

SAÉ 21- Construire un réseau info. pour petite structure



Picot Quentin
Brosse Luderic
Falcomer Mathéo

3A

Plan d'adressage IP :

Photo de l'adressage IP

Etape 1 : Construction de coeur de réseau avec les switches d'accès et le Multilayer switch

Switch bas gauche:

Switch bas droit :

MLS:

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

Service dhcp :

Service DNS:

ASA :

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

ASA:

Création de la DMZ:

ACL:

Policy-map:

FAI :

Connexion:

ACL:

Etape 4 : Ajout du réseau publique 8.8.0.0/16 et interconnexion avec le FAI

FAI:

INTERCONNEXION:

NAT:

EIGRP:

Internet:

INTERCONNEXION:

EIGRP:

Test:

INTERCONNEXION:

IP ROUTES FINALES :

MLS:

ASA:

FAI:

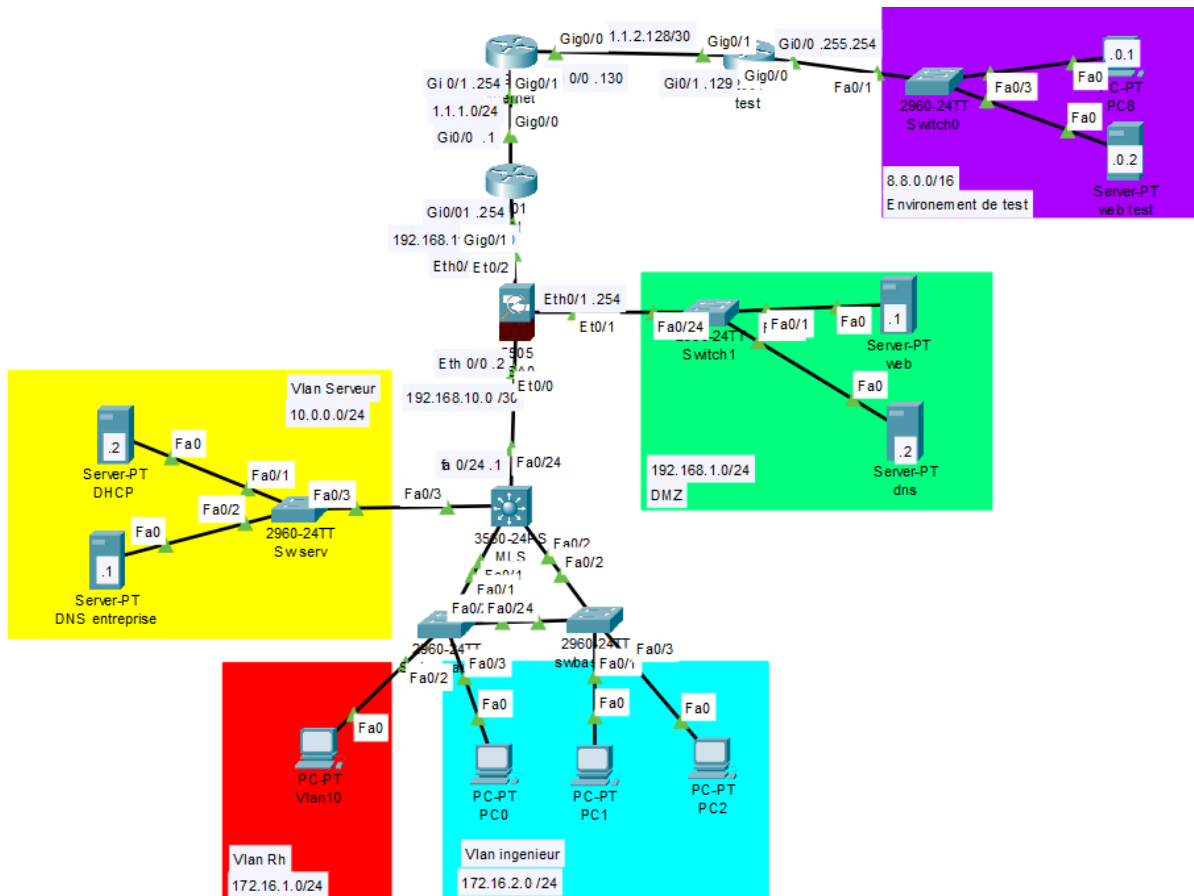
INTERNET

TEST

Mot de passe :

