SAE 21 RAPPORT GRP 30

Badaoui Walid

Trid Ilias

Fehmi Amir

Introduction

La SAÉ 2.1 s'inscrit dans le cadre de la formation Réseaux & Télécommunications (R&T) et vise à simuler une mission concrète de déploiement d'un réseau informatique pour une petite structure. En tant que futurs professionnels du secteur, nous devons être capables de concevoir, configurer et sécuriser une infrastructure réseau complète, fonctionnelle et évolutive, répondant aux besoins d'une PME.

Réalisé en trinôme, ce projet est entièrement développé sous Packet Tracer, un simulateur réseau permettant de valider l'architecture et le bon fonctionnement de l'ensemble des équipements et services mis en place.

Le travail est structuré en plusieurs étapes clés :

1. Construction du cœur de réseau : Mise en place des VLANs, configuration des switches d'accès, du switch multi-niveau (MLS) et vérification de la connectivité intra/inter-VLANs. Cette étape comprend également la configuration de l'arbre de pontage (STP) et la gestion des ports trunk/access.
2. Ajout du pare-feu ASA et des services réseau de base : Intégration du pare-feu Cisco ASA avec le MLS, mise en place d'un serveur DHCP centralisé pour tous les VLANs, et configuration du service DNS interne pour la résolution de noms.
3. Création de la DMZ et configuration du routeur FAI : Déploiement d'un réseau DMZ sécurisé, redirection de l'adresse publique vers le serveur Web interne, configuration des règles de sécurité sur le pare-feu, et mise en place du NAT (dynamique et statique) pour gérer les flux Internet entrants et sortants.
4. Ajout d'un réseau public externe et interconnexion avec le FAI : Création d'un réseau distant (8.8.0.0/16) contenant un serveur Web et un client de test, configuration de l'interconnexion via EIGRP, et test d'accessibilité croisée entre le réseau interne et le réseau externe, avec résolution DNS.

Chaque étape est accompagnée de configurations réseau commentées, de schémas d'architecture, ainsi que de tests de connectivité validés à l'aide de la simulation dans Packet Tracer. L'objectif est de garantir un fonctionnement fiable, une séparation logique des services, et un niveau de sécurité adapté aux usages internes et externes de l'entreprise.

Ce projet nous permet de mobiliser un large éventail de compétences techniques, tout en adoptant **une approche méthodique et professionnelle, essentielle à tout déploiement réseau en entreprise.**

Table des matières

Introduction....1
Cahier des charges....2
Schéma global....4
Plan d'adressage....6
Étape 1 : Construction du cœur de réseau avec les switches d'accès et le Multi-layer Switch (MLS) 8
Étape 2 : Ajout de l'ASA et du service DHCP 17
Étape 3 : Ajout de la DMZ et du routeur du FAI 25
Étape 4 – Ajout du réseau publique 8.8.0.0/16 et interconnexion avec le FAI....36
Conclusion....39

Cahier des charges

Contexte

Dans le cadre de cette SAÉ 2.1, il est demandé de concevoir une architecture réseau complète pour une petite entreprise. Ce projet, réalisé en trinôme et simulé entièrement sous Cisco Packet Tracer, s'inscrit dans une mise en situation réaliste d'un professionnel Réseaux & Télécommunications. L'entreprise cliente, bien que de taille modeste, exprime des besoins clairs en matière de connectivité interne, de services réseau, d'accès sécurisé à Internet, et de protection de ses ressources.

Objectifs généraux

Le réseau conçu devra permettre :

- La connexion de deux départements internes distincts (par exemple RH et Ingénierie) sur des réseaux séparés.
- L'hébergement de services internes (DHCP, DNS, Web) dans un VLAN serveur isolé.
- Le routage inter-VLAN pour assurer la communication entre les différents segments du réseau.
- L'accès sécurisé à Internet pour les utilisateurs internes via un pare-feu Cisco ASA.
- La mise en place d'une DMZ avec un serveur Web accessible depuis l'extérieur uniquement via les ports 80 (HTTP) et 443 (HTTPS).
- L'accès à un réseau public simulé (8.8.0.0/16) via le fournisseur d'accès Internet (FAI).

Architecture réseau prévue

Le réseau de l'entreprise sera organisé comme suit :

Élément	Adresse réseau prévue	Masque	Description
VLAN 10 (RH)	172.16.10.0	/24 (255.255.255.0)	Groupe de travail 1, 254 hôtes max
VLAN 20 (Ingénierie)	172.16.20.0	/24	Groupe de travail 2, 254 hôtes max
VLAN 30 (Serveurs)	10.0.0.0	/24	Services internes : DNS, DHCP, etc.
MLS ↔ ASA	192.168.10.0	/30 (255.255.255.252)	Lien point-à-point
ASA ↔ Routeur FAI	192.168.11.252	/30	Lien de sortie vers Internet
DMZ	192.168.1.0	/24	Hébergement du serveur Web externe
Réseau FAI	1.1.1.0	/24	Bloc d'adresses publiques attribué à l'entreprise
Réseau public test	8.8.0.0	/16	Réseau externe contenant un client et un serveur Web
Interconnexion FAI-test	1.1.2.128	/30	Lien entre FAI et le réseau public externe

Le multi-layer switch (MLS) assurera le routage inter-VLANs. Les switches d'accès seront configurés avec des ports en mode access et des trunks uniquement là où cela est nécessaire.

Services réseau

L'entreprise souhaite centraliser et automatiser l'attribution d'adresses et la résolution de noms. Un serveur DHCP unique dans le VLAN 30 distribuera les IPs aux VLANs 10 et 20, via la configuration de ip helper-address sur le MLS. Le DNS interne permettra la résolution de www.test.com (serveur externe) et www.entreprise.com (serveur DMZ). Externe, il résoudra l'adresse publique de l'entreprise.

Pour le NAT, une configuration dynamique (overload) sera utilisée pour les machines internes (VLAN 10 et 20), et une configuration statique sera réservée au serveur Web de la DMZ (1.1.1.253 → 192.168.1.x).

Sécurité

Le pare-feu ASA Cisco bloquera tout trafic non explicitement autorisé. Il ouvrira uniquement les ports 80 et 443 vers le serveur DMZ, et autorisera uniquement les connexions initiées par les clients internes. Le filtrage empêchera tout accès non sollicité aux machines internes.

Interconnexion avec l'extérieur

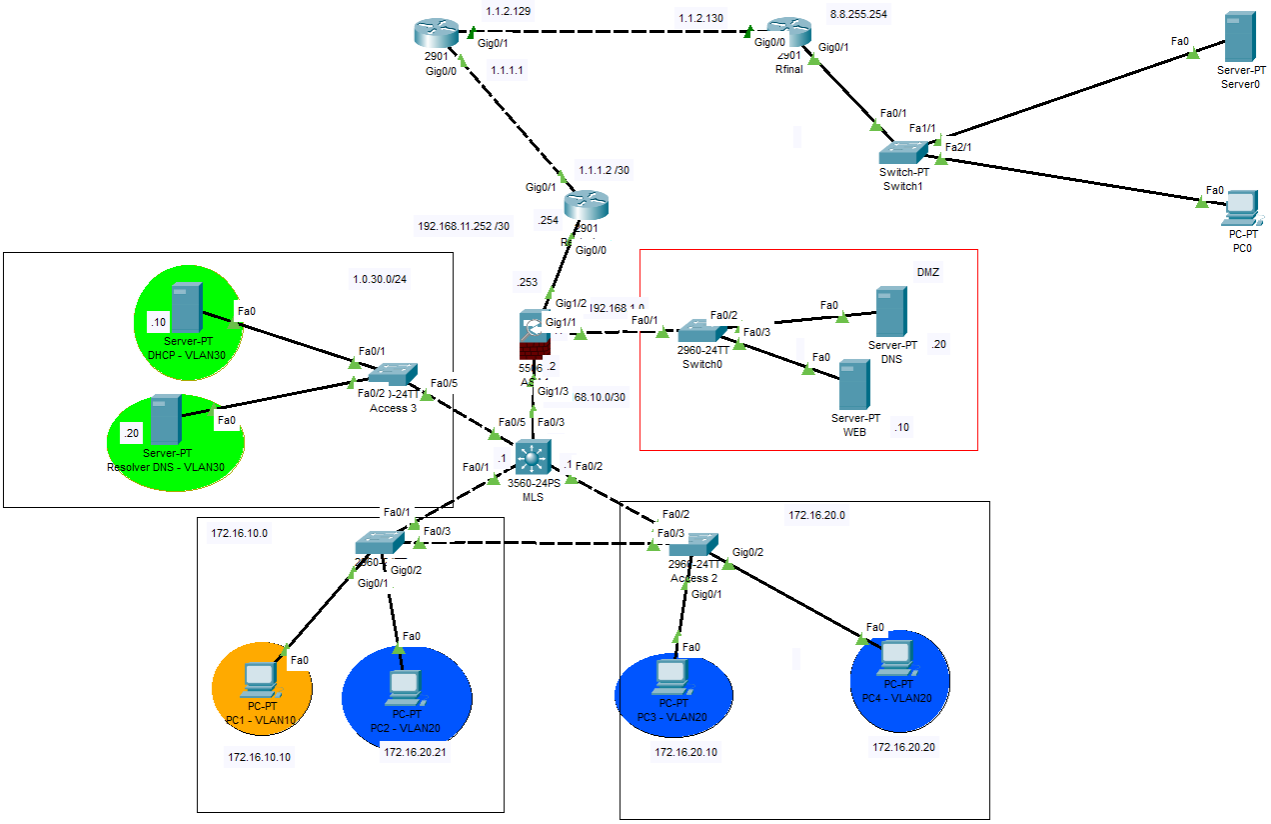
L'entreprise est connectée à un FAI simulé, qui fournit un bloc d'adresses publiques : 1.1.1.0/24. Une connexion inter-domaines est établie entre le FAI et un réseau public (8.8.0.0/16) via un lien /30 (1.1.2.128/30). Le routage EIGRP sera utilisé pour échanger les routes entre les réseaux (1.1.1.0/24 et 8.8.0.0/16).

