Evan BROCCA

COMPTE-RENDU SAE 201

Concevoir le réseau informatique d'une petite entreprise

13/06/2026

SOMMAIRE

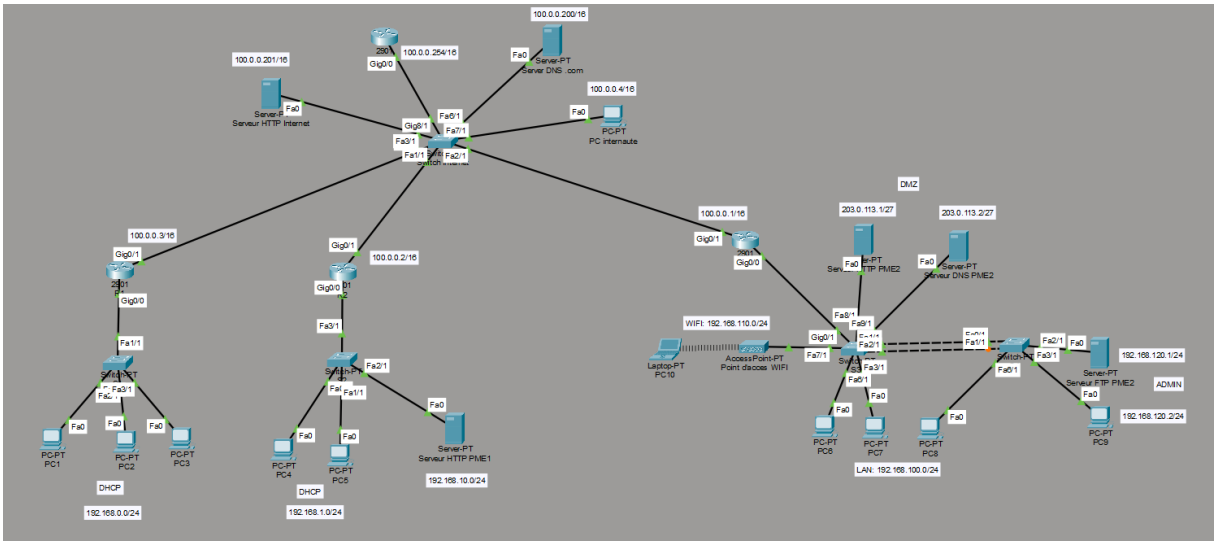
INTRODUCTION :

Ce document est le compte-rendu technique de la SAE 201. Il décrit la conception et la mise en œuvre d'un réseau d'entreprise simulé sur Cisco Packet Tracer, composé d'un TPE, de deux PME et d'une zone Internet. Pour chaque réseau, nous détaillerons les configurations des équipements, justifierons les choix techniques effectués et présenterons les tests de vérification réalisés pour valider le cahier des charges.

Résumé :

1) Structure et fonctionnement :

Le réseau est composé de quatre entités interconnectées via une zone Internet : un TPE avec un LAN simple, une PME1 avec un LAN et une DMZ, une PME2 avec quatre VLANs (LAN, WIFI, ADMIN, DMZ) et une zone Internet centrale. Chaque zone dispose d'un routeur assurant le NAT/PAT et le routage vers Internet via OSPF. Les entreprises communiquent entre elles à travers le routeur Internet qui centralise les échanges et redistribue les routes.



