs, dû à l'oubli d'activer le routage IP car nous pensions qu'il était activé de base mais après avoir vérifié dans le cours nous l'avons rajouté. Après avoir ajouté la commande ip routing, les pings entre les VLANs ont fonctionné correctement.

Les tests de connectivité ont confirmé que les machines pouvaient communiquer au sein du même VLAN et entre des VLANs différents, validant ainsi la configuration initiale du réseau.

5.3. Tests de connectivité :

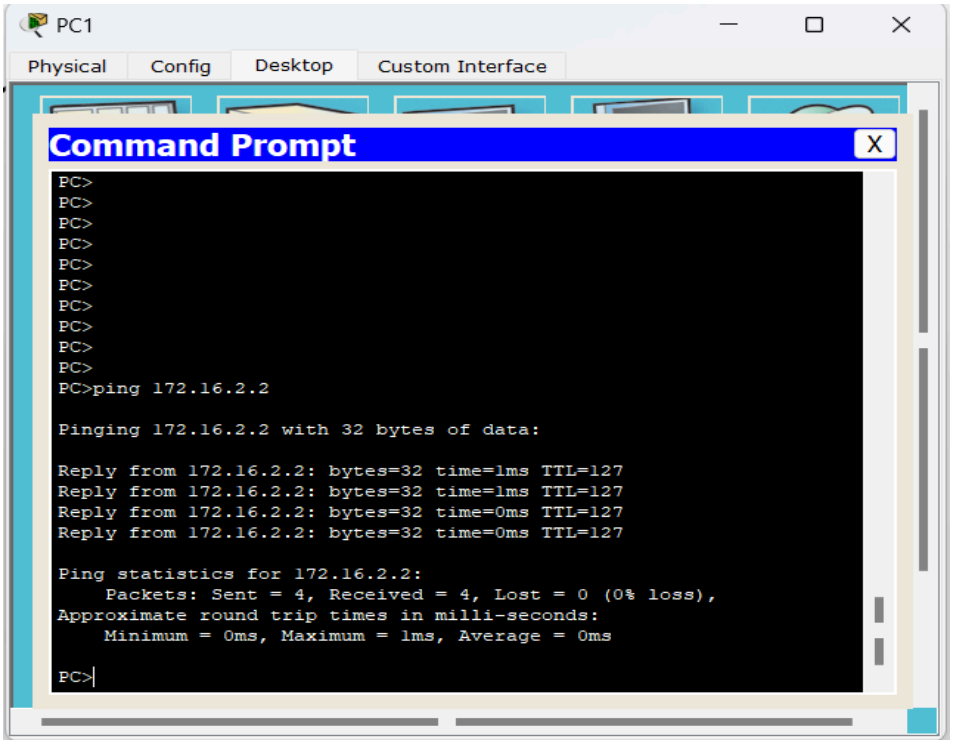
-Ping entre deux machines du même VLAN

PC2 (VLAN 20) à PC3 (VLAN 20) :



-Ping entre deux machines de VLANs différents

PC1 (VLAN 10) à PC3 (VLAN 20) :



Vérification de la configuration STP :

Sur le MLS :

```
MLS#show spanning-tree
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    4106
             Address     0040.0BA5.9BEC
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4106  (priority 4096 sys-id-ext 10)
             Address     0040.0BA5.9BEC
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    4116
             Address     0040.0BA5.9BEC
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4116  (priority 4096 sys-id-ext 20)
             Address     0040.0BA5.9BEC
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority    4126
             Address     0040.0BA5.9BEC
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4126  (priority 4096 sys-id-ext 30)
             Address     0040.0BA5.9BEC
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
```

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

MLS#
```

Sur le switch 3 :

```
Switch#show spanning-tree
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              Address     0040.0BA5.9BEC
              Cost        19
              Port        3(FastEthernet0/3)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0040.0B51.003C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    4116
              Address     0040.0BA5.9BEC
              Cost        19
              Port        3(FastEthernet0/3)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     0040.0B51.003C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID     Priority    4126
              Address     0040.0BA5.9BEC
              Cost        19
              Port        3(FastEthernet0/3)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32798  (priority 32768 sys-id-ext 30)
              Address     0040.0B51.003C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p
```

6. Étape 2 : Ajout de l’ASA et du service DHCP

6.1. Configuration de base de l’ASA :

hostname ASA5505 : Définit le nom d'hôte de l'ASA à "ASA5505".

domain-name ASA5505.tp : Définit le nom de domaine de l'ASA à "ASA5505.tp".

Configuration des interfaces Ethernet :

Interface Ethernet0/0

switchport access vlan 300 : Configure l'interface Ethernet0/0 en mode accès pour le VLAN 300.

no shutdown : Active l'interface.

Interface Ethernet0/1

switchport access vlan 100 : Configure l'interface Ethernet0/1 en mode accès pour le VLAN 100.

no shutdown : Active l'interface.

Interface Ethernet0/2

switchport access vlan 200 : Configure l'interface Ethernet0/2 en mode accès pour le VLAN 200.

no shutdown : Active l'interface.

Configuration des interfaces VLAN :

Interface Vlan1

no nameif : Supprime le nom de l'interface.

no security-level : Supprime le niveau de sécurité.

no ip address : Supprime l'adresse IP.

Interface Vlan2

no forward interface Vlan1 : Empêche le transfert vers le VLAN 1.

no nameif : Supprime le nom de l'interface.

no security-level : Supprime le niveau de sécurité.

no ip address : Supprime l'adresse IP.

Interface Vlan3

no forward interface Vlan1 : Empêche le transfert vers le VLAN 1.

no nameif : Supprime le nom de l'interface.

no security-level : Supprime le niveau de sécurité.

no ip address : Supprime l'adresse IP.

Interface Vlan100

nameif inside : Nomme l'interface "inside".

security-level 100 : Définit le niveau de sécurité à 100 (plus élevé).

ip address 192.168.10.2 255.255.255.252 : Assigne l'adresse IP 192.168.10.2 avec un masque de sous-réseau /30.

no shutdown : Active l'interface.

Interface Vlan200

no forward interface Vlan100 : Empêche le transfert vers le VLAN 100.

nameif dmz : Nomme l'interface "dmz".

security-level 50 : Définit le niveau de sécurité à 50 (intermédiaire).

ip address 192.168.1.254 255.255.255.0 : Assigne l'adresse IP 192.168.1.254 avec un masque de sous-réseau /24.

no shutdown : Active l'interface.

Interface Vlan300

nameif outside : Nomme l'interface "outside".

security-level 0 : Définit le niveau de sécurité à 0 (plus bas).

ip address 192.168.11.253 255.255.255.252 : Assigne l'adresse IP 192.168.11.253 avec un masque de sous-réseau /30.

no shutdown : Active l'interface.