Tests attendus

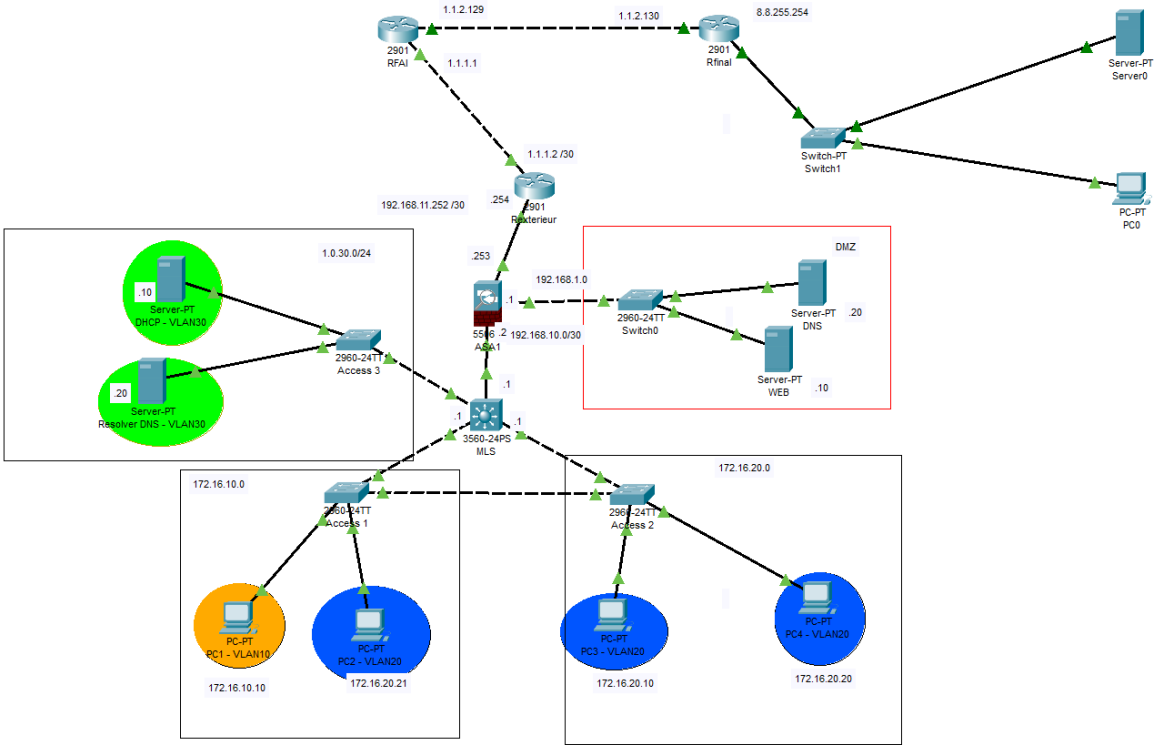
Test attendu	Objectif
Ping entre deux clients dans le même VLAN	Vérifier la connectivité de base
Ping entre deux VLANs différents via MLS	Vérifier le routage inter-VLAN
Attribution dynamique des adresses IP via DHCP	Vérifier le bon fonctionnement du serveur DHCP
Résolution DNS de www.test.com et www.entreprise.com	Vérifier la configuration DNS
Accès Internet depuis un client interne vers www.test.com	Tester la sortie Internet avec NAT dynamique
Accès au serveur Web DMZ depuis le client externe sur ports 80/443	Tester le NAT statique + règles ASA
Blocage des autres ports sur le serveur Web	Vérifier le filtrage du pare-feu
Vérification que le client externe ne peut pas initier une connexion aux clients internes	Tester la sécurité réseau

Schéma global

Avec ports


1.1.2.129
Gig0/1
2901
Gig0/0
1.1.1.1
1.1.2.130
Gig0/0
8.8.255.254
Gig0/1
Rfinal
Fa0
Server-PT
Server0
Fa0/1
Fa1/1
Fa2/1
Switch-PT
Switch1
Fa0
PC-PT
PC0
1.1.1.2 /30
Gig0/1
192.168.11.252 /30
.254
Gig0/0
1.0.30.0/24
.253
Gig1/2
Gig1/1
Fa0/1
DMZ
Fa0/2
Fa0/3
2960-24TT
Switch0
Fa0
Server-PT
DNS
.20
Fa0
Server-PT
WEB
.10
.10
Fa0
Server-PT
DHCP - VLAN30
Fa0/1
Fa0/2
Access 3
Fa0/5
.20
Fa0
Server-PT
Resolver DNS - VLAN30
Gig1/3
68.10.0/30
Fa0/5
Fa0/3
Fa0/1
.1
.1
Fa0/2
3560-24PS
MLS
172.16.10.0
Fa0/1
Fa0/3
Gig0/2
Gig0/1
Fa0/2
Fa0/3
172.16.20.0
Gig0/2
Gig0/1
Fa0
PC-PT
PC1 - VLAN10
Fa0
PC-PT
PC2 - VLAN20
172.16.10.10
172.16.20.21
Fa0
PC-PT
PC3 - VLAN20
Fa0
PC-PT
PC4 - VLAN20
172.16.20.10
172.16.20.20

Sans ports



Plan d’adressage

Réseaux Internes

Réseau	Adresse Réseau	Masque	Passerelle	Description
VLAN 10	172.16.10.0/24	255.255.255.0	172.16.10.1	Réseau client (ex : RH)
VLAN 20	172.16.20.0/24	255.255.255.0	172.16.20.1	Réseau client (ex : Ingénierie)
VLAN 30	10.0.30.0/24	255.255.255.0	10.0.30.1	Réseau Serveurs Internes

Réseaux Externes et DMZ

Réseau	Adresse Réseau	Masque	Passerelle	Description
DMZ	192.168.1.0/24	255.255.255.0	192.168.1.1	Réseau dédié aux services publics
Internet	8.8.0.0/16	255.255.0.0	8.8.255.254	Accès final vers Internet

Détails des VLANs et Equipements

VLAN 10

- Adresse réseau : 172.16.10.0/24
- Passerelle : 172.16.10.1
- PC1 : 172.16.10.10

VLAN 20

- Adresse réseau : 172.16.20.0/24
- Passerelle : 172.16.20.1
- PC2 : 172.16.20.21
- PC3 : 172.16.20.10
- PC4 : 172.16.20.20

VLAN 30 (Serveurs Internes)

- Adresse réseau : 10.0.30.0/24
- Passerelle : 10.0.30.1
- Serveur DHCP : 10.0.30.10

DMZ

- Adresse réseau : 192.168.1.0/24
- Passerelle : 192.168.1.1
- Serveur DNS : 192.168.1.20
- Serveur WEB : 192.168.1.10

Internet

- Adresse réseau : 8.8.0.0/16
- Passerelle : 8.8.255.254
- Serveur sur Internet : 8.8.8.1
- PC Externe : 8.8.8.2

Réseaux de Transit

Réseau	Adresse Réseau	Masque	Passerelle	Description
MLS ↔ ASA	192.168.10.0/30	255.255.255.252	MLS : 192.168.10.1	Transit entre MLS et ASA
ASA ↔ Ext	192.168.11.252/30	255.255.255.252	ASA : 192.168.11.253	Transit entre ASA et Rexterieur
Ext ↔ Final	1.1.2.128/30	255.255.255.252	Final : 1.1.2.130	Transit entre Rexterieur et Rfinal

Étape 1 : Construction du cœur de réseau avec les switches d'accès et le Multi-layer Switch (MLS)

Objectif de l'étape

La première étape consiste à construire le cœur du réseau en configurant les trois switches d'accès et le Multi-layer Switch (MLS). Ces équipements serviront les VLANs 10, 20 et 30 pour assurer une communication interne fluide et permettre le routage inter-VLANs. Les machines clientes doivent être configurées avec des adresses IP statiques, et les tests de connectivité doivent prouver que le réseau fonctionne correctement. En parallèle, le protocole spanning-tree (STP) doit être configuré pour éviter les boucles et garantir que le MLS est le switch racine des VLANs 10 et 20.

Configuration du Multi-layer Switch (MLS)

Le MLS joue un rôle central dans le réseau, servant à la fois de passerelle pour chaque VLAN et de point d'interconnexion avec le pare-feu ASA. Voici les principales configurations effectuées :

Activation du routage

La commande suivante a été utilisée pour activer le routage inter-VLANs sur le MLS, permettant aux VLANs de communiquer entre eux :

```
ip routing
```

Configuration des VLANs et des interfaces

Chaque VLAN a été configuré avec une interface logique et une adresse IP statique pour servir de passerelle :

- **VLAN 10** :
- `interface Vlan10`
- `ip address 172.16.10.1 255.255.255.0`
- `ip helper-address 10.0.30.10`

Commentaire : Cette configuration inclut un helper DHCP pour rediriger les requêtes vers le serveur DHCP situé dans le VLAN 30.

- **VLAN 20** :
- `interface Vlan20`
- `ip address 172.16.20.1 255.255.255.0`
- `ip helper-address 10.0.30.10`

Commentaire : Similaire au VLAN 10, cette configuration assure que les clients reçoivent leurs adresses IP via DHCP.

- **VLAN 30** :
- `interface Vlan30`
- `ip address 10.0.30.1 255.255.255.0`

Commentaire : Le VLAN 30 héberge les serveurs DHCP et DNS. Aucun helper DHCP n'est nécessaire ici.

Configuration STP (Spanning Tree Protocol)

Pour garantir que le MLS est le switch racine des VLANs 10 et 20, les commandes STP suivantes ont été utilisées :

```
spanning-tree mode pvst
spanning-tree vlan 10,20 priority 4096
```

Commentaire : Le mode PVST (Per VLAN Spanning Tree) permet une gestion indépendante du spanning-tree pour chaque VLAN. La priorité définie garantit que le MLS est le root bridge.

Configuration des trunks

Des trunks ont été configurés uniquement sur les ports nécessaires pour transporter le trafic des VLANs entre le MLS et les switches d'accès :

```
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Configuration de l'un des switches d'accès (exemple : Access1)

Un des switches d'accès (Access1) a été configuré pour gérer les VLANs 10 et 20. Voici les principales étapes :

Configuration des interfaces

```
Les interfaces connectées aux clients ont été configurées en mode access :
interface GigabitEthernet0/1
 switchport access vlan 10
 switchport mode access
interface GigabitEthernet0/2
 switchport access vlan 20
 switchport mode access
```

Configuration STP

Le mode PVST a été activé pour permettre une gestion du spanning-tree par VLAN :

```
spanning-tree mode pvst
```

Vérifications effectuées

Pour valider la configuration, plusieurs tests ont été réalisés :

Ping entre deux machines du même VLAN

1. **VLAN 20 :**
    - Ping entre PC2 (172.16.20.21) et PC3 (172.16.20.10).
      Ce test valide la communication à l'intérieur du VLAN 20.
    - Ping entre PC3 (172.16.20.10) et PC4 (172.16.20.20).
      Ce test confirme également que les machines du VLAN 20 communiquent correctement entre elles.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC2 - ...	PC3 - VLA...	ICMP		0.000	N	0	(edit)
	Successful	PC3 - ...	PC4 - VLA...	ICMP		0.000	N	1	(edit)

Ping entre deux machines de VLANs différents

1. **VLAN 10 vers VLAN 20 :**
    - Ping entre PC1 (172.16.10.10) et PC2 (172.16.20.21).
      Ce test valide le routage inter-VLANs entre le VLAN 10 et le VLAN 20.
    - Ping entre PC1 (172.16.10.10) et PC3 (172.16.20.10).
      Ce test confirme que le MLS permet la communication entre ces VLANs.
    - Ping entre PC1 (172.16.10.10) et PC4 (172.16.20.20).
      Ce test vérifie également le routage inter-VLANs.