2) Configurations des équipements :

Le routeur R1 dispose d'un pool DHCP pour le réseau 192.168.0.0/24 avec la passerelle 192.168.0.254 et le DNS Internet 100.0.0.200. L'interface Gig0/0 est configurée en inside NAT avec l'adresse 192.168.0.254, et l'interface Gig0/1 en outside NAT avec l'adresse publique 100.0.0.3/16 et l'IPv6 2001:100::3/32. L'ACL 1 autorise le NAT pour le réseau 192.168.0.0/24, et une route par défaut pointe vers 100.0.0.254. OSPF est activé sur le réseau 100.0.0.0/16.

```
R1>enable
R1#sh run
Building configuration...

Current configuration : 1065 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
!
!
ip dhcp pool LAN1
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.254
 dns-server 100.0.0.200
!
!
!
ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
!
license udi pid CISCO2901/K9 sn FTX1524N9BG-
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 192.168.0.254 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 100.0.0.3 255.255.0.0
 ip nat outside
 duplex auto
 speed auto
 ipv6 address 2001:100::3/32
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes
 network 100.0.0.0 0.0.255.255 area 0
!
ip nat inside source list 1 interface GigabitEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 100.0.0.254
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.0.0 0.0.0.255
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

Le routeur R2 dispose d'un pool DHCP pour le réseau 192.168.1.0/24. Il utilise deux sous-interfaces : Gig0/0.1 pour le LAN (192.168.1.254/24, IPv6 2001:1234:ABCD:1::1/64) et Gig0/0.2 pour la DMZ (192.168.10.254/24, IPv6 2001:1234:ABCD:10::1/64). L'interface Gig0/1 est l'interface publique (100.0.0.2/16, IPv6 2001:100::2/32). Le NAT est activé pour les réseaux 192.168.1.0/24 et 192.168.10.0/24, avec une redirection de port TCP 80 vers le serveur HTTP (192.168.10.1). OSPF pour l'IPv4 et l'IPv6 sont configurés sur le réseau 100.0.0.0/16.

```
R2>enable
R2#sh run
Building configuration...

Current configuration : 1578 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
!
!
!
!
ip dhcp pool LAN1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.254
 dns-server 100.0.0.200
!
!
!
ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
!
license udi pid CISCO2901/K9 sn FTX152404NQ-
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
```

```
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 192.168.1.254 255.255.255.0
 ip nat inside
 ipv6 address 2001:1234:ABCD:1::1/64
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.10.254 255.255.255.0
 ip nat inside
 ipv6 address 2001:1234:ABCD:10::1/64
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1
 ip address 100.0.0.2 255.255.0.0
 ip nat outside
 duplex auto
 speed auto
 ipv6 address 2001:100::2/32
 ipv6 ospf 1 area 0
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 network 100.0.0.0 0.0.255.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
!
ipv6 router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
!
ip nat inside source list 1 interface GigabitEthernet0/1 overload
ip nat inside source static tcp 192.168.10.1 80 100.0.0.2 80
ip classless
ip route 0.0.0.0 0.0.0.0 100.0.0.254
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.10.0 0.0.0.255
!
```