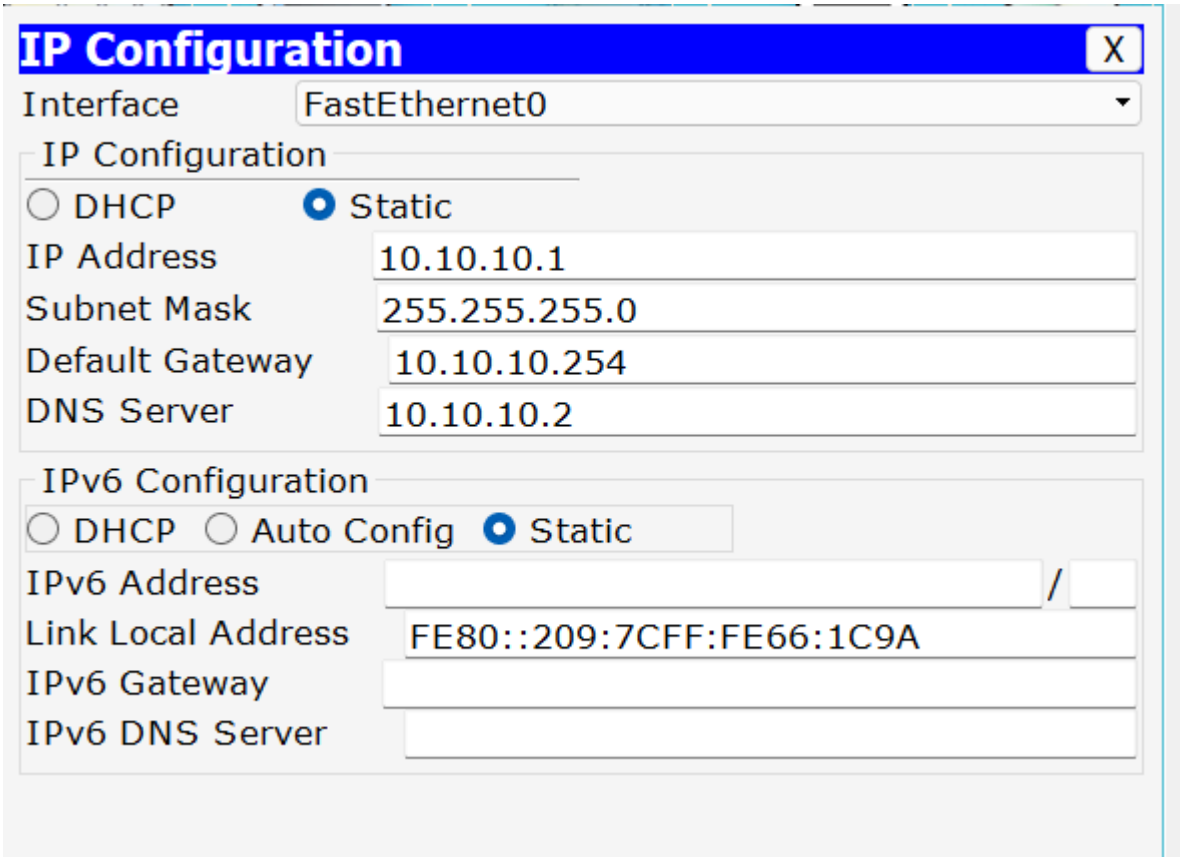
Configuration des routes :

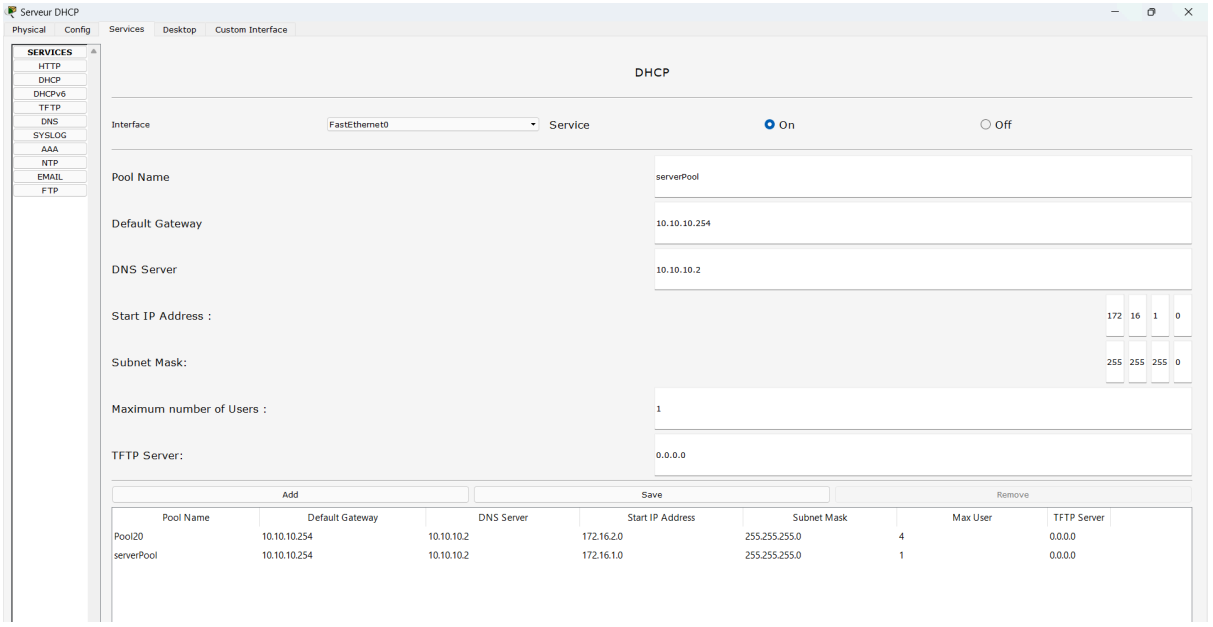
route inside 172.16.1.0 255.255.255.0 192.168.10.1 1 : Ajoute une route pour le réseau 172.16.1.0/24 (vlan 10) via 192.168.10.1.

route inside 172.16.2.0 255.255.255.0 192.168.10.1 1 : Ajoute une route pour le réseau 172.16.2.0/24 (vlan 20) via 192.168.10.1.