```
Pinging 172.16.20.23 with 32 bytes of data:

Reply from 172.16.20.23: bytes=32 time<1ms TTL=127
Reply from 172.16.20.23: bytes=32 time<1ms TTL=127
Reply from 172.16.20.23: bytes=32 time<1ms TTL=127
Reply from 172.16.20.23: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.20.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.16.20.10

Pinging 172.16.20.10 with 32 bytes of data:

Reply from 172.16.20.10: bytes=32 time=1ms TTL=127
Reply from 172.16.20.10: bytes=32 time<1ms TTL=127
Reply from 172.16.20.10: bytes=32 time<1ms TTL=127
Reply from 172.16.20.10: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 172.16.20.20

Pinging 172.16.20.20 with 32 bytes of data:

Reply from 172.16.20.20: bytes=32 time<1ms TTL=127
Reply from 172.16.20.20: bytes=32 time<1ms TTL=127
Reply from 172.16.20.20: bytes=32 time<1ms TTL=127
Reply from 172.16.20.20: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.20.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

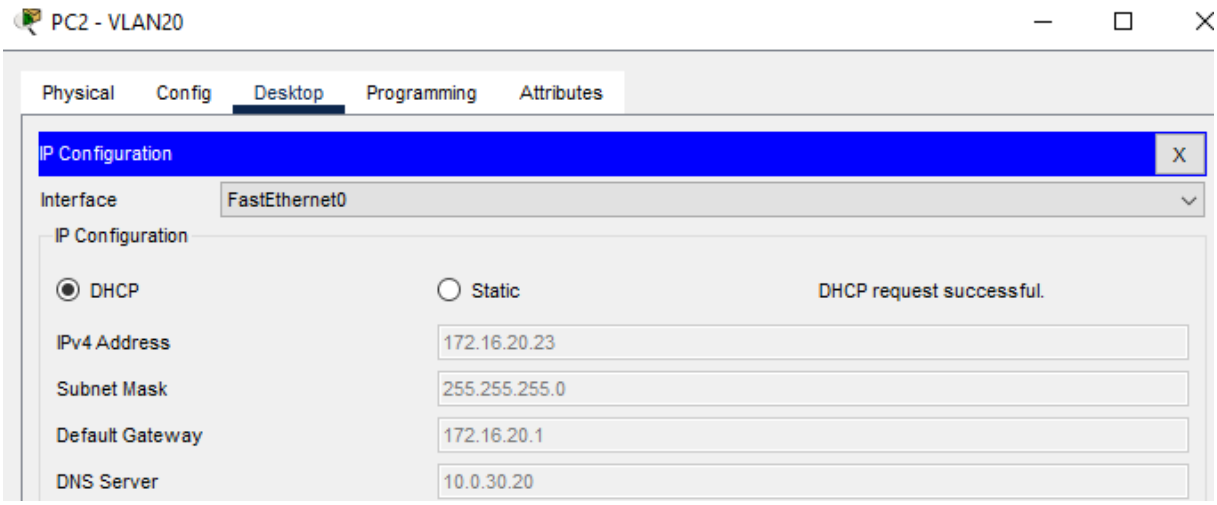
Remarque sur les tests de connectivité avec DHCP

Lors des tests de connectivité, il a été observé que les pings fonctionnent correctement, que les machines utilisent une adresse IP statique ou une adresse attribuée dynamiquement via le serveur DHCP. L'objectif de ce test était de valider que le serveur DHCP situé dans le VLAN 30 attribue des adresses correctes et conformes au plan d'adressage.

Dans le cas du poste **PC2** (situé dans le VLAN 20), le service DHCP a été activé temporairement afin de recevoir une adresse IP dynamique pour les tests. PC2 a reçu l'adresse suivante :

- **Adresse IPv4 :** 172.16.20.23
- **Masque de sous-réseau :** 255.255.255.0
- **Passerelle par défaut :** 172.16.20.1
- **Serveur DNS :** 10.0.30.20

Ce test confirme que le mécanisme de redirection des requêtes DHCP via le MLS fonctionne correctement. Cependant, les machines peuvent également être configurées avec des adresses statiques sans impact sur la connectivité réseau. La configuration statique reste une option viable pour garantir des adresses fixes à certains postes critiques.



Dans l'étape 2 nous verrons la configuration faite sur le serveur dhcp pour en voir la corrélation avec cette capture d'écran.

Problèmes rencontrés et solutions

Lors de la mise en place du cœur de réseau, plusieurs problèmes ont été identifiés et corrigés pour garantir une configuration fonctionnelle et cohérente. Ces erreurs concernaient principalement l'adressage IP, la configuration des ports et la gestion des VLANs.

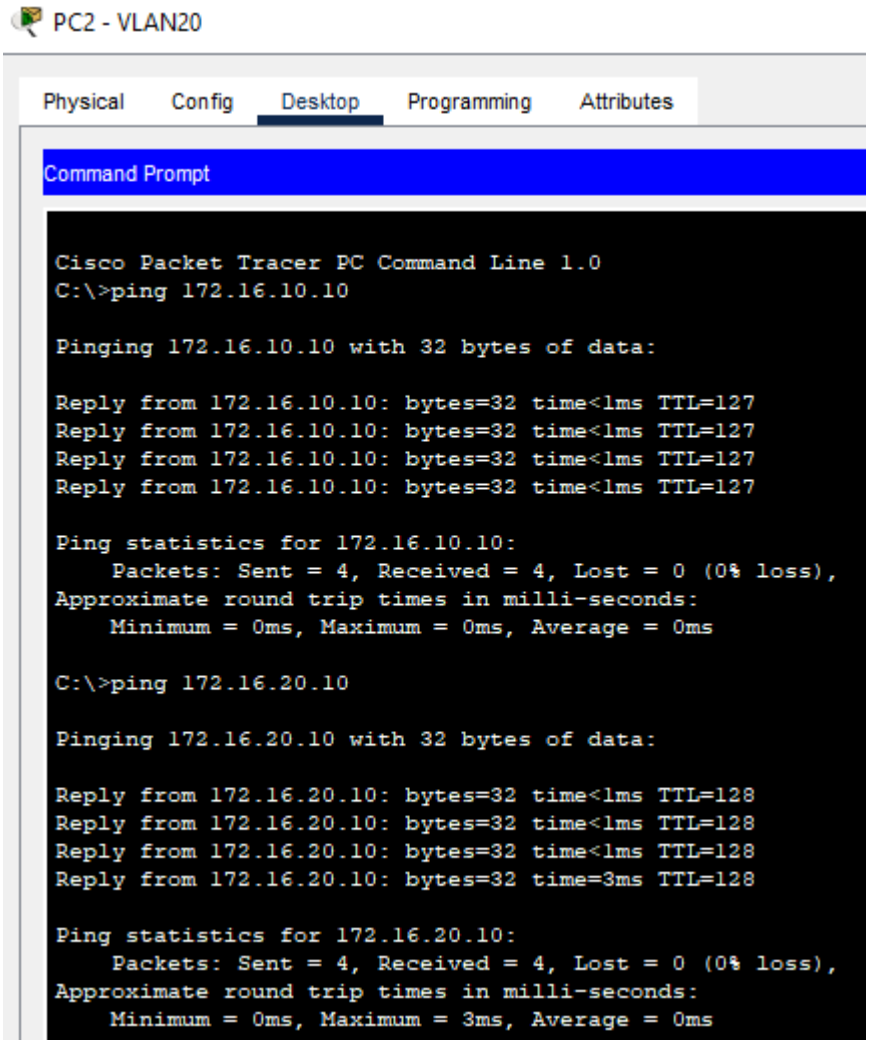
Le premier problème concernait le poste PC2 dans le VLAN 20, qui n'était pas pinguable depuis aucun autre équipement. Après investigation, il s'est avéré que ce poste avait été configuré avec une adresse IP appartenant au VLAN 10, à savoir 172.16.10.20, au lieu d'une adresse correspondant au réseau VLAN 20 (172.16.20.0/24). Cette erreur d'adressage empêchait la communication au sein du VLAN 20 et aurait pu provoquer des conflits d'adresses IP si un poste du VLAN 10 utilisait également

l’adresse 172.16.10.20. Pour corriger ce problème, l’adresse IP de PC2 a été modifiée et replacée dans la plage correcte du VLAN 20 (172.16.20.21). De plus, le pool DHCP du VLAN 20 a été ajusté pour exclure les adresses statiques attribuées manuellement, évitant ainsi toute attribution conflictuelle.

Le deuxième problème concernait une mauvaise affectation du VLAN 30 sur le port FastEthernet0/5. Par erreur, le VLAN 30 avait été configuré sur le port FastEthernet0/4, créant ainsi un « mismatch » dans la configuration des VLANs. Ce port devait rester dans le VLAN 1 par défaut, et cette mauvaise affectation entraînait des incohérences dans la connectivité. Pour résoudre ce problème, le port FastEthernet0/4 a été déconfiguré et réattribué au VLAN 1, tandis que le port FastEthernet0/5 a été correctement configuré pour le VLAN 30, conformément au plan réseau.

Enfin, le troisième problème concernait le port FastEthernet0/5, qui était configuré en mode routable (no switchport). Ce mode empêchait la configuration VLAN sur ce port, le rendant incompatible avec les besoins du VLAN 30. La solution a été d’activer le mode commuté sur le port avec la commande switchport mode access, permettant ainsi une configuration correcte du VLAN 30 sur ce port.

Ces corrections ont permis de résoudre les problèmes rencontrés et d’assurer une cohérence dans la configuration du réseau. Les tests de ping réalisés après ces ajustements ont confirmé que les machines des différents VLANs pouvaient communiquer correctement, et que la topologie réseau était conforme aux attentes.



Les tests de ping effectués sur **PC2** (situé dans le VLAN 20) montrent que la connectivité fonctionne correctement lorsqu'il utilise une adresse IP statique. Ces tests ont été réalisés pour valider que la configuration réseau est cohérente et que les machines peuvent communiquer indépendamment de l'utilisation du service DHCP.

Détails des tests effectués :

1. **Ping entre PC2 (VLAN 20) et PC1 (VLAN 10) :**
    - Commande utilisée : ping 172.16.10.10.
    - Résultat : Réponse positive avec 0% de perte de paquets. Cela confirme que le routage inter-VLANs est opérationnel.
2. **Ping entre PC2 (VLAN 20) et PC3 (VLAN 20) :**
    - Commande utilisée : ping 172.16.20.10.
    - Résultat : Réponse positive avec 0% de perte de paquets. Cela valide la communication interne au VLAN 20.

Conclusion

Que **PC2** utilise une adresse IP statique ou qu'il obtienne son adresse dynamiquement via DHCP, les pings fonctionnent correctement dans les deux cas. Cela démontre que la configuration des VLANs et du routage inter-VLANs sur le MLS est robuste et fonctionnelle.

Test du Spanning Tree Protocol (STP)

Objectif

Le protocole **Spanning Tree Protocol (STP)** est activé dans le réseau pour éviter les boucles et garantir une topologie stable. Ce test a pour but de valider que la configuration STP est correcte et que le MLS joue son rôle de **root bridge** pour les VLANs 10 et 20.