```
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

Le routeur R3 dispose de deux pools DHCP : LAN (192.168.100.0/24, passerelle 192.168.100.254, DNS 203.0.113.2) et WIFI (192.168.110.0/24, passerelle 192.168.110.254). Il possède quatre sous-interfaces : Gig0/0.10 pour le LAN (192.168.100.254), Gig0/0.20 pour le WIFI (192.168.110.254), Gig0/0.30 pour l'ADMIN (192.168.120.254) avec l'ACL 100 en sortie, et Gig0/0.40 pour la DMZ (203.0.113.30/27). L'interface Gig0/1 est l'interface publique (100.0.0.1/16). Le NAT est activé via l'ACL 99, avec des redirections de port pour HTTP (203.0.113.1:80) et DNS (203.0.113.2:53). Les ACL 100 et 101 assurent le filtrage. SSH est configuré sur les lignes VTY avec l'ACL 10. OSPF est activé sur le réseau 100.0.0.0/16 et la DMZ 203.0.113.0/27.

```
R3>enable
R3#sh run
Building configuration...

Current configuration : 2721 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R3
!
!
!
!
ip dhcp excluded-address 192.168.100.254
ip dhcp excluded-address 192.168.110.254
!
ip dhcp pool LAN
 network 192.168.100.0 255.255.255.0
 default-router 192.168.100.254
 dns-server 203.0.113.2
ip dhcp pool WIFI
 network 192.168.110.0 255.255.255.0
 default-router 192.168.110.254
 dns-server 203.0.113.2
!
!
!
ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
username admin privilege 15 secret 5 $1$mERr$AFX/pZT1Lh
!
!
license udi pid CISCO2901/K9 sn FTX15240ZTJ-
!
!
ip ftp username admin
ip ftp password cisco123
ip domain-name pme_2
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.100.254 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.110.254 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.120.254 255.255.255.0
 ip nat inside
 ip access-group 100 out
!
interface GigabitEthernet0/0.40
 encapsulation dot1Q 40
 ip address 203.0.113.30 255.255.255.224
 ip nat inside
!
interface GigabitEthernet0/1
 ip address 100.0.0.1 255.255.0.0
 ip nat outside
 ip access-group 101 in
 duplex auto
 speed auto
 ipv6 address 2001:100::1/32
 ipv6 ospf 1 area 0
!
interface Vlan1
 no ip address
 shutdown
```

```
.
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 100.0.0.0 0.0.255.255 area 0
!
ipv6 router ospf 1
 log-adjacency-changes
!
ip nat inside source list 99 interface GigabitEthernet0/1 overload
ip nat inside source static udp 203.0.113.2 53 100.0.0.1 53
ip nat inside source static tcp 203.0.113.2 53 100.0.0.1 53
ip nat inside source static tcp 203.0.113.1 80 100.0.0.1 80
ip classless
ip route 0.0.0.0 0.0.0.0 100.0.0.254
!
ip flow-export version 9
!
!
access-list 101 permit tcp any host 203.0.113.1 eq www
access-list 101 permit udp any host 203.0.113.2 eq domain
access-list 101 deny ip any 192.168.100.0 0.0.0.255
access-list 101 deny ip any 192.168.110.0 0.0.0.255
access-list 101 deny ip any 192.168.120.0 0.0.0.255
access-list 101 permit ip any any
access-list 100 deny ip 192.168.100.0 0.0.0.255 192.168.120.0 0.0.0.255
access-list 100 deny ip 192.168.110.0 0.0.0.255 192.168.120.0 0.0.0.255
access-list 100 deny ip 203.0.113.0 0.0.0.31 192.168.120.0 0.0.0.255
access-list 100 deny ip any 192.168.120.0 0.0.0.255
access-list 100 permit ip any any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 access-class 10 in
 login local
 transport input ssh
!
!
!
end
```

Le routeur R4 est le routeur central de la zone Internet. Son interface Gig0/0 est configurée avec l'adresse 100.0.0.254/16 et l'IPv6 2001:100::254/32. OSPF est activé sur le réseau 100.0.0.0/16 avec le router-id 1.1.1.1, et OSPFv3 est également activé pour l'IPv6.

```
R4>enable
R4#sh run
Building configuration...

Current configuration : 833 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R4
!
!
!
!
!
!
!
!
ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
!
license udi pid CISCO2901/K9 sn FTX15246K4M-
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
.
interface GigabitEthernet0/0
 ip address 100.0.0.254 255.255.0.0
 duplex auto
 speed auto
 ipv6 address 2001:100::254/32
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 100.0.0.0 0.0.255.255 area 0
!
ipv6 router ospf 1
 log-adjacency-changes
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

Le switch S3 dispose des quatre VLANs (10, 20, 30, 40). L'interface Gig0/1 est en trunk vers le routeur, les interfaces Fa1/1 et Fa2/1 sont en trunk vers S4 pour la redondance. Les ports d'accès sont affectés à leurs VLANs respectifs : Fa3/1 et Fa6/1 en VLAN 10 (LAN), Fa7/1 en VLAN 20 (WIFI), Fa8/1 et Fa9/1 en VLAN 40 (DMZ). Une interface VLAN 30 avec l'adresse 192.168.120.3/24 permet l'administration à distance. SSH est restreint au réseau ADMIN via l'ACL 10.