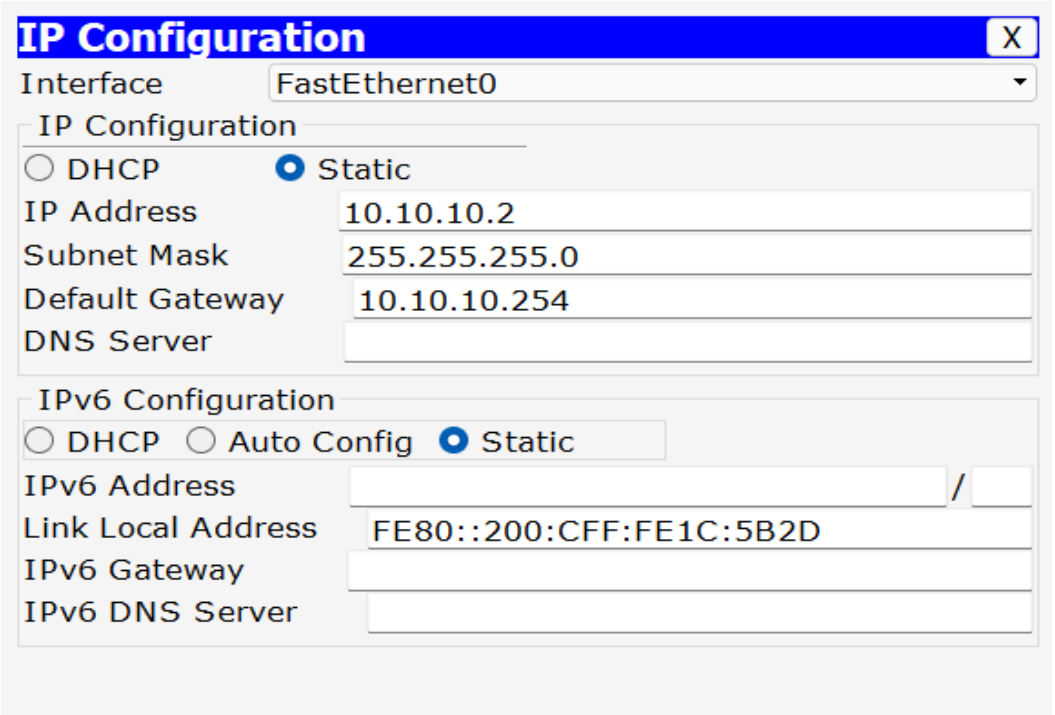
route outside 0.0.0.0 0.0.0.0 192.168.11.254 1 : Ajoute une route par défaut pour tout le trafic via 192.168.11.254.

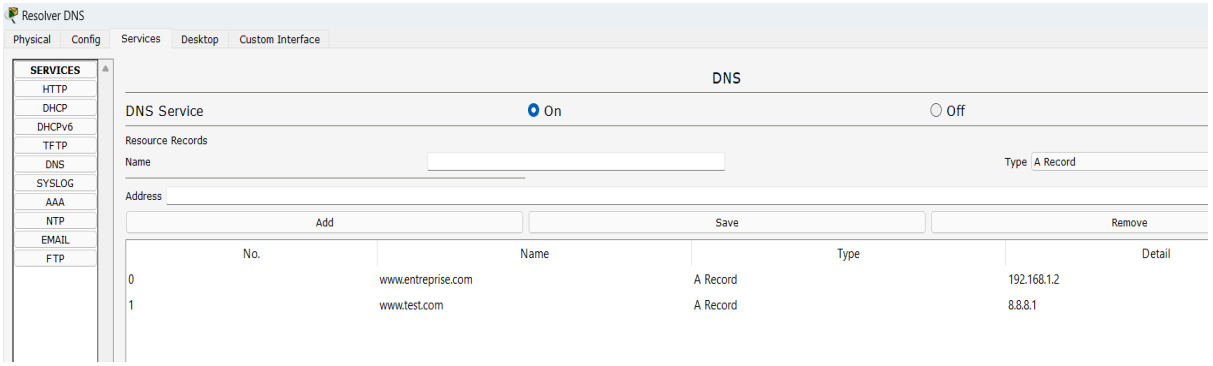
6.2. Configuration du DHCP :





6.3. Configuration du resolver DNS :





6.4. Résumé du déroulement de la partie 2 :

Nous avons commencé par tester la connectivité en utilisant des adresses IP statiques. Après avoir confirmé que tout fonctionnait correctement, nous avons configuré le serveur DHCP.

Une adresse IP fixe a été attribuée au serveur DHCP. Nous avons ensuite créé deux pools DHCP : un pour le VLAN 10 (en faites on a juste modifié la configuration du pool de base serverPool), limité à un hôte, et un autre pour le VLAN 20 appelé Pool20, capable de gérer jusqu'à quatre hôtes (car avec 3 il y avait un bug genre le pc4 n'obtenait pas d'adresse ip). Les adresses du serveur DNS ont également été configurées pour ces deux pools.

Pour permettre au serveur DHCP de desservir tous les VLANs, on a utilisé ip helper sur le MLS et on lui a ajouté une passerelle par défaut pour assurer la communication entre les VLANs.

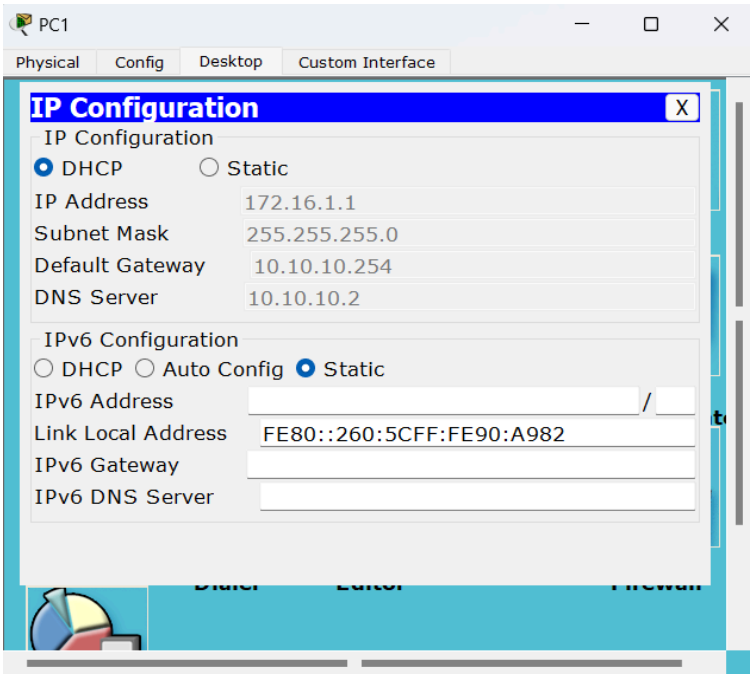
Après, on a mis les PC en DHCP, leur permettant ainsi d'obtenir automatiquement leurs adresses IP, passerelles et serveurs DNS. Les tests de connectivité n'ont révélé aucun problème.

Nous avons ensuite attribué une adresse IP statique au serveur DNS et créé deux enregistrements de type A : l'adresse IP 8.8.8.1 pour le domaine www.test.com et l'adresse IP 192.168.1.2 pour le domaine www.entreprise.com. Ces enregistrements lient les noms de domaine aux adresses IP correspondantes.