Screens de vérifications :

Plan d'adressage IP :



Etape 1 : Construction de coeur de réseau avec les switches d'accès et le Multilayer switch

Switch bas gauche :

- Configuration des vlan et attribution d'un nom pour une identification plus clair, ici "vlan 2" et "vlan 3" vont prendre le nom "RH" :

```
Switch(conf)#vlan 2
Switch(conf-vlan)# name Ingenieur
Switch(conf-vlan)#exit
Switch(conf)#vlan 3
Switch(conf-vlan)# name RH
Switch(conf-vlan)#exit
```

- Attribution des ports pour les vlan correspondante, ici les ports "fa 0/0" et "fa 0/24" sont affectés à la "vlan 2", le "mode access" signifie qu'il sont attribués qu'à un seul appareil et à un seul vlan. Ici, le "mode access" est choisi, contrairement au mode "trunk" puisqu'on a fait le choix d'envoyer tout le trafic de la "vlan RH" via le switch bas gauche vers le MLS. Ce choix est effectué puisqu'aucunes "collisions" sont présentes, une seule vlan est retransmis vers un équipement, le MLS.

```
Switch(conf)# int range Fa 0/0 , Fa 0/24
Switch(conf-if) switchport mode access
Switch(conf-if)#switchport access vlan 2
Switch(conf-if)#exit
```

- Même objectif que la commande ci-dessus, les interfaces "fa 0/1" et "fa 0/23" sont affectés à la "vlan 3" :

```
Switch(conf)# int range Fa 0/1 , Fa 0/23
Switch(conf-if) switchport mode access
Switch(conf-if)#switchport access vlan 3
Switch(conf-if)#exit
```

Switch bas droit :

- Configuration du "vlan 3" avec une attribution du nom "ingenieur" et une attribution des ports "fa 0/0", "fa 0/1" et "fa 0/23" à la "vlan 3" en mode access (décrit au dessus). Ici, le "mode access" est une nouvelle fois choisi mais pour orienter tout le trafic de la "vlan ingénieur" vers le MLS. Ce choix est effectué puisqu'aucunes "collisions" sont présentes, une seule vlan est retransmis vers un équipement, le MLS.

```
Switch(conf)#vlan 3
Switch(conf-vlan)# name ingenieur
Switch(conf-vlan)#exit
Switch(conf)# int range Fa 0/0-1 , Fa 0/23
Switch(conf-if) switchport mode access
Switch(conf-if)#switchport access vlan 3
Switch(conf-if)#exit
```

MLS:

- Configuration du MLS (Multi-Layer Switch) qui a pour but de relier différentes "vlan" de différentes "switch" entre elles. Cette configuration permet de modifier en quelque sorte un switch et un routeur. Ici, on active le routage avec la commande "ip routing" et on crée un lien via la ligne 2. Puis on attribue

comme précédemment des vlan aux ports choisis. De plus, on attribue des adresses ip aux ports choisis. Grâce à la commande "ip helper-address" on redirige les requêtes DHCP vers un serveur choisi.

```
MLS(conf)#ip routing
MLS(conf)#ip route 0.0.0.0 0.0.0.0 192.168.10.2
MLS(conf)#vlan 2
MLS(conf-vlan)# name RH
MLS(conf-vlan)#exit
MLS(conf)#vlan 3
MLS(conf-vlan)# name ingénieur
MLS(conf-vlan)#exit
MLS(conf)#vlan 4
MLS(conf-vlan)# name Serveur
MLS(conf-vlan)#exit
MLS(conf)#int fa 0/1
MLS(conf-if)# switchport mode acces
MLS(conf-if)#switchport access vlan 2
MLS(conf-if)#exit
MLS(conf)#int fa 0/2
MLS(conf-if)# switchport mode acces
MLS(conf-if)#switchport access vlan 3
MLS(conf-if)#exit
MLS(conf)#int fa 0/3
MLS(conf-if)# switchport mode acces
MLS(conf-if)#switchport access vlan 4
MLS(conf-if)#exit
MLS(conf)#int fa 0/24
MLS(conf-if)#no switchport
MLS(conf-if)#ip add 192.168.10.1 255.255.255.252
MLS(conf-if)#no shut
MLS(conf-if)#exit
MLS(conf)#int vlan 2
MLS(conf-vlan)#ip add 172.16.1.254 255.255.255.0
MLS(conf-vlan)#ip ip helper-address 10.0.0.2
MLS(conf-vlan)#exit
MLS(conf)#int vlan 3
MLS(conf-vlan)#ip add 172.16.2.254 255.255.255.0
MLS(conf-vlan)#ip ip helper-address 10.0.0.2
MLS(conf-vlan)#exit
MLS(conf)#int vlan 2
MLS(conf-vlan)#ip add 10.0.0.254 255.255.255.0
MLS(conf-vlan)#exit
```