```
S3#sh run
Building configuration...

Current configuration : 1405 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S3
!
ip ftp username admin
ip ftp password cisco123
!
!
!
ptp clock transparent domain 0 profile default
!
username admin secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 10,20,30,40
 switchport mode trunk
!
interface FastEthernet1/1
 switchport trunk allowed vlan 10,20,30,40
 switchport mode trunk
!
interface FastEthernet2/1
 switchport trunk allowed vlan 10,20,30,40
 switchport mode trunk
!
interface FastEthernet3/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet4/1
!
interface FastEthernet5/1
!
interface FastEthernet6/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet7/1
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet8/1
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet9/1
 switchport access vlan 40
 switchport mode access
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan30
 ip address 192.168.120.3 255.255.255.0
!
ip default-gateway 192.168.120.254
!
!
!
!
access-list 10 permit 192.168.120.0 0.0.0.255
line con 0
!
line vty 0 4
 access-class 10 in
 login local
 transport input ssh
line vty 5 15
 login
!
!
!
!
end
```

Le switch S4 dispose également des quatre VLANs. Les interfaces Fa0/1 et Fa1/1 sont en trunk vers S3. Les ports Fa2/1 et Fa3/1 sont en VLAN 30 (ADMIN), Fa6/1 en VLAN 10 (LAN). Une interface VLAN 30 avec l'adresse 192.168.120.4/24 permet l'administration à distance. SSH est également restreint au réseau ADMIN.

```
S4#sh run
Building configuration...