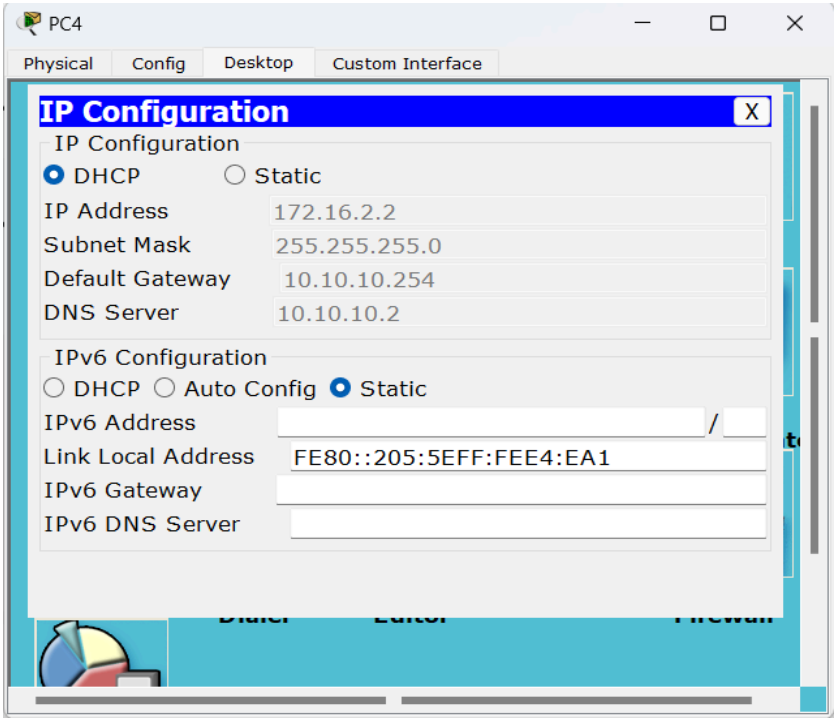
6.5. Tests de connectivité :

Vérification de la configuration DHCP :

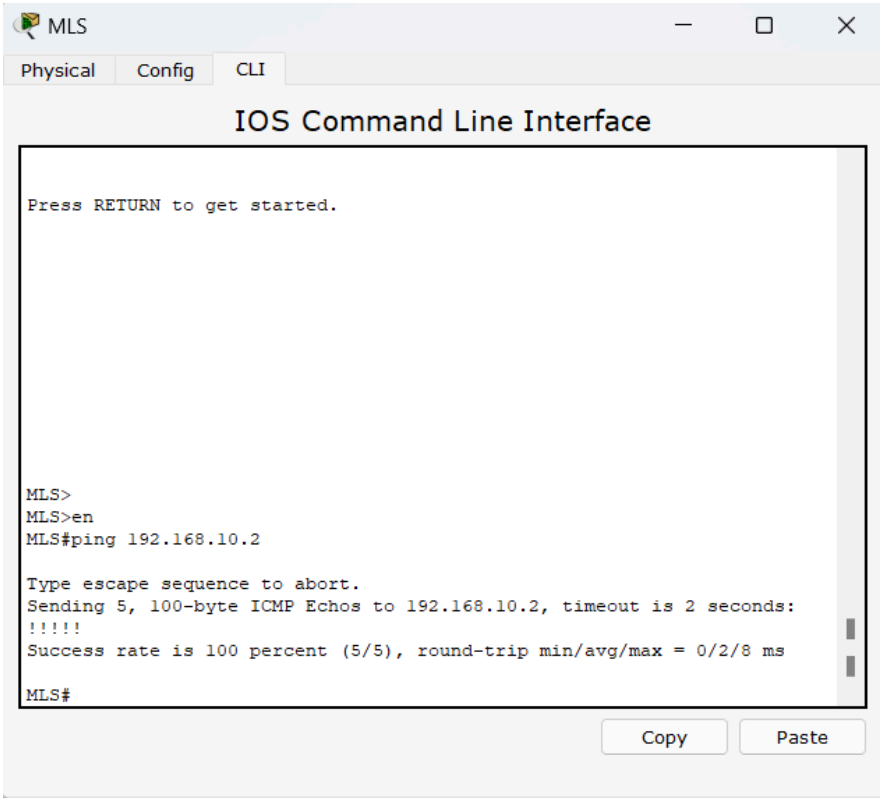
Connecter un PC à VLAN 10 et vérifier qu'il obtient une adresse IP automatiquement :



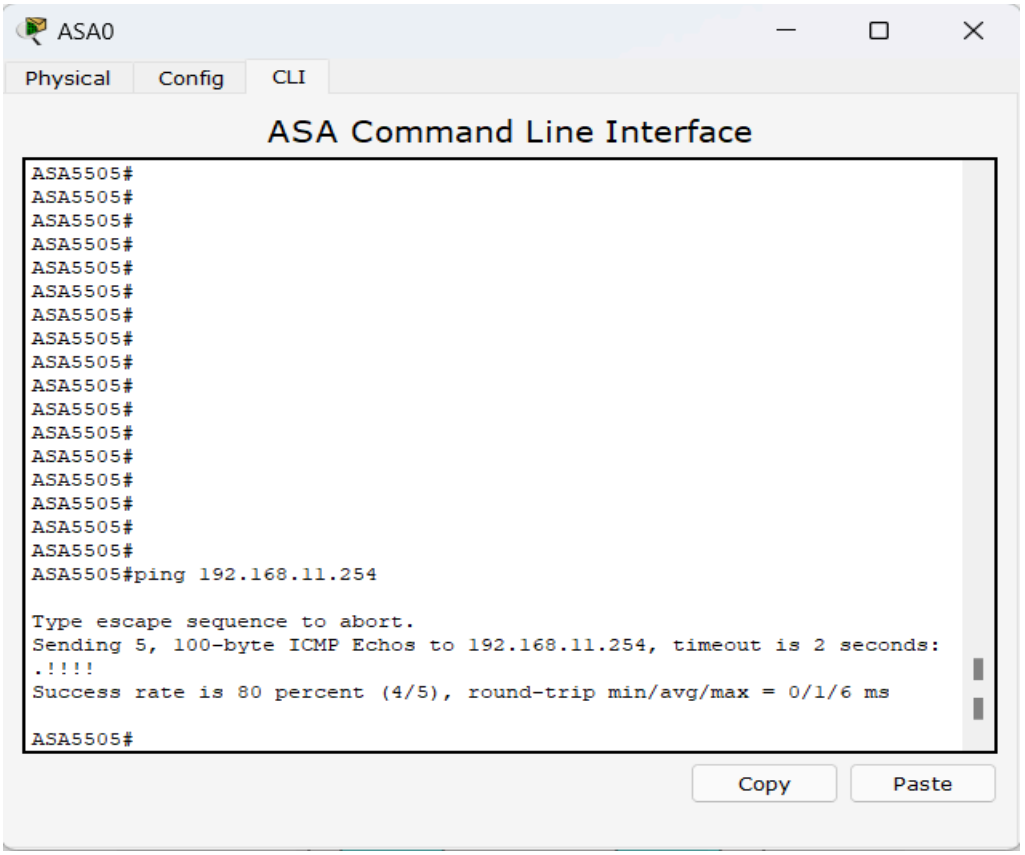
Connecter un PC à VLAN 20 et vérifier qu'il obtient une adresse IP automatiquement :



Vérification de la connectivité entre ASA et MLS :



Vérification de la connectivité entre ASA et le routeur entreprise :



7. Étape 3 : Ajout de la DMZ et du routeur du FAI

7.1. Configuration du routeur entreprise :

Configuration des interfaces :

Interface GigabitEthernet0/0

ip address 1.1.1.2 255.255.255.0 : Assigne l'adresse IP 1.1.1.2 avec un masque de sous-réseau /24.

ip nat outside : Configure l'interface pour NAT en tant qu'interface externe.

no shutdown : Active l'interface.

Interface GigabitEthernet0/1

ip address 192.168.11.254 255.255.255.252 : Assigne l'adresse IP 192.168.11.254 avec un masque de sous-réseau /30.