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

Service dhcp :

- Il assure la distribution des adresses IP et des masques de sous réseaux aux différents services et équipements dédiés.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User
vlan 20	172.16.2.254	10.0.0.1	172.16.2.1	255.255.255.0	253
vlan 10	172.16.1.254	10.0.0.1	172.16.1.1	255.255.255.0	253
serverPool	0.0.0.0	0.0.0.0	10.0.0.0	255.255.255.0	512

Service DNS:

- Le service DNS donne un nom logique à des adresses IP.

No.	Name	Type	Detail
0	www.entreprise.com	A Record	192.168.1.1
1	www.test.com	A Record	8.8.0.2

ASA :

- La configuration de l'ASA (Adaptive Security Appliance). Elle a pour but de protéger le réseau local. L'ASA agit comme un pare-feu entre le réseau local et Internet en contrôlant le trafic entrant et sortant selon les règles qu'on lui applique. Ici, on configure la « vlan 1 » pour l'intérieur du réseau avec un niveau de sécurité de 100 (zone de confiance). Pour la « vlan 2 », on la configure pour l'extérieur (Internet) avec un niveau de 0. La logique est que le trafic est autorisé du plus sécurisé vers le moins sécurisé, mais bloqué dans l'autre sens, sauf si on autorise manuellement.

```
ASA(conf)#int vlan 1
ASA(conf-if)#name inside
ASA(conf-if)#security-level 100
ASA(conf-if)#ip address 192.168.10.2 255.255.255.252
ASA(conf-if)#exit
ASA(conf)#int eth 0/0
ASA(conf-if)#switchport mode access
ASA(conf-if)#switchport access vlan 1
```

```
ASA(conf)#int vlan 2
ASA(conf-if)#name outside
ASA(conf-if)#security-level 0
ASA(conf-if)#ip add 192.168.11.253 255.255.255.252
ASA(conf-if)#exit
ASA(conf)#int eth 0/2
ASA(conf-if)#switchport mode access
ASA(conf-if)#switchport access vlan 2
```

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

ASA:

Création de la DMZ:

- *La création de la DMZ (zone démilitarisée) sert à créer une zone isolée entre internet et le réseau interne pour plus de sécurité. Ici, on crée une zone tampon sur le « vlan 3 », avec un niveau de sécurité moyen (50), pour héberger des serveurs exposés à Internet en les isolant du réseau interne. Le “no forward” empêche les communications directes entre la DMZ et le réseau local pour éviter que les données du réseau interne ne soient accessibles via la DMZ, c’est un gage de sécurité.*

```
ASA(conf)#int vlan 3
asa(conf-if)#no forward int vlan 1 # Empêche les communications directes entre VLAN 3 (DMZ) et VLAN 1 (interne)
ASA(conf-if)#name dmz
ASA(conf-if)#security-level 50
ASA(conf-if)#ip address 192.168.1.254 255.255.255.0
ASA(conf-if)#exit
ASA(conf)#int eth 0/1
ASA(conf-if)#switchport mode access
ASA(conf-if)#switchport access vlan 3
```

ACL:

- Les ACL (access control list) servent à ajouter des règles de sécurité sur le flux réseau . Ici, l'ACL autorise certains services comme le web, le DNS et les pings depuis internet vers des serveurs internes, tout en bloquant le reste par défaut.

```
ASA(config)#access-list outside extended permit tcp any host 192.168.1.1 eq 80 # autorise HTTP (ext->dmz)
ASA(config)#access-list outside extended permit tcp any host 192.168.1.1 eq 443 # autorise HTTPS (ext -> dmz)
ASA(config)#access-list outside extended permit udp any host 192.168.1.2 eq 53 # autorise DNS (ext -> dmz)
ASA(config)#access-list outside extended permit icmp any any echo-reply # autorise les réponses aux pings
ASA(config)#access-list outside extended permit icmp any host 192.168.1.1 # autorise les ping au servweb
ASA(config)#access-list outside extended permit icmp any host 192.168.1.2 # autorise les ping au servDNS
```

```
ASA(config)#access-group outside in interface outside
```