Current configuration : 1104 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S4
!
ip ftp username admin
ip ftp password cisco123
!
!
!
ptp clock transparent domain 0 profile default
!
username admin secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk allowed vlan 10,20,30,40
 switchport mode trunk
!
interface FastEthernet1/1
 switchport trunk allowed vlan 10,20,30,40
 switchport mode trunk
!
interface FastEthernet2/1
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet3/1
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet4/1
!
interface FastEthernet5/1
!
interface FastEthernet6/1
 switchport access vlan 10
 switchport mode access
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan30
 ip address 192.168.120.4 255.255.255.0
!
ip default-gateway 192.168.120.254
!
!
!
!
line con 0
!
line vty 0 4
 access-class 10 in
 login local
 transport input ssh
line vty 5 15
 login
!
!
!
!
end
```

3) Justification des choix :

Nous avons choisi d'utiliser des adresses IPv4 privées pour les réseaux internes car elles ne sont pas routables sur Internet. Pour la DMZ de PME2, nous avons opté pour des adresses publiques afin que les serveurs soient directement accessibles depuis Internet. Pareil pour la DMZ de PME1, où cette fois ce sont des adresses publiques en IPv6. Le masque /27 est suffisant pour nos besoins.

Nous avons activé le DHCP uniquement sur les VLANs LAN et WIFI car les utilisateurs de ces zones n'ont pas besoin d'une adresse fixe. En revanche, les serveurs de la DMZ et de l'ADMIN disposent d'adresses statiques car si leur adresse venait à changer, les services deviendraient inaccessibles et les règles NAT et DNS ne fonctionneraient plus correctement.

Nous avons segmenté le réseau en quatre VLANs (LAN, WIFI, ADMIN, DMZ) afin d'isoler les différentes zones entre elles. Ainsi, un équipement du LAN ne peut pas communiquer directement avec un équipement de la DMZ sans passer par le routeur, ce qui nous permet de contrôler précisément les échanges grâce aux ACL.