ip nat inside : Configure l'interface pour NAT en tant qu'interface interne.

no shutdown : Active l'interface.

Interface Vlan1

no ip address : Supprime toute adresse IP assignée à l'interface VLAN 1.

shutdown : Désactive l'interface VLAN 1.

Configuration NAT (Network Address Translation) :

ip nat inside source list 1 interface GigabitEthernet0/0 overload : Configure la surcharge NAT (PAT) pour les adresses IP internes spécifiées par la liste d'accès 1 via l'interface GigabitEthernet0/0.

ip nat inside source static 192.168.1.2 1.1.1.253 : Configure une translation NAT statique de l'adresse interne 192.168.1.2 à l'adresse publique 1.1.1.253.

Configuration des routes et autres paramètres IP :

ip route 0.0.0.0 0.0.0.0 192.168.11.253 : Ajoute une route par défaut pointant vers 192.168.11.253.

ip route 8.8.0.0 255.255.0.0 1.1.1.1 : Ajoute une route statique pour le réseau 8.8.0.0/16 via l'adresse 1.1.1.1.

ip route 192.168.10.0 255.255.255.0 192.168.11.253 : Ajoute une route statique pour le réseau 192.168.10.0/24 via l'adresse 192.168.11.253.

Configuration des listes d'accès :

access-list 1 permit 192.168.1.0 0.0.0.255 : Permet le trafic provenant du réseau 192.168.1.0/24.

access-list 1 permit 192.168.10.0 0.0.0.3 : Permet le trafic provenant du réseau 192.168.10.0/30.

access-list 1 permit 172.16.1.0 0.0.0.255 : Permet le trafic provenant du réseau 172.16.1.0/24 (vlan 10).

access-list 1 permit 172.16.2.0 0.0.0.255 : Permet le trafic provenant du réseau 172.16.2.0/24 (vlan 20).

7.2. Configuration du routeur FAI :

Configuration des interfaces :

Interface GigabitEthernet0/0

ip address 1.1.1.1 255.255.255.0 : Assigne l'adresse IP 1.1.1.1 avec un masque de sous-réseau /24.

no shutdown : Active l'interface.

Interface GigabitEthernet0/1

ip address 1.1.2.130 255.255.255.252 : Assigne l'adresse IP 1.1.2.130 avec un masque de sous-réseau /30.

no shutdown : Active l'interface.

Interface Vlan1

no ip address : Supprime toute adresse IP assignée à l'interface VLAN 1.

shutdown : Désactive l'interface VLAN 1.

Configuration du protocole de routage EIGRP :

router eigrp 1 : Active le processus EIGRP

network 1.1.1.0 0.0.0.255 : Ajoute le réseau 1.1.1.0/24 au processus EIGRP.

network 1.1.2.128 0.0.0.3 : Ajoute le réseau 1.1.2.128/30 au processus EIGRP.

Configuration des routes et autres paramètres IP :

ip route 0.0.0.0 0.0.0.0 1.1.1.2 : Ajoute une route par défaut pointant vers 1.1.1.2.

ip route 8.8.0.0 255.255.0.0 1.1.2.129 : Ajoute une route statique pour le réseau 8.8.0.0/16 via l'adresse 1.1.2.129.

7.3. Configuration finale de l'ASA :

hostname ASA5505 : Définit le nom d'hôte de l'ASA à "ASA5505".

domain-name ASA5505.tp : Définit le nom de domaine de l'ASA à "ASA5505.tp".

Configuration des interfaces Ethernet

Interface Ethernet0/0

switchport access vlan 300 : Configure l'interface Ethernet0/0 en mode accès pour le VLAN 300.

no shutdown : Active l'interface.

Interface Ethernet0/1

switchport access vlan 100 : Configure l'interface Ethernet0/1 en mode accès pour le VLAN 100.

no shutdown : Active l'interface.

Interface Ethernet0/2

switchport access vlan 200 : Configure l'interface Ethernet0/2 en mode accès pour le VLAN 200.

no shutdown : Active l'interface.

Interface Vlan1 :

no nameif : Supprime le nom de l'interface.

no security-level : Supprime le niveau de sécurité.

no ip address : Supprime l'adresse IP.

Interface Vlan2 :

no forward interface Vlan1 : Empêche le transfert vers le VLAN 1.

no nameif : Supprime le nom de l'interface.

no security-level : Supprime le niveau de sécurité.

ip address dhcp : Configure l'interface pour obtenir une adresse IP via DHCP.

Interface Vlan3 :

no forward interface Vlan1 : Empêche le transfert vers le VLAN 1.

no nameif : Supprime le nom de l'interface.

no security-level : Supprime le niveau de sécurité.

no ip address : Supprime l'adresse IP.

Interface Vlan100

nameif inside : Nomme l'interface "inside".

security-level 100 : Définit le niveau de sécurité à 100 (plus élevé).

ip address 192.168.10.2 255.255.255.252 : Assigne l'adresse IP 192.168.10.2 avec un masque de sous-réseau /30.

no shutdown : Active l'interface.

Interface Vlan200

no forward interface Vlan100 : Empêche le transfert vers le VLAN 100.

nameif dmz : Nomme l'interface "dmz".

security-level 50 : Définit le niveau de sécurité à 50 (intermédiaire).

ip address 192.168.1.254 255.255.255.0 : Assigne l'adresse IP 192.168.1.254 avec un masque de sous-réseau /24.

no shutdown : Active l'interface.

Interface Vlan300

nameif outside : Nomme l'interface "outside".

security-level 0 : Définit le niveau de sécurité à 0 (plus bas).

ip address 192.168.11.253 255.255.255.252 : Assigne l'adresse IP 192.168.11.253 avec un masque de sous-réseau /30.

no shutdown : Active l'interface.

Configuration des routes :

route inside 172.16.1.0 255.255.255.0 192.168.10.1 1 : Ajoute une route pour le réseau 172.16.1.0/24 via 192.168.10.1.

route inside 172.16.2.0 255.255.255.0 192.168.10.1 1 : Ajoute une route pour le réseau 172.16.2.0/24 via 192.168.10.1.

route outside 0.0.0.0 0.0.0.0 192.168.11.254 1 : Ajoute une route par défaut pour tout le trafic via 192.168.11.254.

ACL accessDMZ :

access-list accessDMZ extended permit tcp any host 192.168.1.2 eq www : Permet le trafic TCP sur le port 80 (HTTP) vers l'hôte 192.168.1.2.

access-list accessDMZ extended permit tcp any host 192.168.1.2 eq 443 : Permet le trafic TCP sur le port 443 (HTTPS) vers l'hôte 192.168.1.2.

access-list accessDMZ extended permit tcp any host 8.8.8.1 eq www : Permet le trafic TCP sur le port 80 (HTTP) vers l'hôte 8.8.8.1.

access-list accessDMZ extended permit tcp any host 8.8.8.1 eq 443 : Permet le trafic TCP sur le port 443 (HTTPS) vers l'hôte 8.8.8.1.