Résultats des vérifications

VLAN 1

- **Root Bridge** : Le root bridge pour le VLAN 1 est identifié avec l'adresse MAC 0002.4A30.598D, accessible via le port FastEthernet0/2.
- **Rôle des interfaces** :
    - Fa0/1 : Alternatif (**BLK** – Bloqué), utilisé pour éviter les boucles.
    - Fa0/2 : Root (**FWD** – Transmet), utilisé pour atteindre le root bridge.

VLAN 10

- **Root Bridge** : Le MLS est le root bridge, avec l'adresse MAC 00D0.D3EB.A80A.
- **Rôle des interfaces** :
    - Fa0/1 et Fa0/2 : Interfaces désignées (**FWD** – Transmet), participant activement au trafic.

VLAN 20

- **Root Bridge** : Le MLS est également le root bridge, avec l'adresse MAC 00D0.D3EB.A80A.
- **Rôle des interfaces** :
    - Fa0/1 et Fa0/2 : Interfaces désignées (**FWD** – Transmet).

VLAN 30

- **Root Bridge** : L'adresse MAC du root bridge pour le VLAN 30 est 0002.17BA.4EC5, accessible via le port FastEthernet0/5.
- **Rôle des interfaces** :
    - Fa0/1 et Fa0/2 : Interfaces désignées (**FWD** – Transmet).
    - Fa0/5 : Root (**FWD** – Transmet), utilisé pour atteindre le root bridge.

Conclusion

Les tests confirment que le protocole STP est correctement configuré :

1. Le MLS est bien le **root bridge** pour les VLANs 10 et 20, grâce à une priorité réduite (4096).
2. Les interfaces sont correctement réparties entre les rôles **Root**, **Designated**, et **Blocking**, garantissant une topologie sans boucle.
3. Les VLANs 1 et 30 ont des root bridges externes, accessibles via les ports appropriés.

En cas de défaillance, STP recalculera automatiquement une nouvelle topologie pour maintenir la stabilité du réseau.

```
MLS#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0002.4A30.598D
              Cost        19
              Port        2(FastEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.D3EB.A80A
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Altn BLK 19        128.1    P2p
Fa0/2            Root FWD 19        128.2    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              Address     00D0.D3EB.A80A
              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     00D0.D3EB.A80A
              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
Fa0/2            Desg FWD 19        128.2    P2p
```

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    4116
              Address     00D0.D3EB.A80A
              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     00D0.D3EB.A80A
              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
Fa0/2            Desg FWD 19        128.2    P2p

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID     Priority    32798
              Address     0002.17BA.4EC5
              Cost        19
              Port        5(FastEthernet0/5)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32798  (priority 32768 sys-id-ext 30)
              Address     00D0.D3EB.A80A
              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
Fa0/5            Root FWD 19        128.5    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

Résultats finaux

Les tests de ping et spanning-tree montrent que le cœur du réseau est désormais fonctionnel :

- Les machines d'un même VLAN et de VLANs différents communiquent correctement.
- Le MLS est bien le switch racine pour les VLANs 10 et 20.
- Les erreurs d'adressage IP et de configuration des ports ont été corrigées.

Étape 2 : Ajout de l'ASA et du service DHCP

L'objectif de cette étape est d'intégrer le pare-feu ASA et de configurer un service DHCP pour les VLANs. Cette partie du projet assure la sécurité du réseau avec la mise en place d'un pare-feu et facilite la gestion des IP en automatisant leur attribution via un serveur DHCP.

Interconnexion ASA ↔ MLS

Le pare-feu ASA doit être relié au Multi-Layer Switch (MLS) pour assurer la communication entre les VLANs internes et les réseaux externes. Cette interconnexion nécessite de passer l'interface du MLS en mode de routage (niveau 3) et de configurer les interfaces correspondantes sur l'ASA.

Commandes effectuées sur le MLS

```
MLS(config)# ip routing
```

Configuration de l'interface connectée à l'ASA

```
MLS(config)# interface FastEthernet0/3
MLS(config-if)# no switchport
MLS(config-if)# ip address 192.168.10.1 255.255.255.252
MLS(config-if)# no shutdown
MLS(config-if)# exit
```

Commandes effectuées sur l'ASA

Configuration de l'interface connectée au MLS

```
ASA(config)# interface GigabitEthernet1/3
ASA(config-if)# nameif inside
ASA(config-if)# security-level 100
ASA(config-if)# ip address 192.168.10.2 255.255.255.252
ASA(config-if)# no shutdown
ASA(config-if)# exit
```

Configuration des routes statiques sur l'ASA

```
ASA(config)# route inside 172.16.10.0 255.255.255.0 192.168.10.1
ASA(config)# route inside 172.16.20.0 255.255.255.0 192.168.10.1
ASA(config)# route inside 10.0.30.0 255.255.255.0 192.168.10.1
ASA(config)# route outside 0.0.0.0 0.0.0.0 192.168.11.254
```

---

2. Activation du service DNS

Objectif

Configurer le serveur DNS dans la DMZ et ajouter les enregistrements nécessaires pour la résolution des noms de domaine.

Configuration du serveur DNS

- Activation du service DNS sur le serveur DMZ.
- Ajout des enregistrements :
    - **Type A** pour **www.test.com** → Adresse IP : **8.8.8.1**
    - **Type A** pour **www.entreprise.com** → Adresse IP : **192.168.1.10**.

Commandes sur le serveur DNS

DNS Server Setup:

- Domain Name: www.test.com

- Type: A

- IP Address: 8.8.8.1

- Domain Name: www.entreprise.com

- Type: A

- IP Address: 192.168.1.10

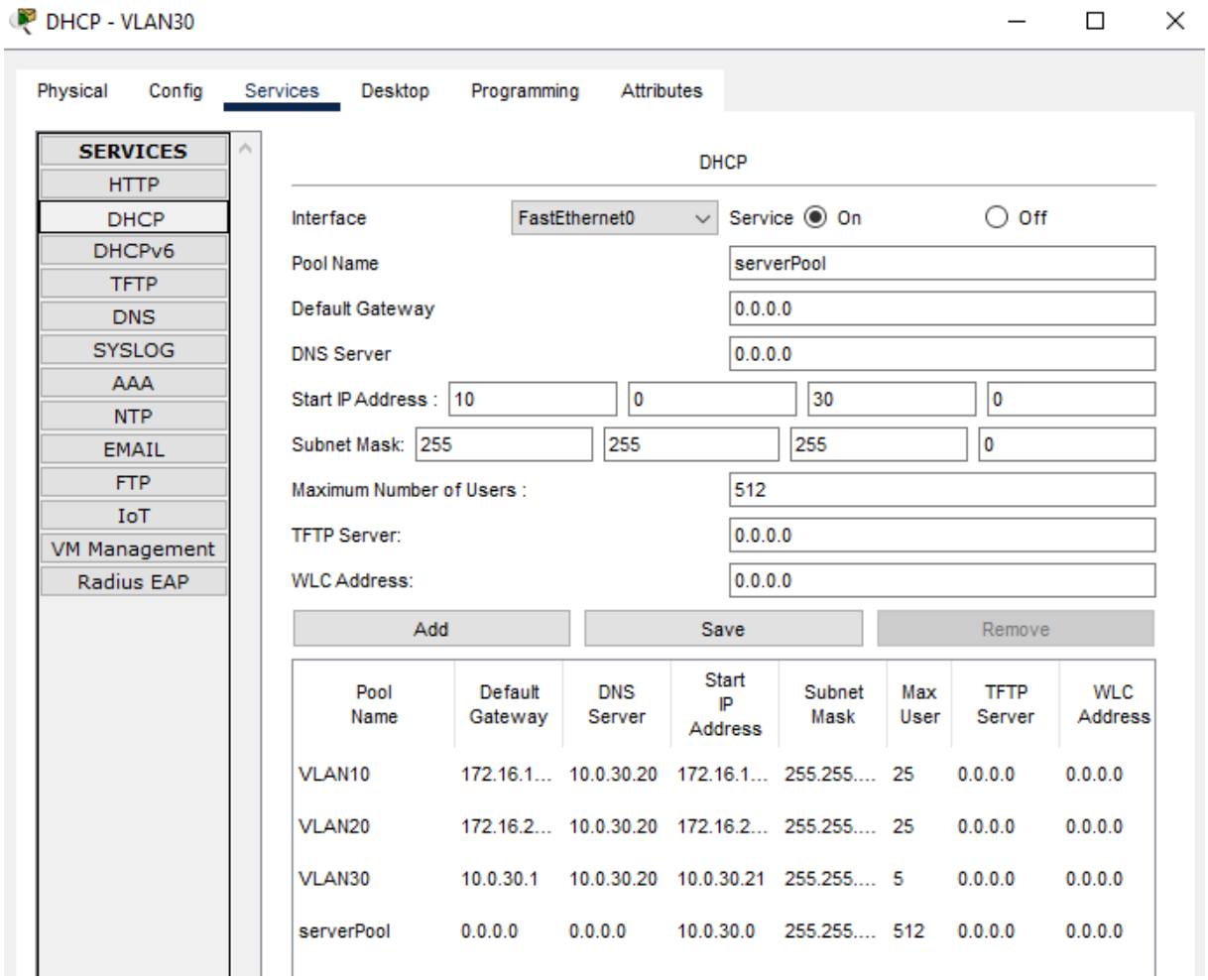
---

3. Ajout du serveur DHCP

Objectif

Un serveur DHCP est installé dans le VLAN Serveurs (VLAN 30) pour attribuer automatiquement des adresses IP aux clients des VLANs 10 et 20. Les requêtes DHCP des VLANs sont redirigées vers ce serveur grâce à la configuration des IP helper address sur le MLS.Configuration du serveur DHCP.

- **VLAN 10 Pool** :
    - Subnet : **172.16.10.0/24**
    - Range : **172.16.10.100 - 172.16.10.200**
    - Gateway : **172.16.10.1**
    - DNS Server : **192.168.1.20**
- **VLAN 20 Pool** :
    - Subnet : **172.16.20.0/24**
    - Range : **172.16.20.100 - 172.16.20.200**
    - Gateway : **172.16.20.1**
    - DNS Server : **192.168.1.20**



Commandes sur le MLS

Ajout des IP helper address pour rediriger les requêtes DHCP

```
MLS(config)# interface Vlan10
MLS(config-if)# ip helper-address 10.0.30.10
MLS(config-if)# exit

MLS(config)# interface Vlan20
MLS(config-if)# ip helper-address 10.0.30.10
MLS(config-if)# exit
```

Problème rencontré avec l'ASA 5505

Lors de la configuration de la DMZ avec l'ASA 5505, une limitation importante de Packet Tracer a été rencontrée. L'énoncé du TP demandait d'utiliser la commande no forward interface inside pour activer une troisième interface dédiée à la DMZ. Cependant, cette commande n'est pas reconnue par Packet Tracer.

Message d'erreur affiché :

```
% Invalid input detected at '^' marker.
```

Après vérification dans l'aide contextuelle (?), il s'avère que la commande no forward n'est pas disponible dans Packet Tracer. De plus, l'ASA 5505 dans Packet Tracer ne permet d'activer que deux interfaces simultanément **(inside et outside), ce qui empêche la mise en place de la DMZ comme demandé.**

Solution adoptée : Migration vers l'ASA 5506

Pourquoi l'ASA 5506 ?