Nous avons mis en place le NAT pour permettre à tous les équipements internes de partager une seule adresse IP publique pour accéder à Internet. Nous avons également configuré des redirections de ports pour que les serveurs HTTP et DNS de la DMZ restent accessibles depuis Internet via l'IP publique du routeur.

Nous avons choisi OSPF comme protocole de routage dynamique car il permet aux routeurs d'apprendre automatiquement les routes des autres entreprises. Cela évite de devoir configurer manuellement des routes statiques entre chaque entreprise ce qui permet d’éviter les erreurs.

Nous avons mis en place des ACL pour séparer les différentes zones du réseau. Le réseau ADMIN est rendu inaccessible depuis le LAN, le WIFI, la DMZ et Internet car il contient des équipements sensibles comme le PC ADMIN et le serveur FTP. Concernant la DMZ, nous n'autorisons que le trafic HTTP et DNS depuis Internet car ce sont les seuls services destinés à être publics, tout autre accès est bloqué pour limiter les risques d'intrusion.

Nous avons choisi SSH plutôt que Telnet pour administrer les équipements réseau car il chiffre les communications, ce qui empêche l'interception des mots de passe. Nous avons également restreint l'accès SSH au seul réseau ADMIN via une ACL, afin qu'aucun utilisateur extérieur ne puisse tenter de se connecter aux équipements.

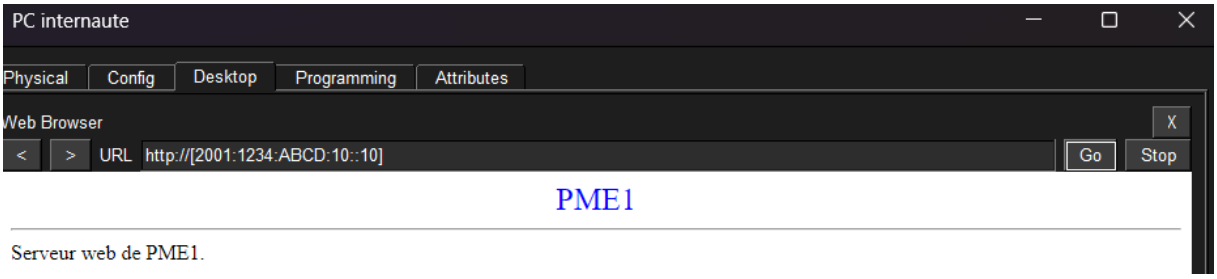
Nous avons configuré un serveur FTP dans le réseau ADMIN pour centraliser les sauvegardes des configurations du routeur et des switches. En cas de panne ou de mauvaise manipulation, cela permet de restaurer rapidement une configuration

fonctionnelle. L'accès au serveur FTP est limité au réseau ADMIN pour éviter qu'un utilisateur non autorisé ne puisse récupérer ou modifier ces fichiers.