access-group accessDMZ in interface outside : Applique l'ACL accessDMZ à l'interface outside pour le trafic entrant.

Configuration NAT (Network Address Translation) :

nat (inside,outside) dynamic interface : Configure la NAT dynamique pour les adresses internes sortant via l'interface outside.

Configuration des classes et des politiques de trafic :

class-map traficInsideOutside : Classe de trafic trafic Inside Outside

match default-inspection-traffic : Définit une classe pour le trafic par défaut à inspecter.

Politique de trafic traficPolicy (policy-map traficPolicy) :

class traficInsideOutside : Applique la politique à la classe traficInsideOutside.

inspect http : Inspecte le trafic HTTP.

inspect icmp : Inspecte le trafic ICMP.

service-policy traficPolicy global : Applique la politique de service traficPolicy à l'échelle globale.

Configuration des services supplémentaires :

dhcpd auto_config outside : Configure automatiquement le DHCP pour l'interface outside..

7.4. Résumé du déroulement de la partie 3 :

Pour commencer, nous avons configuré les interfaces du routeur entreprise pour gérer les connexions internes et externes, en assignant les IP appropriées. Puis, nous avons mis en place les configurations NAT pour que les clients internes puissent accéder à Internet et que le serveur Web de la DMZ soit accessible de l'extérieur.

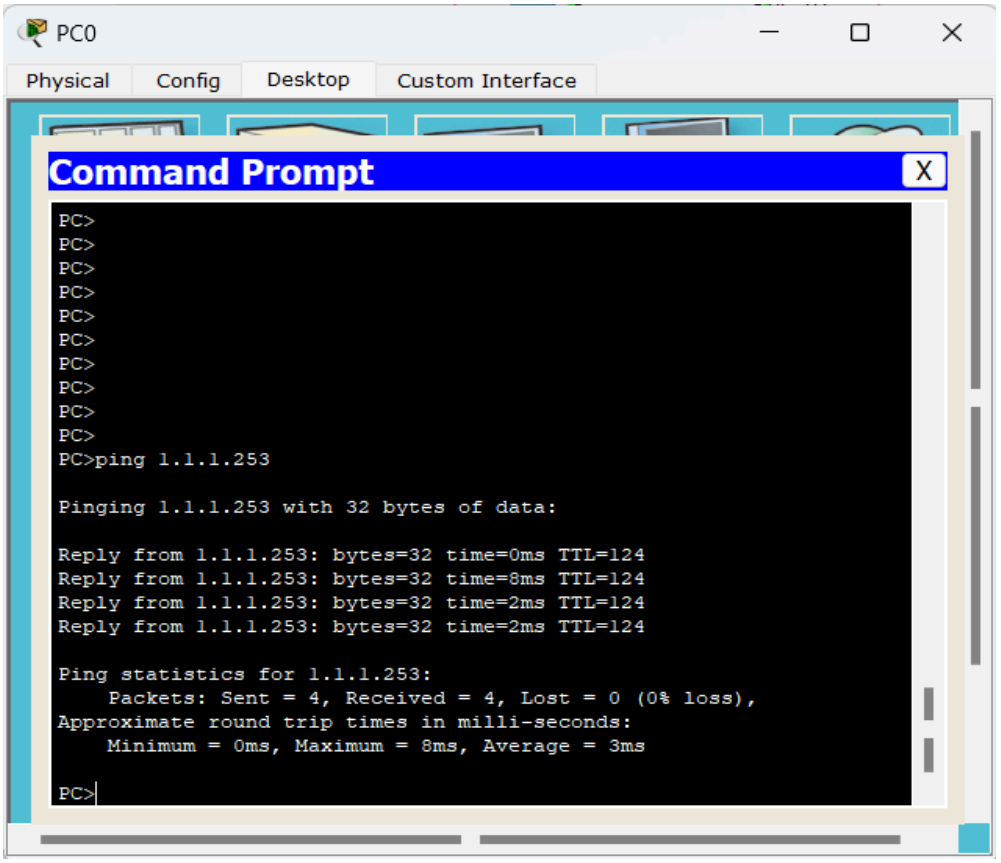
Puis, pour permettre aux clients locaux de partager une adresse IP publique unique (NAT dynamique), nous avons configuré le NAT overload. Nous avons également configuré le NAT statique pour que le serveur Web de la DMZ soit accessible à l'adresse externe 1.1.1.253, garantissant une accessibilité constante.

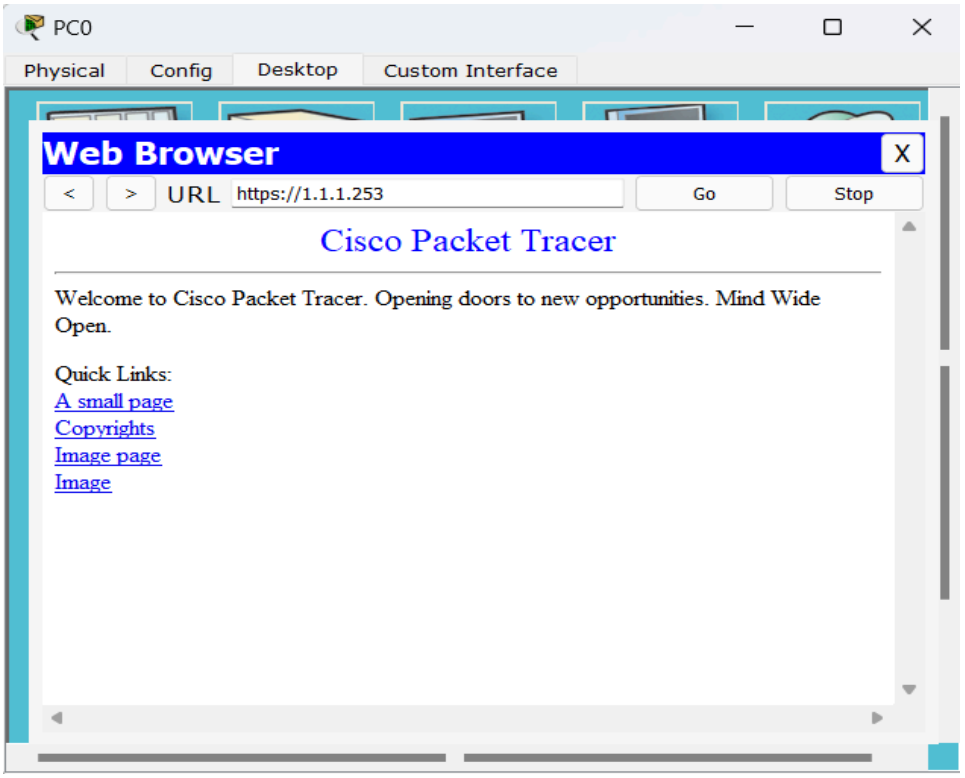
Ensuite, nous avons configuré les règles de pare-feu nécessaires sur l'ASA pour sécuriser les accès, en permettant uniquement le trafic sur les ports spécifiques pour les serveurs de la DMZ (HTTP et HTTPS) et en autorisant le trafic venant de l'extérieur uniquement s'il a été initié par les clients locaux, renforçant ainsi la sécurité du réseau interne.