Policy-map:

- La configuration du policy-map applique une nouvelle loi de protection des paquets lors du passage de ceux-ci dans le pare-feu. La configuration ci-dessous inspecte le trafic "HTTP" et "ICMP" lorsque l'on est dans le réseau local via la commande "policy-map global_policy". A contrario, la commande "policy-map dmz-policy" va vérifier les paquets HTTP et ICMP lorsque l'on est dans la dmz. Cela permet de recevoir les réponses attendues par les "pc" concernés (aperçu de pages web, pings...).

```
ASA(config)# class-map inspection-default
ASA(config-cmap)# match default-inspection-traffic
ASA(config-cmap)# exit
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection-default
ASA(config-pmap-c)# inspect http # regarde les fichiers http entre entreprise a dmz
ASA(config-pmap-c)# inspect icmp # regarde les fichier ICMP entre entreprise a dmz
ASA(config-pmap-c)#exit
ASA(config)# policy-map dmz-policy
ASA(config-pmap)# class inspection-default
ASA(config-pmap-c)# inspect http # regarde les fichiers http entre dmz a entreprise
ASA(config-pmap-c)# inspect icmp # regarde les fichier icmp entre dmz a entreprise
ASA(config-pmap-c)#exit
ASA(config)# service-policy global_policy interface inside # Applique la policy-map sur l'intérieur
ASA(config)# service-policy dmz-policy interface dmz # Applique la policy-map sur la dmz
```


FAI :

- Cette configuration du port "gi 0/1" est faite pour pouvoir effectuer du "NAT" ultérieurement sur le côté du réseau local. Cela a pour but de pouvoir communiquer vers l'extérieur via une autre interface.

Connexion:

```
FAI(conf)#int gi0/1
FAI(conf-if)# ip address 192.168.11.254 255.255.255.252
FAI(conf-if)#ip nat inside
FAI(conf-if)#no shut
```

- Cette configuration permet a certain réseau privés de se connecter au FAI (via les commandes "permit") et en refuse l'accès à d'autres (via les commandes "deny").

ACL:

```
FAI(config)#access-list 1 deny 10.0.0.0 0.255.255.255 # n'autorise pas les réseaux privée à sortir
FAI(config)#access-list 1 deny 172.16.0.0 0.15.255.255 # n'autorise pas les réseaux privée à sortir
FAI(config)#access-list 1 deny 192.168.0.0 0.0.255.255 # n'autorise pas les réseaux privée à sortir
FAI(config)#access-list 1 permit any any
```

```
FAI(config)#access-list 2 permit 172.16.1.0 0.0.0.255 # autorise les réseaux à être traduite
FAI(config)#access-list 2 permit 172.16.2.0 0.0.0.255 # autorise les réseaux à être traduite
```

Etape 4 : Ajout du réseau publique 8.8.0.0/16 et interconnexion avec le FAI

FAI:

- Cette configuration du port "gi 0/0" est faite pour pouvoir effectuer du "NAT" sur le côté du réseau public. Cela a pour but de pouvoir communiquer vers l'extérieur via une adresse public et elle obéit aux règles des "ACL" 1 créés précédemment.

INTERCONNEXION:

```
FAI(conf)#int gi0/0
FAI(conf-if)# ip address 1.1.1.1 255.255.255.0
FAI(conf-if)#ip access-group 1 out
FAI(conf-if)#ip nat outside
```

- Le NAT (Network Address Translation) sert à transformer des adresses privées en adresses publiques pour communiquer sur Internet en protégeant et en cachant le réseau interne. Ici, la configuration crée

un groupe d'adresses publiques que les machines du réseau privé peuvent utiliser pour sortir sur Internet. Elle dit aussi que deux adresses privées spécifiques auront toujours la même adresse publique, pour qu'on puisse les retrouver facilement depuis l'extérieur.

Le NAT permet la conversion des adresses privées en adresses publiques pour accéder à Internet.