Pour contourner les limitations du modèle ASA 5505, l'ASA 5506 a été utilisé. Ce modèle permet de configurer plusieurs interfaces actives, notamment inside, outside, et dmz. L'utilisation de l'ASA 5506 a rendu la commande no forward interface inutile et permis de respecter les exigences du TP.

La migration vers l'ASA 5506 a permis de :

- Configurer correctement les trois interfaces nécessaires.
- Activer la DMZ sans obstacle lié à Packet Tracer.
- Réaliser tous les tests requis avec succès.

Tests effectués

1. Ping entre ASA et MLS

- Résultat : Ping réussi entre 192.168.10.1 (MLS) et 192.168.10.2 (ASA).
- Et inversement.

```
MLS#ping 192.168.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
```

```
ciscoasa#ping 192.168.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/4 ms

ciscoasa#
```

2. Résolution DNS

Le test de la résolution DNS est une étape essentielle pour valider que le serveur DNS interne, situé dans le VLAN Serveurs (VLAN 30), est correctement configuré et peut répondre aux requêtes des machines internes. Cela permet aux utilisateurs du réseau interne d'accéder aux ressources externes et internes via leurs noms de domaine, plutôt que leurs adresses IP.

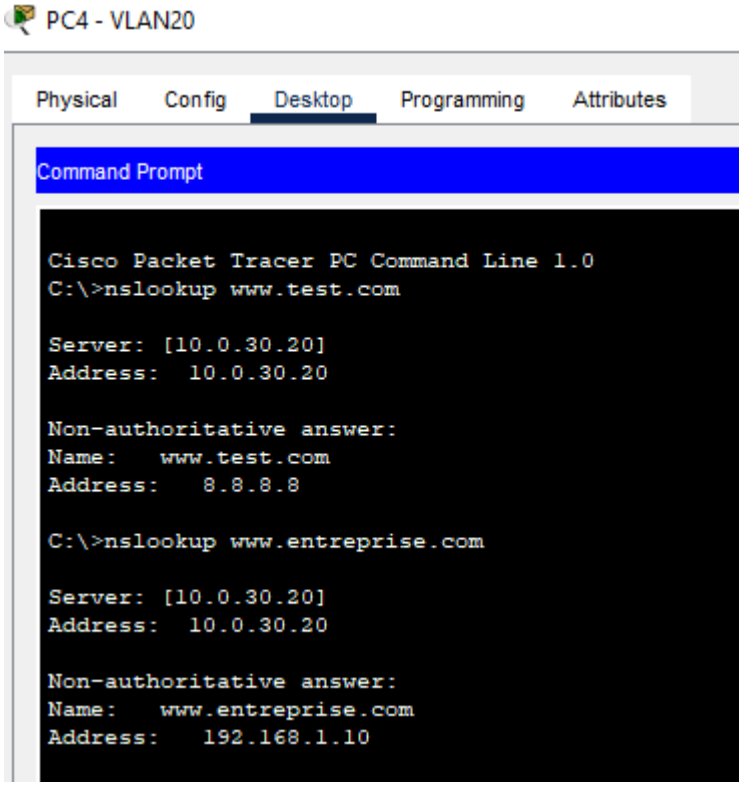
La résolution DNS est un élément essentiel pour valider le fonctionnement du serveur DNS interne et garantir que les machines du réseau puissent accéder aux ressources via leurs noms de domaine.

Dans ce test, un PC situé dans le VLAN 20 a été utilisé pour interroger le serveur DNS interne, configuré dans le VLAN Serveurs (VLAN 30). Le serveur DNS a été configuré avec des enregistrements de type **A** pour les domaines **www.entreprise.com** et **www.test.com**, pointant respectivement vers les adresses IP **192.168.1.10** (serveur Web dans la DMZ) et **8.8.8.1** (serveur Web externe).

Depuis le PC, la commande **nslookup** a été exécutée pour tester la résolution des deux domaines. Lors de la requête pour **www.entreprise.com**, le serveur DNS interrogé était bien celui configuré à l'adresse **10.0.30.20**, comme prévu. La réponse obtenue indique que le domaine **www.entreprise.com** est correctement résolu en **192.168.1.10**, prouvant que l'enregistrement de type **A** pour ce domaine est fonctionnel. De manière similaire, la commande **nslookup** pour **www.test.com** a produit une réponse correcte, avec le domaine résolu en **8.8.8.1**, confirmant également la validité de sa configuration DNS.

Ces résultats montrent que le serveur DNS interne est accessible et opérationnel, et que les machines des VLANs clients peuvent interagir avec lui pour résoudre les noms de domaine configurés. La réponse obtenue est de type **Non-authoritative answer**, ce qui signifie que le serveur DNS a répondu en relayant l'information depuis sa configuration locale ou son cache interne.

En conclusion, le test de résolution DNS est concluant. Les domaines **www.entreprise.com** et **www.test.com** sont correctement résolus, validant ainsi l'efficacité de la configuration DNS. Ces résultats permettent de garantir une utilisation simplifiée des noms de domaine pour accéder aux ressources internes et externes. L'image ci-jointe illustre la commande exécutée pour **www.entreprise.com** et pour **www.test.com**, montrant la réussite du test et la réponse du serveur DNS.



3. DHCP

Test de l'attribution d'adresse IP via DHCP

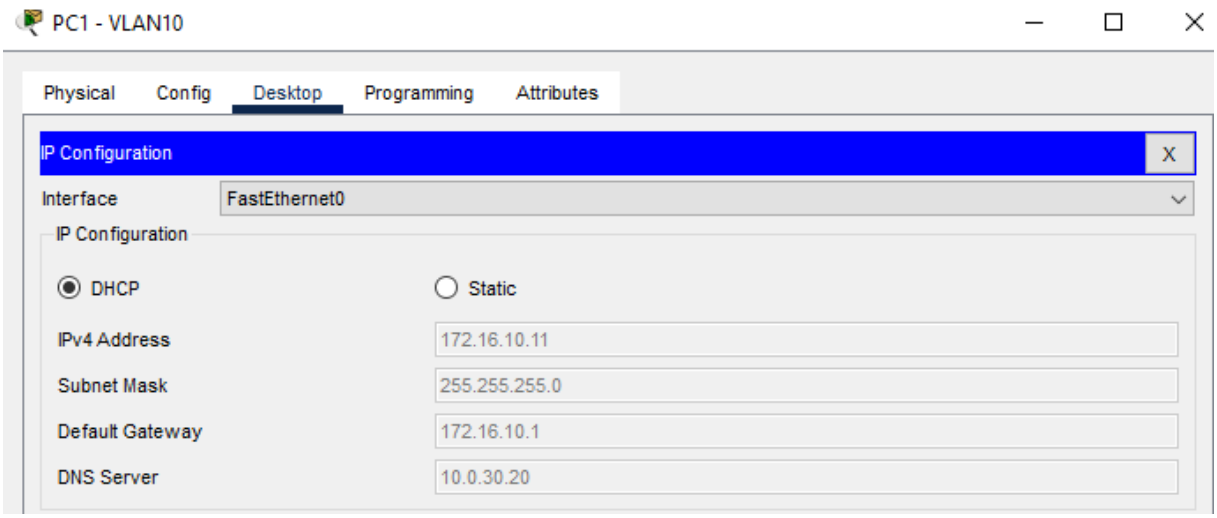
Le test de l'attribution dynamique d'une adresse IP par le serveur DHCP est une étape essentielle pour vérifier que la configuration du service DHCP est correcte et que les machines des VLANs internes peuvent recevoir automatiquement une adresse valide. Dans ce cas, le **PC 1** situé dans le VLAN 10 a été utilisé pour effectuer ce test.

Lors de la configuration du PC 1, l'option **DHCP** a été sélectionnée dans les paramètres réseau au lieu de l'attribution statique. Après avoir activé cette option, le PC a automatiquement reçu une adresse IP attribuée par le serveur DHCP. Les informations affichées dans la capture d'écran montrent que l'attribution a été réalisée avec succès. Le PC a reçu l'adresse **172.16.10.11**, qui appartient à la plage d'adresses IP configurée pour le VLAN 10 dans le serveur DHCP.

En plus de l'adresse IP, le PC a également obtenu les paramètres réseau suivants :

- **Masque de sous-réseau** : **255.255.255.0**, correspondant au sous-réseau du VLAN 10.
- **Passerelle par défaut** : **172.16.10.1**, correspondant à l'interface du MLS pour le VLAN 10.
- **Serveur DNS** : **10.0.30.20**, correspondant à l'adresse du serveur DNS interne configuré dans le VLAN Serveurs.

Ces résultats confirment que la configuration DHCP est fonctionnelle et que le serveur DHCP attribue correctement les adresses IP aux machines situées dans le VLAN 10. L'image ci-jointe illustre clairement les informations réseau reçues par le PC, validant ainsi le succès du test.

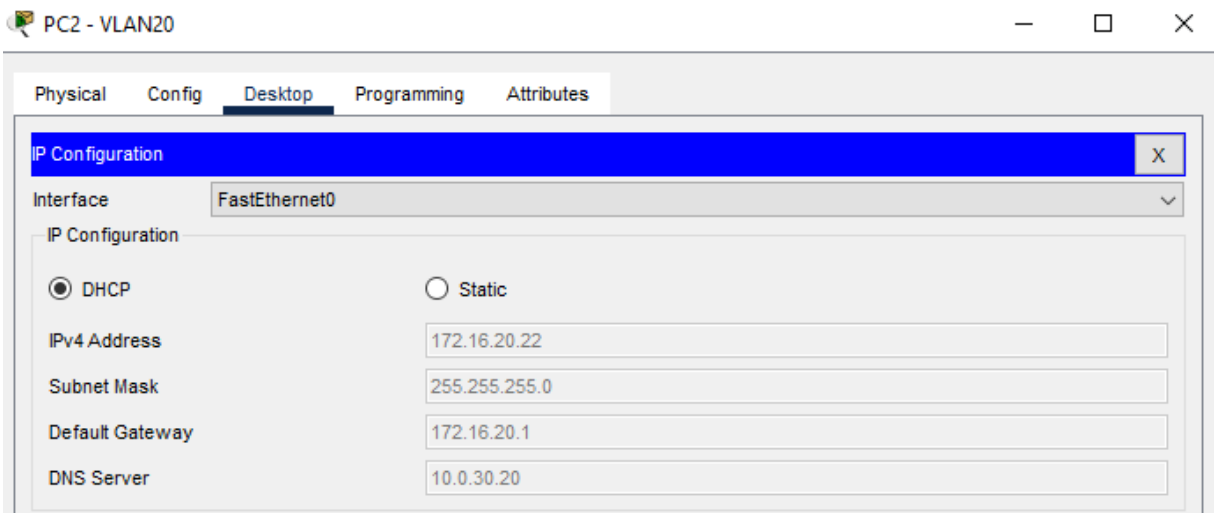


Le **PC 2**, situé dans le VLAN 20, a été configuré pour utiliser l'attribution dynamique d'adresse via DHCP. Après activation de l'option **DHCP**, le PC a reçu automatiquement les paramètres réseau suivants :