Nous avons rencontré plusieurs problèmes. Tout d'abord, il y avait des problèmes avec l'interface VLAN 3 sur l'ASA où nous n'avons pas pu attribuer un nameif à VLAN 3 . Nous avons résolu cela en supprimant et en reconfigurant l'ASA (nous ne savons toujours pas quel était le problème). Ensuite, les configurations initiales sur les VLANs 1 et 2 causaient des dysfonctionnements donc nous avons changé les VLANs pour des numéros différents (100, 200, et 300). Enfin, nous avions oublié de configurer la route par défaut vers l'interface outside, ce qui empêchait les pings de fonctionner. Après avoir ajouté la route par défaut, les pings ont commencé à fonctionner correctement.

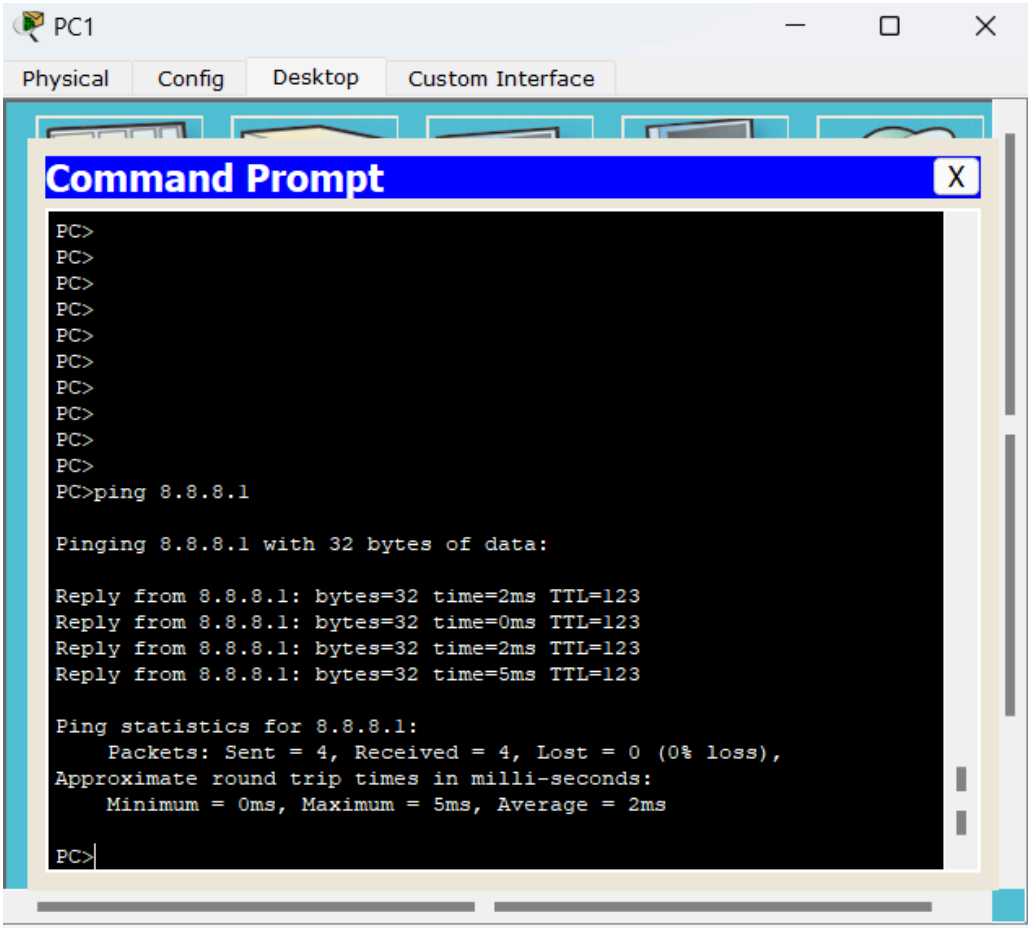
7.5. Tests de connectivité :

Vérification de l'accès au serveur Web de la DMZ depuis l'extérieur :





Vérification du NAT dynamique pour les clients locaux :



8. Étape 4 : Ajout du réseau public 8.8.0.0/16 et interconnexion avec le FAI

8.1. Configuration externe :

Configuration des interfaces
Interface GigabitEthernet0/0
ip address 8.8.8.2 255.255.0.0 : Assigne l'adresse IP 8.8.8.2 avec un masque de sous-réseau /16.
no shutdown : Active l'interface.
Interface GigabitEthernet0/1
ip address 1.1.2.129 255.255.255.252 : Assigne l'adresse IP 1.1.2.129 avec un masque de sous-réseau /30.
no shutdown : Active l'interface.
Interface Vlan1
no ip address : Supprime toute adresse IP assignée à l'interface VLAN 1.
shutdown : Désactive l'interface VLAN 1.

Configuration du protocole de routage EIGRP
router eigrp 1 : Active le processus EIGRP
network 8.8.0.0 0.0.255.255 : Ajoute le réseau 8.8.0.0/16 au processus EIGRP.
network 1.1.2.128 0.0.0.3 : Ajoute le réseau 1.1.2.128/30 au processus EIGRP.
Configuration des routes
ip route 0.0.0.0 0.0.0.0 1.1.2.130 : Ajoute une route par défaut pointant vers 1.1.2.130.