- *Le pool ent avec l'adresse 1.1.1.2 est utilisé pour faire du NAT dynamique (avec surcharge, grâce à overload) pour les réseaux 172.16.1.0 et 172.16.2.0.*
- *Le NAT statique associe les IP internes 192.168.1.1 et 192.168.1.2 à des IP publiques fixes (1.1.1.253 et 1.1.1.252) pour qu'elles soient joignables de l'extérieur. Cela permet par exemple d'héberger un site web ou serveur DNS dans la DMZ.*

NAT:

```
FAI(conf)#ip nat pool ent 1.1.1.2 1.1.1.2 netmask 255.255.255.0
```

```
FAI(conf)#ip nat inside source list 2 pool ent overload
```

```
FAI(conf)#ip nat inside source static 192.168.1.1 1.1.1.253
```

```
FAI(conf)#ip nat inside source static 192.168.1.2 1.1.1.252
```

- *EIGRP est un protocole qui permet une optimisation du trafic. Grâce à lui, les routeurs peuvent échanger leurs informations de route pour une efficacité optimale. Ici, la configuration indique au routeur que le réseau "1.1.1.0 0.0.0.255" doit être surveillé pour partager leurs routes avec les autres routeurs EIGRP.*

EIGRP:

```
FAI(config)#router eigrp 1
```

```
FAI(config-router)#network 1.1.1.0 0.0.0.255
```

```
FAI(config-router)#passive-interface GigabitEthernet0/1
```

Internet:

- *C'est une configuration classique des ports "gi 0/0" et "gi 0/1" ou l'on affecte une adresse IP et un masque.*

INTERCONNEXION:

```
Internet(conf)#int gi0/0
```

```
Internet(conf-if)# ip address 1.1.2.130 255.255.255.252
```

```
Internet(conf-if)#no shut
```

```
Internet(conf)#int gi 0/1
```

```
Internet(conf-if)# ip address 1.1.1.254 255.255.255.0
```

```
Internet(conf-if)#no shut
```

- *C'est plus ou moins la même configuration EIGRP que celle effectuée précédemment mais elle permet également de récupérer les routes statiques présentes sur les routeurs.*

EIGRP:

```
Internet(config)#router eigrp 1
```

```
Internet(config-router)#redistribute static
```

```
Internet(config-router)#network 1.1.1.0 0.0.0.255
```

```
Internet(config-router)#network 1.1.2.128 0.0.0.3
```

```
Internet(config-router)# passive-interface GigabitEthernet0/0
```

Test:

- *C'est une configuration classique des ports "gi 0/0" et "gi 0/1" ou l'on affecte une adresse IP et un masque.*

INTERCONNEXION:

```
test(conf)#int Gi 0/0
```

```
test(conf-if)#ip address 8.8.255.254 255.255.0.0
```

```
test(conf-if)#no shut
```

```
test(conf)#int Gi 0/1
```

```
test(conf-if)#ip address 1.1.2.129 255.255.255.252
```

```
test(conf-if)#no shut
```

IP ROUTES FINALES :

- *Création des différentes routes pour faire la liaison entre les différents éléments du réseau packet tracer. Il y a des routes par défaut (exemple : "ip route 0.0.0.0 0.0.0.0 1.1.2.130) et des routes statiques (exemple : "ip route 172.16.1.0 255.255.255.0 192.168.11.253) pour assurer la bonne communication.*

MLS:

```
MLS(conf)#ip route 0.0.0.0 0.0.0.0 192.168.10.2
```

-

ASA:

```
ASA(conf)#route outside 0.0.0.0 0.0.0.0 192.168.11.254 1
ASA(conf)#route inside 172.16.1.0 255.255.255.0 192.168.10.1 1
ASA(conf)#route inside 172.16.2.0 255.255.255.0 192.168.10.1 1
```

FAI:

```
FAI(conf)#ip route 172.16.1.0 255.255.255.0 192.168.11.253
FAI(conf)#ip route 172.16.2.0 255.255.255.0 192.168.11.253
FAI(conf)#ip route 192.168.1.0 255.255.255.0 192.168.11.253
```