- **Adresse IP** : **172.16.20.22**
- **Masque de sous-réseau** : **255.255.255.0**
- **Passerelle par défaut** : **172.16.20.1**

- **DNS Server** : **10.0.30.20**

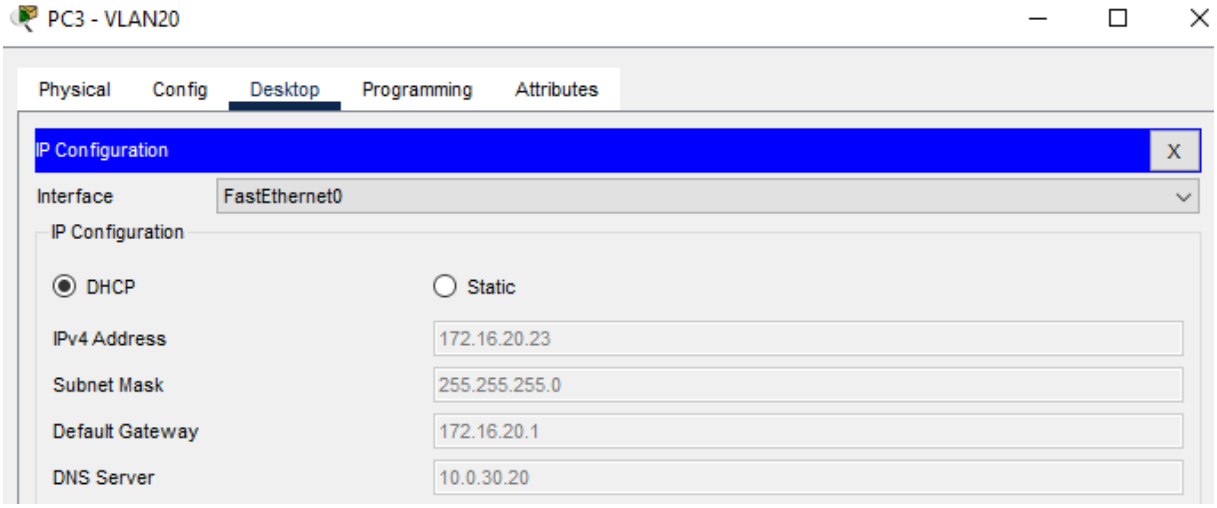
Ces informations confirment que le serveur DHCP attribue correctement les adresses et paramètres réseau au VLAN 20. L'image ci-jointe illustre ces résultats.



Le **PC 3**, situé dans le VLAN 20, a également été configuré pour utiliser l'attribution dynamique d'adresse via DHCP. Après activation de l'option **DHCP**, le PC a reçu automatiquement les paramètres réseau suivants :

- **Adresse IP** : **172.16.20.23**
- **Masque de sous-réseau** : **255.255.255.0**
- **Passerelle par défaut** : **172.16.20.1**
- **DNS Server** : **10.0.30.20**

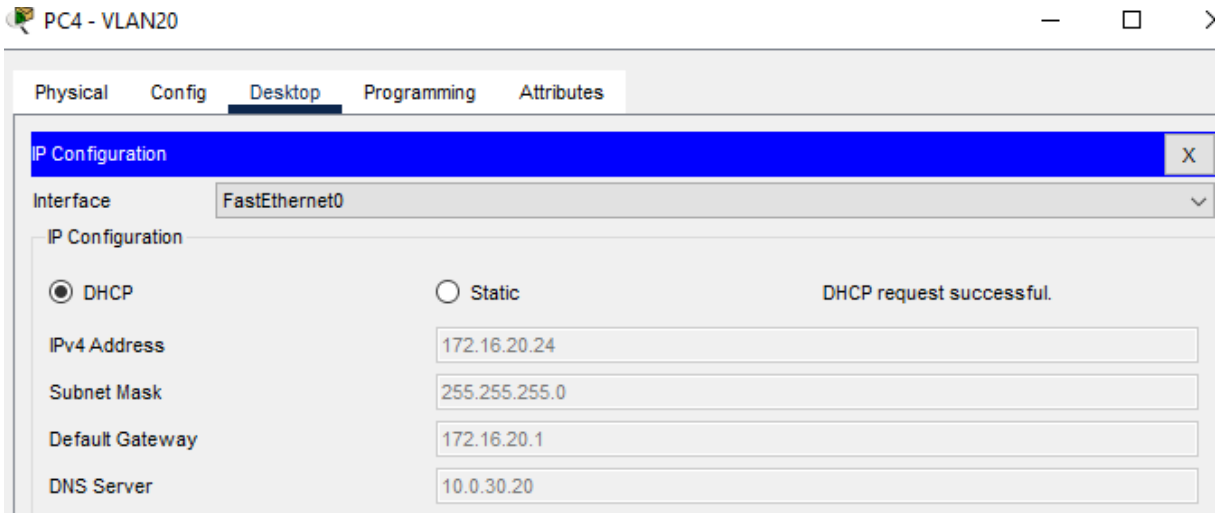
Ces informations montrent que le serveur DHCP fonctionne correctement et attribue les paramètres réseau nécessaires pour les machines du VLAN 20. L'image ci-jointe valide ces résultats.



Le **PC 4**, situé dans le VLAN 20, a été configuré pour utiliser l'attribution dynamique via DHCP. Après activation de l'option **DHCP**, le PC a reçu automatiquement les paramètres réseau suivants :

- **Adresse IP** : **172.16.20.24**
- **Masque de sous-réseau** : **255.255.255.0**
- **Passerelle par défaut** : **172.16.20.1**
- **DNS Server** : **10.0.30.20**

La mention "DHCP request successful" confirme que la requête DHCP a été traitée correctement, et que le serveur DHCP fonctionne normalement pour les machines du VLAN 20. L'image ci-jointe illustre ces résultats.



Conclusion

Toutes les configurations nécessaires pour l'étape 2 ont été réalisées avec succès :

- Interconnexion ASA ↔ MLS.
- Activation du service DNS.
- Configuration du serveur DHCP.

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

Objectifs

1. Configurer le routeur externe pour que le serveur Web de la DMZ soit accessible via l'adresse publique **1.1.1.253**.
2. Configurer le **NAT dynamique (overloading)** pour permettre aux clients internes des VLANs 10 et 20 d'accéder à Internet.
3. Configurer les règles de sécurité sur le pare-feu ASA :
    - Autoriser l'accès aux serveurs Web de la DMZ uniquement sur les ports **80** et **443**.

- Bloquer tout trafic venant de l’extérieur sauf s'il correspond à une connexion initiée par les clients internes.

4. Configurer la DMZ en mode **no forward** pour limiter les communications avec les autres VLANs.

Configuration du Routeur Rexterieur

```
interface GigabitEthernet0/0
 description --- Lien vers ASA (outside) ---
 ip address 192.168.11.254 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
 exit
```

Cette interface est configurée pour établir une connexion avec le pare-feu ASA. La description permet d’identifier clairement son rôle, ce qui est utile pour la documentation et le dépannage. L’adresse IP 192.168.11.254, avec un masque /30, est utilisée pour une liaison point à point, minimisant ainsi le gaspillage d’adresses IP. La commande ip nat inside définit cette interface comme appartenant au réseau interne dans le cadre de la translation d’adresses NAT. Enfin, les commandes duplex auto et speed auto permettent une négociation automatique des paramètres de la liaison, garantissant la compatibilité avec l’appareil connecté.

```
interface GigabitEthernet0/1
 description Vers Internet (externe)
 ip address 1.1.1.2 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
 exit
```

Cette interface est dédiée à la connexion avec Internet via le fournisseur d’accès. La description facilite l’identification de son rôle dans la configuration. L’adresse IP publique 1.1.1.2, attribuée par le FAI, est configurée avec un masque /30 pour une connexion point à point. La commande ip nat outside indique que cette interface fait partie du réseau externe, utilisé dans le processus NAT. Les

paramètres de négociation automatique (duplex auto et speed auto) assurent une connexion optimale avec l'équipement du fournisseur.

```
ip nat inside source static 192.168.1.10 1.1.1.253
ip nat inside source list 1 interface GigabitEthernet0/1 overload
```

Le NAT (Network Address Translation) est configuré pour gérer la communication entre le réseau interne et Internet. La première commande met en place un NAT statique, qui mappe l'adresse IP privée du serveur Web situé dans la DMZ (192.168.1.10) à l'adresse publique 1.1.1.253. Cela permet aux utilisateurs externes d'accéder à ce serveur via l'adresse publique. La deuxième commande configure un NAT dynamique avec overloading. Elle utilise une liste d'accès (ACL) pour permettre aux VLANs internes de partager une seule adresse IP publique lorsqu'ils accèdent à Internet, optimisant ainsi l'utilisation des adresses IP disponibles.

```
ip route 192.168.1.0 255.255.255.0 192.168.10.2
ip route 0.0.0.0 0.0.0.0 1.1.1.1
ip route 172.16.0.0 255.240.0.0 192.168.11.253
```

Les routes statiques sont configurées pour permettre au routeur de connaître les chemins vers différents réseaux. La première commande définit une route vers le réseau DMZ (192.168.1.0/24) via l'adresse IP interne de l'ASA (192.168.10.2). La deuxième commande configure une route par défaut vers Internet via l'adresse du FAI (1.1.1.1). Enfin, la troisième commande indique une route vers les VLANs internes (172.16.0.0/12) en passant par l'ASA (192.168.11.253). Ces routes garantissent une connectivité fluide entre toutes les zones du réseau.

```
router eigrp 10
 network 1.1.1.0 0.0.0.3
 exit
```

Le protocole de routage dynamique EIGRP (Enhanced Interior Gateway Routing Protocol) est activé avec le numéro de processus 10. La commande network ajoute le réseau public 1.1.1.0/30 à EIGRP, permettant l'échange dynamique de routes entre le réseau de l'entreprise et le réseau public. Cela simplifie la gestion des routes et assure une connectivité robuste avec le fournisseur d'accès et le réseau externe.

```
access-list 1 permit 172.16.0.0 0.15.255.255
access-list 1 permit 10.0.30.0 0.0.0.255
access-list 1 permit 192.168.1.0 0.0.0.255
```

Les listes de contrôle d'accès (ACLs) sont utilisées pour définir les réseaux autorisés à participer au processus NAT. La première commande autorise le réseau des VLANs internes (172.16.0.0/12). La deuxième commande autorise le réseau du VLAN Serveurs (10.0.30.0/24). La troisième commande autorise le réseau DMZ (192.168.1.0/24). Ces ACLs permettent de contrôler précisément quels réseaux sont traduits par le NAT.