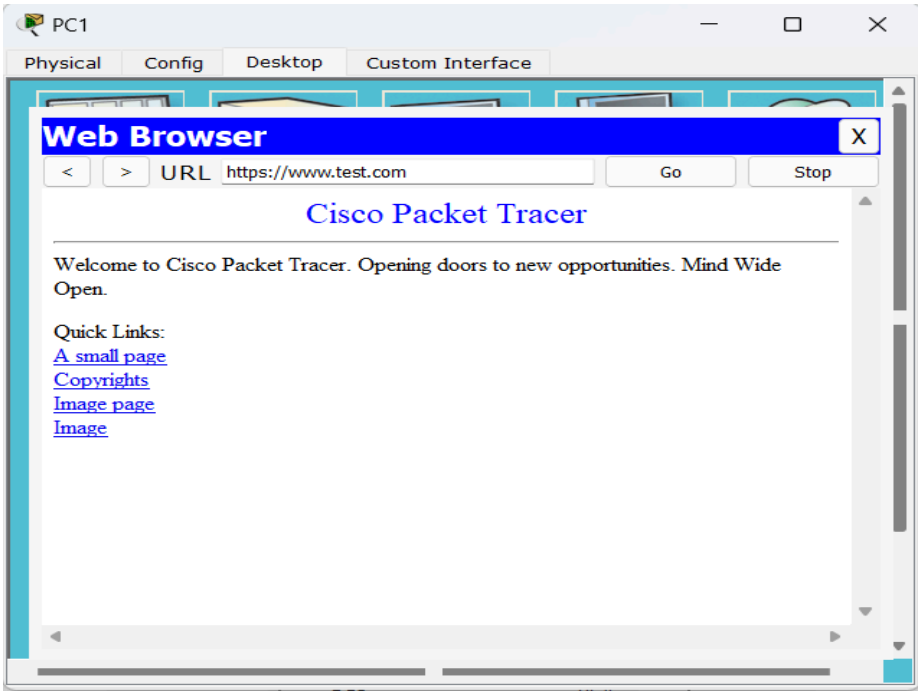
8.2. Résumé du déroulement de la partie 4 :

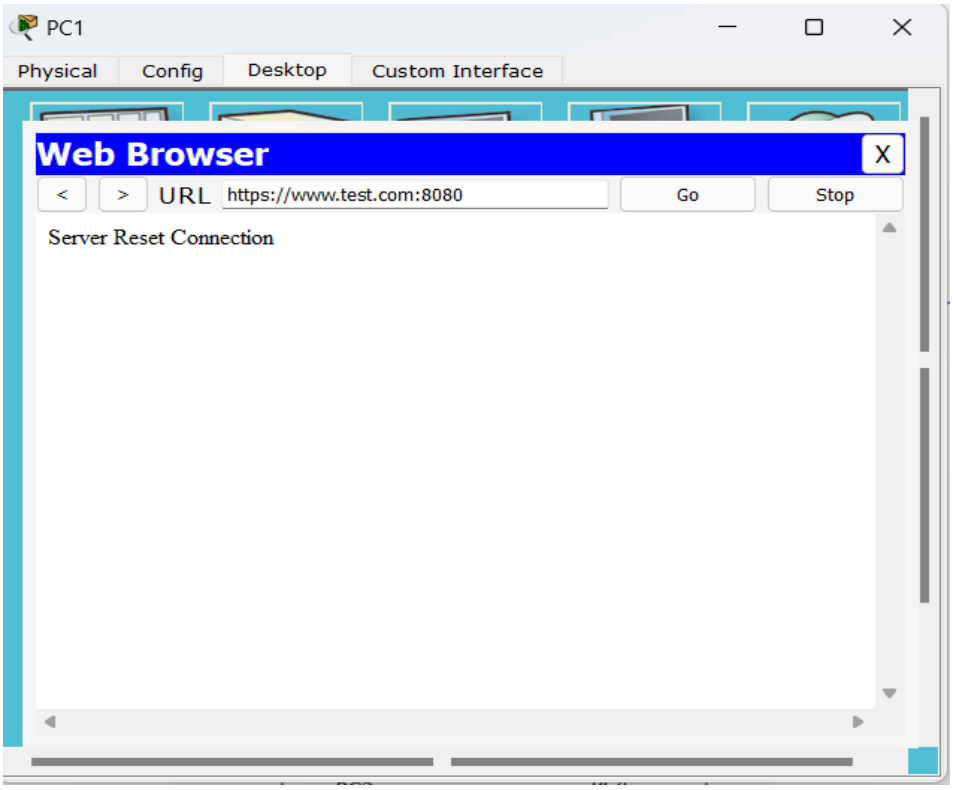
Nous avons dans un 1er temps effectué les commandes de base pour configurer le routeur, puis nous avons mis en place le protocole de routage EIGRP pour échanger les infos de routage avec le routeurFAI. Nous avons spécifié les deux réseaux auxquels le routeur est connecté.

Par la suite, nous avons rencontré un problème de connectivité. Après investigation, nous avons réalisé que nous avions oublié de configurer une route par défaut qui redirige le trafic vers l'intérieur du réseau. Une fois cette route ajoutée, la connectivité a été rétablie et le réseau a commencé à fonctionner correctement.

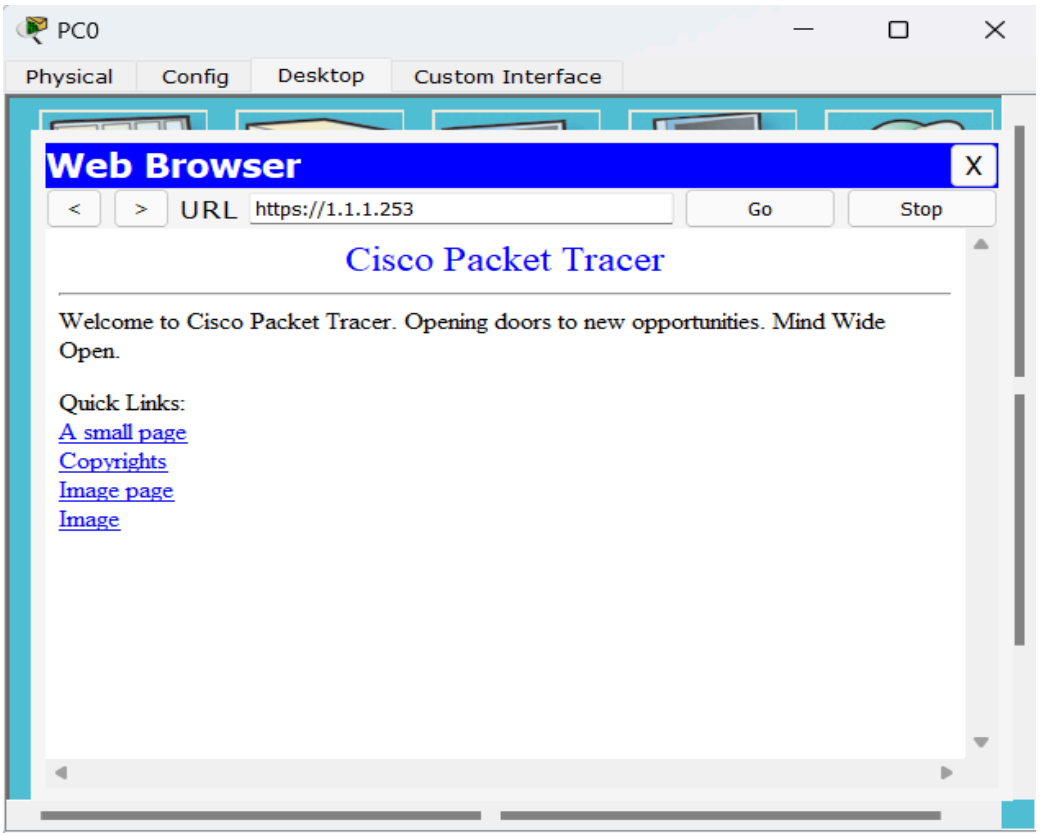
. 8.3. Tests de connectivité :

Vérification de l'accès des clients internes au réseau public :





Vérification de l'accès du client externe au serveur Web de l'entreprise :



9. Bibliographie et webographie :

-https://polar91.wordpress.com/2017/09/27/configure-multilayer-switch-on-packet-tracer/

-https://www.youtube.com/watch?v=SLZS1mSc_VY&list=PLKBs6BGQBEP4HUmB1g27aIL4EPyXeLNx

-https://itexamanswers.net/21-7-5-packet-tracer-configure-asa-basic-settings-and-firewall-using-the-cli-answers.html

-https://www.ccri.edu/faculty_staff/comp/jmowry/Security/ASA5506%209-3-1-2%20Lab%20-%20Configure%20ASA%20Basic%20Settings%20and%20Firewall%20Using%20CLI.pdf

-https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-dmz-00.html