INTERNET

```
Internet(conf)#ip route 8.8.0.0 255.255.0.0 1.1.2.129
```

TEST

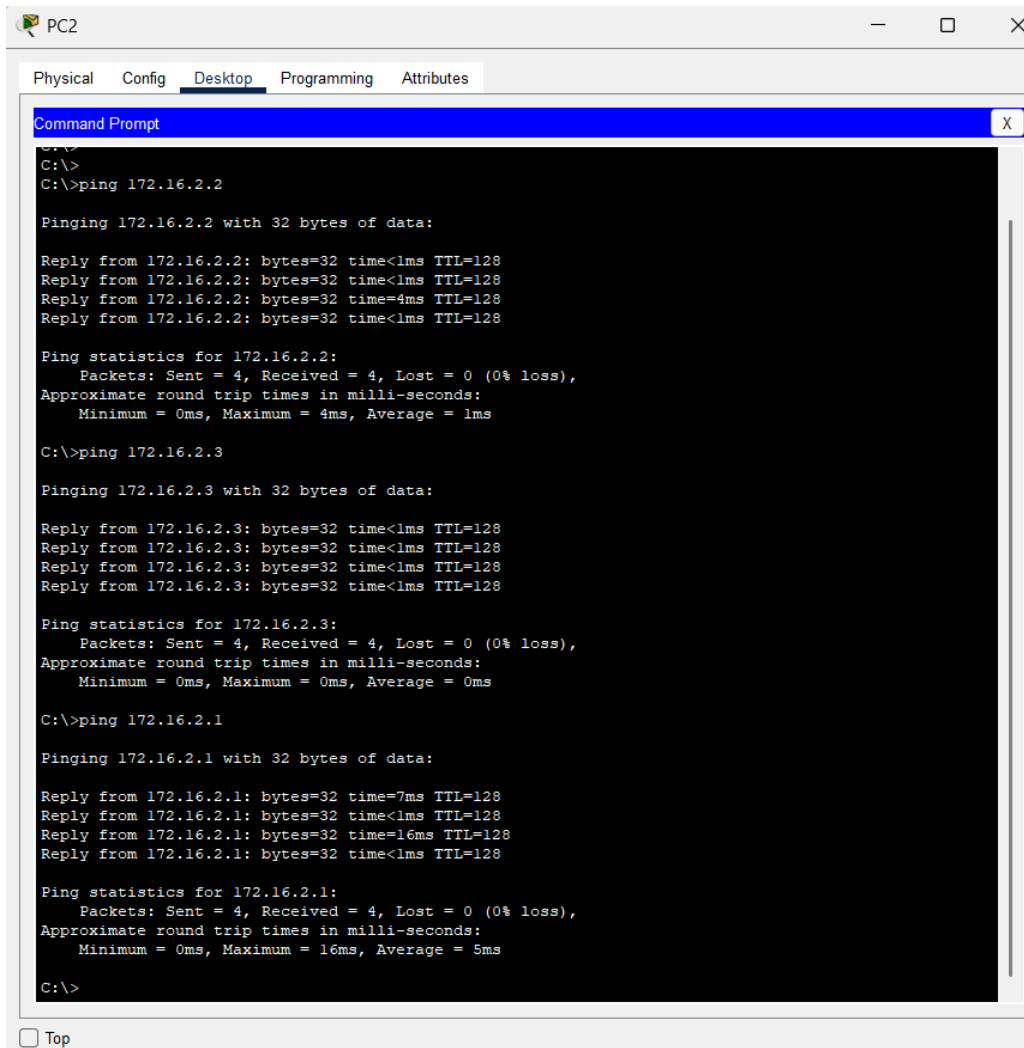
```
Test(conf)#ip route 0.0.0.0 0.0.0.0 1.1.2.130
```

Mot de passe :

mot de passe pour l'ASA : "appuyez sur la touche enter de votre clavier, aucun mot de passe demandé"

Screens de vérifications :

- pings entre machines de même vlan (pc de test : 172.16.2.1 sur les autres pc de la vlan3) ;



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 172.16.2.2

Pinging 172.16.2.2 with 32 bytes of data:

Reply from 172.16.2.2: bytes=32 time<1ms TTL=128
Reply from 172.16.2.2: bytes=32 time<1ms TTL=128
Reply from 172.16.2.2: bytes=32 time=4ms TTL=128
Reply from 172.16.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ping 172.16.2.3

Pinging 172.16.2.3 with 32 bytes of data:

Reply from 172.16.2.3: bytes=32 time<1ms TTL=128
Reply from 172.16.2.3: bytes=32 time<1ms TTL=128
Reply from 172.16.2.3: bytes=32 time<1ms TTL=128
Reply from 172.16.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.16.2.1