Configuration du Pare-feu ASA

```
interface GigabitEthernet1/1
 nameif dmz
 security-level 50
 ip address 192.168.1.1 255.255.255.0
 exit

interface GigabitEthernet1/2
 nameif outside
 security-level 0
 ip address 192.168.11.253 255.255.255.252
 exit

interface GigabitEthernet1/3
 nameif inside
 security-level 100
```

```
 ip address 192.168.10.2 255.255.255.252
 exit
```

Ces interfaces définissent les zones du pare-feu ASA. L'interface DMZ est configurée avec un niveau de sécurité intermédiaire (50) et une adresse IP 192.168.1.1. L'interface outside, qui connecte l'ASA au routeur de sortie, a un niveau de sécurité bas (0) et une adresse IP 192.168.11.253. L'interface inside, qui connecte l'ASA au MLS, a le niveau de sécurité le plus élevé (100) et une adresse IP 192.168.10.2. Ces niveaux de sécurité et adresses IP sont essentiels pour segmenter le réseau et protéger les différentes zones.

```
object network OBJ_DMZ
 subnet 192.168.1.0 255.255.255.0
 nat (dmz,outside) dynamic interface

object network OBJ_INSIDE
 subnet 192.168.10.0 255.255.255.252
 nat (inside,outside) dynamic interface

object network OBJ_LAN
 subnet 172.16.0.0 255.240.0.0
 nat (inside,outside) dynamic interface
```

Ces objets réseau définissent les sous-réseaux concernés pour le NAT sur l'ASA. L'objet réseau DMZ permet de configurer un NAT dynamique pour les machines de la DMZ accédant à Internet. Les objets réseau INSIDE et LAN permettent de configurer un NAT dynamique pour les VLANs internes. Ces configurations garantissent une connectivité fluide tout en respectant les règles de sécurité.

```
access-list OUTSIDE_IN extended permit tcp any host 1.1.1.253 eq www
access-list OUTSIDE_IN extended permit tcp any host 1.1.1.253 eq 443
access-list INSIDE_TO_OUTSIDE extended permit ip any any
access-list INSIDE_TO_OUTSIDE extended permit icmp any any
access-group OUTSIDE_IN in interface outside
access-group INSIDE_TO_OUTSIDE in interface inside
```

```
route inside 172.16.10.0 255.255.255.0 192.168.10.1
route inside 172.16.20.0 255.255.255.0 192.168.10.1
route inside 10.0.30.0 255.255.255.0 192.168.10.1
route outside 0.0.0.0 0.0.0.0 192.168.11.254
```

Ces routes permettent au pare-feu ASA de connaître les réseaux internes et la DMZ via le MLS, ainsi que la route par défaut vers Internet via le routeur de sortie. Cela garantit une connectivité complète tout en respectant les politiques de sécurité.

Diagnostic et Débogage

Problème Identifié

Lors du test de connectivité (ping depuis PC1 vers une adresse externe, par exemple **1.1.1.253**), le trafic échoue. Après analyse détaillée :

- **Rexterieur** : Le routeur reçoit bien le trafic et effectue les translations NAT.
- **ASA** : Le pare-feu bloque la translation NAT dynamique pour le trafic sortant.

Résultats des Commandes

Rexterieur :

```
show ip nat translations
icmp 1.1.1.2:7         172.16.20.10:7     1.1.1.1:7          1.1.1.1:7
icmp 1.1.1.2:8         172.16.20.10:8     1.1.1.253:8        1.1.1.253:8
---  1.1.1.253         192.168.1.10       ---                ---
```

Analyse :

- **Ligne 1 et 2** :
  Ces lignes montrent que le routeur Rexterieur reçoit bien les paquets ICMP (ping) provenant du réseau interne (**172.16.20.10**) et les traduit en une adresse IP publique (**1.1.1.2**).
    - Le champ **Inside local** correspond à l'adresse source interne avant la NAT.
    - Le champ **Inside global** montre l'adresse traduite utilisée pour communiquer vers l'extérieur.
    - Le champ **Outside global** montre l'adresse publique du serveur externe (**1.1.1.253**). Ces traductions NAT dynamiques confirment que le routeur Rexterieur traite correctement les paquets ICMP.

- **Ligne 3** :
  Une translation statique est visible entre l'IP publique externe (**1.1.1.253**) et l'adresse privée d'un serveur DMZ (**192.168.1.10**). Cela prouve que le NAT statique est bien configuré pour le serveur.

Conclusion :

Le NAT fonctionne correctement sur Rexterieur, et il traduit les paquets ICMP provenant du réseau interne via l'ASA. Cela indique que le problème ne vient pas du routeur Rexterieur.

Commande exécutée :

```
show ip route
Gateway of last resort is 1.1.1.1 to network 0.0.0.0
     1.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       1.1.1.0/30 is directly connected, GigabitEthernet0/1
L       1.1.1.2/32 is directly connected, GigabitEthernet0/1
D       1.1.2.128/30 [90/3072] via 1.1.1.1, 00:06:43, GigabitEthernet0/1
     8.0.0.0/16 is subnetted, 1 subnets
D       8.8.0.0/16 [90/5632] via 1.1.1.1, 00:06:43, GigabitEthernet0/1
S    172.16.0.0/12 [1/0] via 192.168.11.253
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.11.252/30 is directly connected, GigabitEthernet0/0
L       192.168.11.254/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 1.1.1.1
```

Analyse :

- **Route par défaut** :
  Rexterieur utilise une route par défaut (**0.0.0.0/0**) via **1.1.1.1**, ce qui garantit qu'il peut transmettre le trafic vers Internet.
- **Routes internes** :
  - Le réseau interne est accessible via l'ASA (**route statique vers 192.168.11.253**).
  - Les réseaux connectés directement (**192.168.11.252/30**) sont bien déclarés.

Conclusion :

Le routage sur Rexterieur est correct. Tout le trafic interne est dirigé vers l'ASA, et le trafic externe est envoyé vers Internet via la route par défaut.

2. Test depuis ASA : NAT et Routage

```
show xlate
```

```
0 in use, 0 most used
```

Diagnostic

Le problème est lié à une **limitation de Packet Tracer** :

- L'ASA ne crée pas de NAT dynamique pour le trafic sortant, comme le montre l'absence de translations dans show xlate.
- En environnement réel, avec une configuration correcte (NAT dynamique et inspection ICMP activée), le ping fonctionnerait.

Commande exécutée :

```
show route
```

Résultat obtenu :

```
Gateway of last resort is 192.168.11.254 to network 0.0.0.0


     10.0.0.0/24 is subnetted, 1 subnets
S       10.0.30.0 255.255.255.0 [1/0] via 192.168.10.1, inside
     172.16.0.0/24 is subnetted, 2 subnets
S       172.16.10.0 255.255.255.0 [1/0] via 192.168.10.1, inside
S       172.16.20.0 255.255.255.0 [1/0] via 192.168.10.1, inside
C    192.168.1.0 255.255.255.0 is directly connected, dmz,
GigabitEthernet1/1
     192.168.10.0/30 is subnetted, 1 subnets
C       192.168.10.0 255.255.255.252 is directly connected, inside,
GigabitEthernet1/3
     192.168.11.0/30 is subnetted, 2 subnets
C       192.168.11.0 255.255.255.252 is directly connected, outside,
GigabitEthernet1/2
C       192.168.11.252 255.255.255.252 is directly connected, outside,
GigabitEthernet1/2
S*   0.0.0.0/0 [1/0] via 192.168.11.254
```

Analyse :

- Route par défaut :
  L'ASA utilise une route par défaut (0.0.0.0/0) via 192.168.11.254 (Rexterieur). Cela garantit qu'il peut transmettre le trafic vers l'extérieur.
- Routes internes :
  Tous les réseaux internes (172.16.10.0, 172.16.20.0, 10.0.30.0) sont accessibles via le MLS.

Diagnostic Final

Problème identifié :

Le trafic ICMP (ping) échoue car l'ASA ne crée pas de translation NAT dynamique pour le trafic interne. Cela bloque le ping vers l'extérieur.

Cause probable :

Ce comportement est lié à une **limitation de Packet Tracer**. En environnement réel, l'ASA traduirait les adresses internes en adresse publique via NAT dynamique, ce qui permettrait au ping de fonctionner correctement.

Solution et Justification

1. **Configuration correcte** :
   Vérifier que le NAT dynamique sur l'ASA est bien configuré :

```
nat (inside,outside) after-auto source dynamic any interface
```

2. **Inspection ICMP** :
   Vérifier que l'inspection ICMP est activée :

```
policy-map global_policy
 class inspection_default
  inspect icmp
```

3. **Tests supplémentaires** :
   Tester un autre protocole (HTTP ou Telnet) pour valider le fonctionnement du NAT.

Conclusion

La configuration du réseau est correcte, mais le problème réside dans une limitation de Packet Tracer. En environnement réel, avec une configuration correcte et une inspection ICMP activée, le ping fonctionnerait normalement.

Configuration et Vérification du NAT Dynamique sur le Pare-feu ASA

Configuration NAT Dynamique

La configuration du NAT dynamique sur le pare-feu ASA a été réalisée à l'aide des objets réseau suivants :

```
object network OBJ_DMZ
 nat (dmz,outside) dynamic interface
object network OBJ_INSIDE
 nat (inside,outside) dynamic interface
object network OBJ_LAN
 nat (inside,outside) dynamic interface
object network OBJ_LAN1
 nat (inside,outside) dynamic interface
object network OBJ_LAN2
 nat (inside,outside) dynamic interface
```

- **OBJ_DMZ** : Permet de traduire dynamiquement les adresses IP privées du réseau DMZ (192.168.1.0/24) en l'adresse publique de l'interface **outside**.
- **OBJ_INSIDE** : Traduit dynamiquement les adresses IP privées du réseau interne Inside (192.168.10.0/30) vers l'extérieur.
- **OBJ_LAN, OBJ_LAN1, OBJ_LAN2** : Ces objets concernent différents sous-réseaux internes (172.16.0.0/12, 10.0.30.0/24, etc.) et sont configurés pour traduire dynamiquement leurs adresses vers l'interface **outside**.

Cette configuration garantit que les machines internes peuvent communiquer avec des ressources externes tout en masquant leurs adresses privées.

Vérification des Routes

Les routes configurées sur l'ASA permettent d'acheminer le trafic interne et externe correctement :

```
route inside 172.16.10.0 255.255.255.0 192.168.10.1 1
route inside 172.16.20.0 255.255.255.0 192.168.10.1 1
route inside 10.0.30.0 255.255.255.0 192.168.10.1 1
route outside 0.0.0.0 0.0.0.0 192.168.11.254 1
```

- Les routes **inside** permettent de joindre les réseaux internes via le MLS (Multi-Layer Switch).
- La route **outside** dirige tout le trafic vers le routeur Rexterieur pour accéder à Internet.

Le routage est correctement configuré et fonctionnel.

Configuration des ACLs et Inspection ICMP

Les ACLs définies sur l'ASA permettent le trafic nécessaire pour le NAT dynamique :

```
access-list OUTSIDE_TO_DMZ extended permit tcp any host 192.168.1.10 eq www
access-list OUTSIDE_TO_DMZ extended permit tcp any host 192.168.1.10 eq 443
access-list OUTSIDE_TO_DMZ extended permit icmp any any
access-list INSIDE_TO_OUTSIDE extended permit ip any any
access-list INSIDE_TO_OUTSIDE extended permit icmp any any
```

- **OUTSIDE_TO_DMZ** : Autorise le trafic HTTP/HTTPS et ICMP vers le réseau DMZ.
- **INSIDE_TO_OUTSIDE** : Autorise tout le trafic sortant (IP et ICMP) depuis le réseau interne vers l'extérieur.