Pinging 172.16.2.1 with 32 bytes of data:

Reply from 172.16.2.1: bytes=32 time=7ms TTL=128
Reply from 172.16.2.1: bytes=32 time<1ms TTL=128
Reply from 172.16.2.1: bytes=32 time=16ms TTL=128
Reply from 172.16.2.1: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 16ms, Average = 5ms

C:\>
```

- pings entre machines de vlan différentes (pc de test : 172.16.2.2 sur vlan3 vers vlan2 du pc 172.16.1.1) ;

```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Request timed out.
Reply from 172.16.1.1: bytes=32 time=1ms TTL=127
Reply from 172.16.1.1: bytes=32 time=6ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 2ms

C:\>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|
```

- Ping de bonne interconnexion physique et logique entre l'ASA et le MLS. Le fait que l'interface du MLS réponde montre qu'elle est bien configurée en mode L3 (non switchport + IP address).

```
-----
ASA#ping 192.168.10.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/6/13 ms
```

```
ASA#ping 192.168.10.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/14 ms
```

```
ASA#|
```

- Cette commande teste la résolution DNS interne (le PC demande l'IP de www.test.com au serveur DNS local) et la connectivité NAT sortante vers Internet via l'ASA.

```
C:\>ping www.test.com

Pinging 8.8.0.2 with 32 bytes of data:

Reply from 8.8.0.2: bytes=32 time=1ms TTL=123
Reply from 8.8.0.2: bytes=32 time=2ms TTL=123
Reply from 8.8.0.2: bytes=32 time=2ms TTL=123
Reply from 8.8.0.2: bytes=32 time=1ms TTL=123

Ping statistics for 8.8.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

- Ce ping valide que le nom de domaine interne pointe vers l'IP du serveur DMZ et que le pare-feu ASA laisse passer le trafic depuis l'interne vers la DMZ.

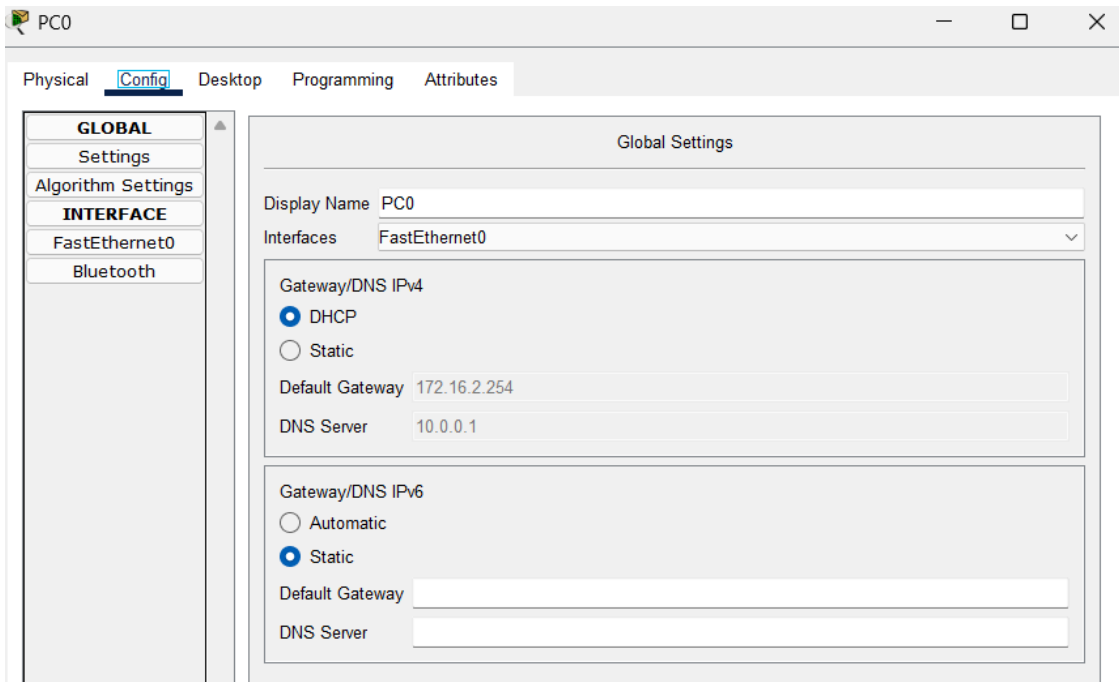
```
C:\>ping www.entreprise.com

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.1: bytes=32 time=1ms TTL=126
Reply from 192.168.1.1: bytes=32 time<1ms TTL=126
Reply from 192.168.1.1: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- L'IP est bien obtenue en DHCP.



- Ce ping traverse l'ASA, arrive au routeur FAI, qui fait du NAT dynamique. Si la réponse revient, cela prouve que la traduction dynamique fonctionne, avec une seule IP publique partagée.