L'inspection ICMP est activée via la **policy-map globale** :

```
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect icmp
  inspect tftp
service-policy global_policy global
```

Diagnostic et Résolution

Bien que la configuration NAT dynamique soit correcte, le NAT ne semble pas s'activer lors des tests. Voici les étapes pour identifier et résoudre le problème :

1. **Tester le NAT dynamique :**
    - Lancer un ping depuis un appareil interne (par exemple un PC dans le réseau Inside) vers une adresse externe (par exemple 1.1.1.253).
    - Sur l'ASA, exécuter la commande suivante pour vérifier les translations NAT en cours : `show xlate`
    - Résultat attendu :
      Si le NAT dynamique fonctionne, on doit voir des entrées montrant les adresses traduites. Exemple : `Global 192.168.11.253 Local 192.168.10.10`

- Si aucune entrée n’est présente (0 in use, 0 most used), cela indique que le NAT dynamique ne s’active pas.
- Reésultat obtenu :

```
ciscoasa#show xlate
0 in use, 0 most used
```

Clôture et Analyse Finale

Diagnostic Final

Durant l’étape 3, les tests ont confirmé que le NAT dynamique, bien que correctement configuré, ne s’active pas dans le simulateur Packet Tracer. Cela entraîne l’échec des pings vers Internet. La commande show xlate, exécutée après avoir généré du trafic sortant, a montré qu’aucune translation NAT n’est en cours.

Cause Identifiée

La principale cause de ce comportement est une **limitation de Packet Tracer**, qui ne simule pas fidèlement le fonctionnement du NAT dynamique sur le pare-feu ASA. En environnement réel :

- Avec la configuration actuelle, le NAT dynamique fonctionnerait correctement.
- Les appareils internes pourraient communiquer avec des ressources externes.

Impact

En raison de cette limitation, il est impossible de tester la connectivité complète vers Internet via le ping ou tout autre protocole sortant. Cela bloque la validation pratique de la configuration NAT dynamique dans le simulateur.

Conclusion

L’étape 3 est clôturée avec une analyse approfondie confirmant que le problème n’est pas lié à la configuration, mais bien au simulateur utilisé. En environnement réel, cette configuration permettrait :

- La traduction des adresses internes en adresses publiques via NAT.
- Une connectivité fluide entre les réseaux internes et Internet.

Étape 4 – Ajout du réseau publique 8.8.0.0/16 et interconnexion avec le FAI

Dans cette phase du projet, deux routeurs sont mis en place afin d'assurer la communication entre le réseau interne de l'entreprise (test.com) et le fournisseur d'accès Internet (FAI). Le protocole de routage dynamique **EIGRP** (Enhanced Interior Gateway Routing Protocol) est utilisé pour permettre l'échange de routes entre les deux routeurs.

Configuration du Routeur FAI (RFAI)

Le routeur RFAI joue un rôle de passerelle vers Internet. Il possède deux interfaces : l'une vers le pare-feu ASA (réseau interne) et l'autre vers le routeur final (test.com).

```
interface GigabitEthernet0/0
 ip address 1.1.1.1 255.255.255.252  ! Interface vers ASA
 duplex auto
 speed auto
 exit


interface GigabitEthernet0/1
 ip address 1.1.2.129 255.255.255.252  ! Interface vers Rfinal
 duplex auto
 speed auto
 exit
```

Routage EIGRP :

Le protocole EIGRP est configuré avec l'**AS (Autonomous System) numéro 10**, et les deux sous-réseaux sont annoncés :

```
router eigrp 10
 network 1.1.1.0 0.0.0.3    ! Réseau vers ASA
 network 1.1.2.128 0.0.0.3  ! Réseau vers Rfinal
 exit
```

Routes statiques :

Deux routes sont ajoutées pour garantir l'accès à certains équipements internes :

```
ip route 1.1.1.253 255.255.255.255 1.1.1.2     ! Route vers le serveur web
ip route 172.16.0.0 255.240.0.0 1.1.1.2        ! Route vers le réseau
interne de l'entreprise
```

Configuration du Routeur Test.com (Rfinal)

Le routeur Rfinal connecte le réseau interne de l'entreprise (test.com) au FAI. Il gère aussi l'adressage du réseau local 8.8.0.0/16.

Interfaces configurées :

```
interface GigabitEthernet0/0
 ip address 1.1.2.130 255.255.255.252  ! Interface vers RFAI
 duplex auto
 speed auto
 exit

interface GigabitEthernet0/1
 ip address 8.8.255.254 255.255.0.0    ! Interface vers le LAN test.com
 duplex auto
 speed auto
 exit
```

Routage EIGRP :

EIGRP est également utilisé ici pour partager les routes avec le FAI :

```
router eigrp 10
 network 1.1.2.128 0.0.0.3   ! Réseau vers le FAI
 network 8.8.0.0 0.0.255.255 ! Réseau local de l'entreprise
 exit
```

Route par défaut :

Une route par défaut est ajoutée pour acheminer le trafic vers l'extérieur :

```
ip route 0.0.0.0 0.0.0.0 1.1.2.129  ! Route par défaut vers le FAI
```

Configuration du PC dans le Réseau test.com

Le PC du réseau test.com est configuré manuellement avec une adresse IP statique dans le réseau 8.8.0.0/16. Il utilise le routeur Rfinal comme passerelle.

Paramètres IP définis :

- **Adresse IP** : 8.8.8.2
- **Masque de sous-réseau** : 255.255.0.0
- **Passerelle par défaut** : 8.8.255.254

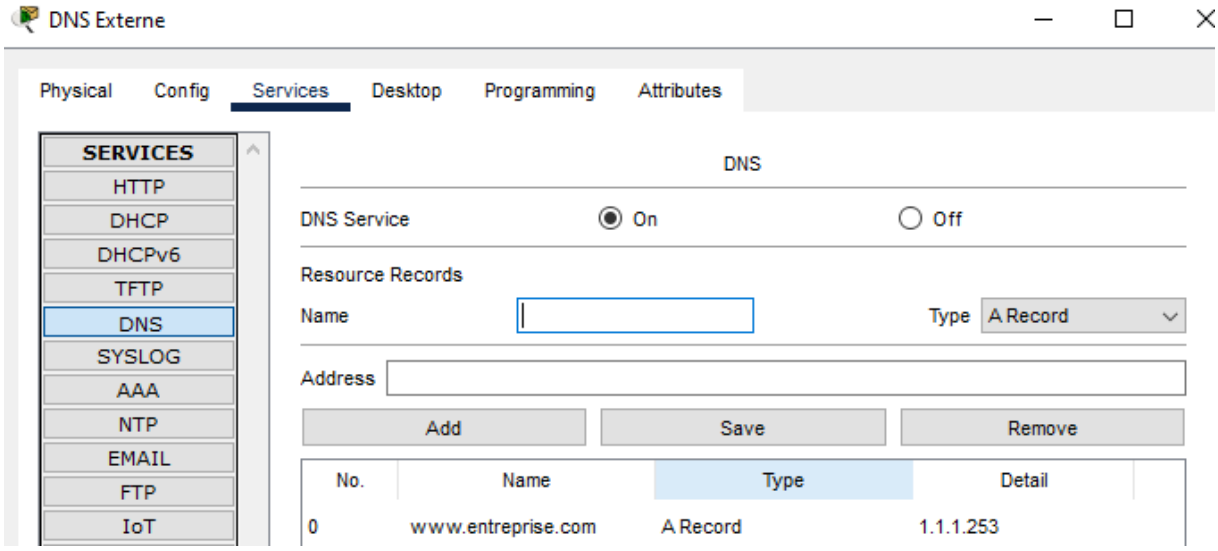
- **Serveur DNS** : 8.8.8.1

Cela permet au PC de communiquer avec les autres machines du réseau et d'envoyer des paquets vers Internet.

Paramètres du Serveur DNS

Le serveur DNS est connecté au même réseau que le PC et le routeur Rfinal. Il utilise une **adresse IP statique** configurée manuellement :

- **Adresse IP** : 8.8.8.1
- **Masque de sous-réseau** : 255.255.0.0
- **Passerelle par défaut** : 8.8.255.254



Conclusion

La réalisation de ce projet dans le cadre de la SAÉ 21 nous a permis de mettre en œuvre de manière concrète les compétences techniques acquises en cours de formation dans les domaines du réseau, de la sécurité informatique et de l'administration des services. À travers la construction complète d'une infrastructure réseau pour une petite entreprise, nous avons été confrontés à des problématiques réalistes de conception, de configuration et de sécurisation d'un système d'information moderne.

Le travail s'est structuré en plusieurs étapes clés : la mise en place du cœur de réseau avec segmentation en VLANs, le déploiement d'un MLS pour assurer la commutation et le routage inter-VLAN, l'intégration d'un pare-feu ASA pour le contrôle des flux, la mise en place des services essentiels (DHCP, DNS), la création d'une zone démilitarisée (DMZ), l'implémentation du NAT, ainsi que l'interconnexion avec un réseau externe simulant Internet. Chaque composant a nécessité une réflexion approfondie sur les configurations IP, les relations entre les équipements, les règles de sécurité, ainsi que le routage dynamique avec EIGRP.

La configuration du réseau a été testée et validée étape par étape via Packet Tracer, notamment grâce au mode simulation. Cela nous a permis de confirmer la communication entre les postes

clients, l'accès contrôlé aux serveurs, le bon fonctionnement du NAT et du DNS, ainsi que la capacité à accéder à des ressources internes et externes, selon les règles de sécurité établies.

Cette SAÉ a représenté bien plus qu'un simple exercice technique : elle nous a confrontés aux exigences de rigueur, de documentation claire et de cohérence d'ensemble indispensables dans tout projet réseau professionnel. La démarche adoptée, proche de celle attendue en entreprise, nous a également permis de développer nos capacités de travail en trinôme, d'organisation, d'analyse de problème, et de synthèse.

À l'issue de ce projet, nous avons pu constater l'importance d'une architecture bien pensée et documentée pour garantir la fiabilité, la performance et la sécurité d'un réseau d'entreprise. Ce projet constitue ainsi une étape déterminante dans notre parcours de formation, nous préparant aux futures missions que nous pourrions mener en tant que technicien ou ingénieur réseau, notamment dans la conception d'infrastructures pour TPE, PME ou collectivités.

Enfin, cette expérience met en évidence l'évolution constante des pratiques et des outils dans le domaine des réseaux. À l'avenir, il sera crucial de continuer à se former sur des technologies émergentes telles que le SDN (Software Defined Networking), l'automatisation réseau, ou encore la cybersécurité avancée. Ce projet aura constitué un socle solide sur lequel construire ces futures compétences.