```
C:\>ping 8.8.0.1

Pinging 8.8.0.1 with 32 bytes of data:

Reply from 8.8.0.1: bytes=32 time=7ms TTL=123
Reply from 8.8.0.1: bytes=32 time=28ms TTL=123
Reply from 8.8.0.1: bytes=32 time=2ms TTL=123
Reply from 8.8.0.1: bytes=32 time<1ms TTL=123

Ping statistics for 8.8.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 28ms, Average = 9ms
```

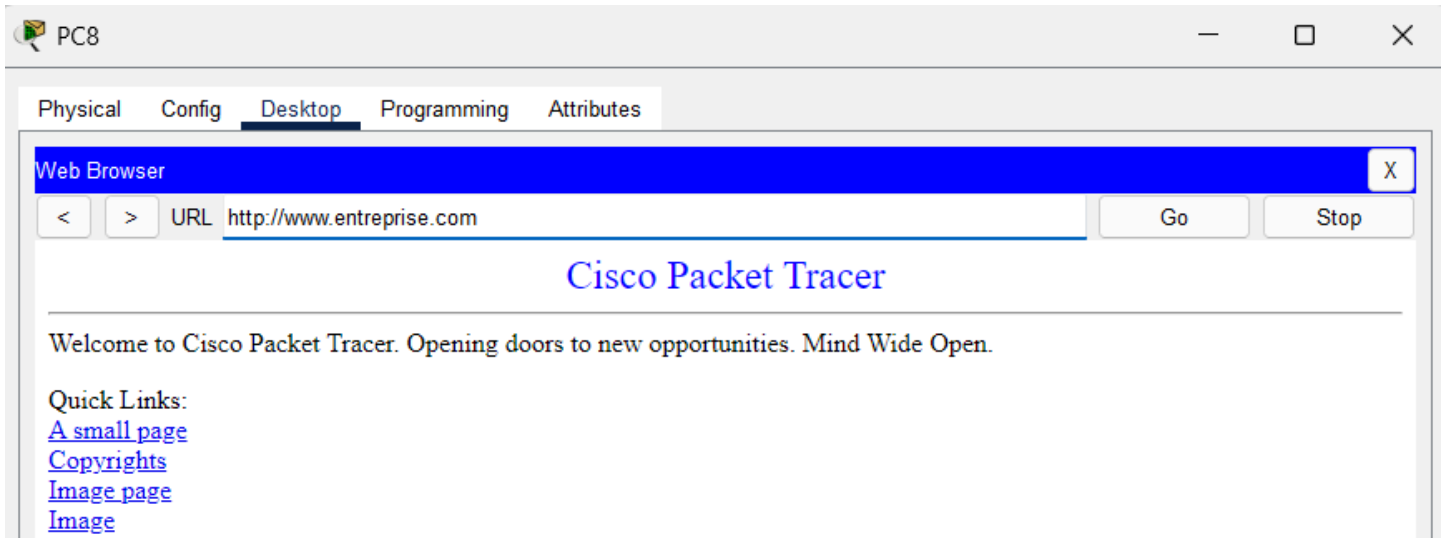
- Le ping est bloqué par le pare-feu ASA (protocole ICMP désactivé). HTTP/HTTPS sont autorisés, donc le serveur web reste accessible.


```
C:\>ping www.entreprise.com

Pinging 1.1.1.253 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 1.1.1.253:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



- Le port 80 (HTTP) doit être autorisé, tandis que le port 21 (FTP) doit être bloqué. Cela vérifie que les règles du pare-feu sont restrictives et précises.

```
C:\>telnet 1.1.1.253 80
Trying 1.1.1.253 ...Open

[Connection to 1.1.1.253 closed by foreign host]
C:\>telnet 1.1.1.253 21
Trying 1.1.1.253 ...
% Connection timed out; remote host not responding
```