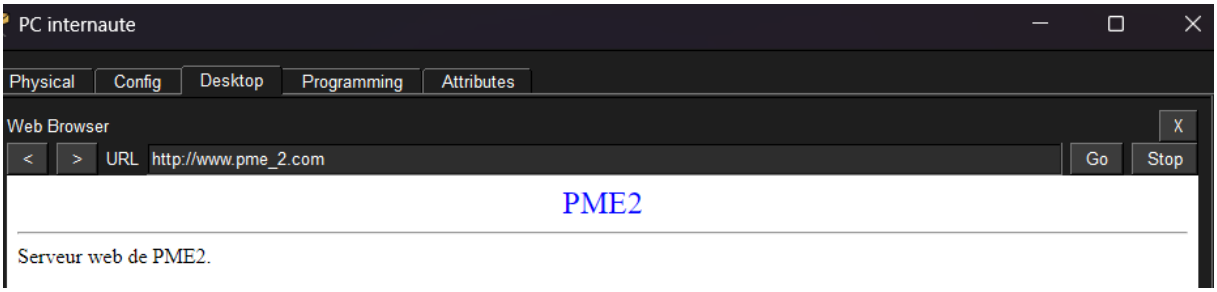
4) Tests :

Tests inter-entreprises et vers Internet :

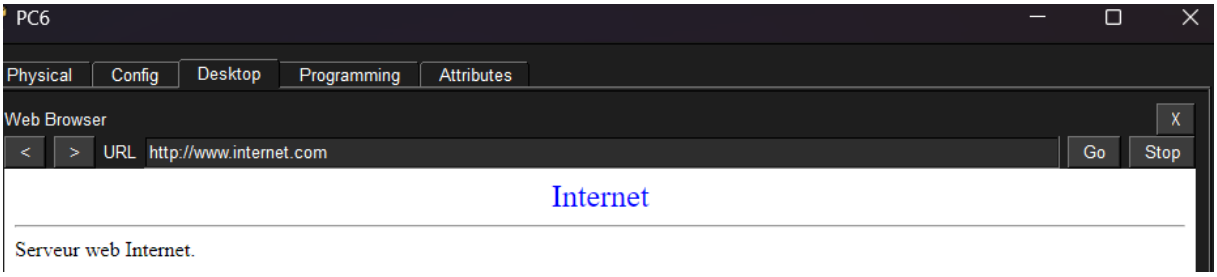
Depuis le PC internaute, nous accédons au serveur HTTP de la DMZ de PME1 via l'adresse publique 100.0.0.2. La page web s'affiche correctement, confirmant que la redirection de port fonctionne bien sur le routeur de PME1.



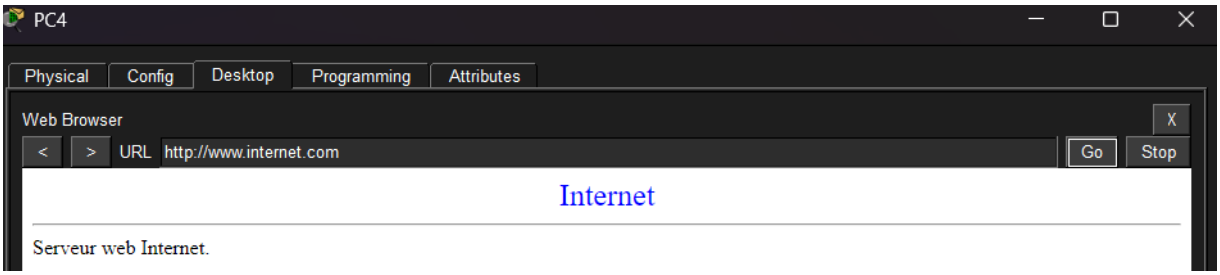
Depuis le PC internaute, nous accédons au serveur HTTP de la DMZ de PME2 via l'adresse publique 100.0.0.1. La page web s'affiche correctement, confirmant que le NAT et la redirection de port fonctionnent bien sur le routeur R3 de PME2.



Depuis un PC du LAN de PME2, nous vérifions l'accès au serveur HTTP Internet (www.internet.com). La résolution DNS et l'accès HTTP fonctionnent correctement, confirmant que le NAT et le routage vers Internet sont opérationnels.

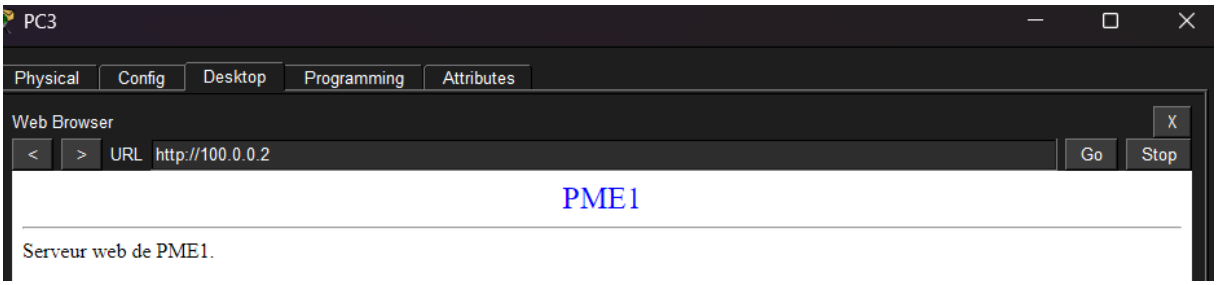


Depuis un PC du LAN de PME1, nous effectuons le même test vers Internet. La connectivité est établie, confirmant que PME1 dispose également d'un accès Internet fonctionnel.

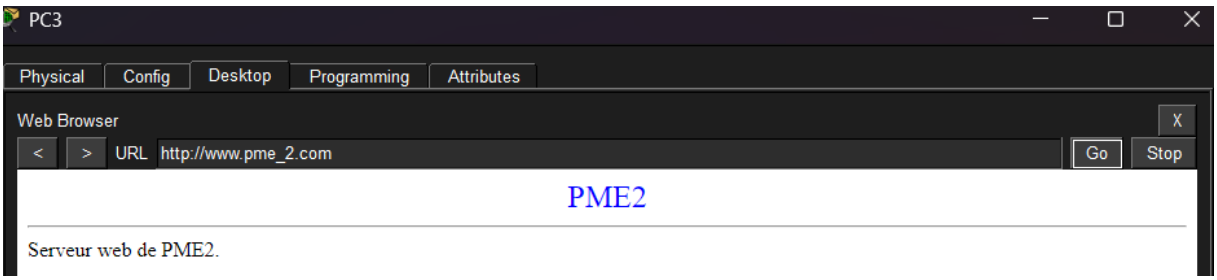


Depuis un PC du TPE, nous vérifions l'accès à Internet. La connectivité est confirmée, le routeur TPE achemine correctement le trafic vers le routeur Internet via la route par défaut.

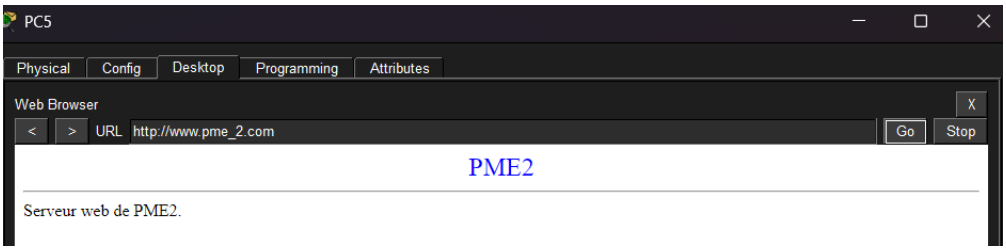
Depuis un PC du TPE, nous accédons au serveur HTTP de PME1. La page web de PME1 s'affiche, confirmant que la communication inter-entreprises via le routeur Internet fonctionne correctement.



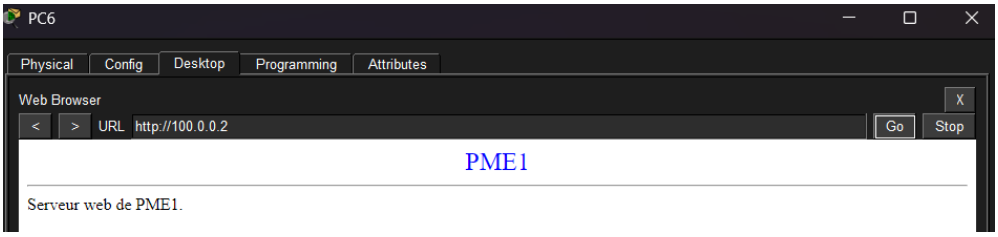
Depuis un PC du TPE, nous accédons au serveur HTTP de PME2. La page web de PME2 s'affiche, confirmant que la communication inter-entreprises via le routeur Internet fonctionne correctement.



Depuis un PC du LAN de PME1, nous accédons au serveur HTTP de PME2. La page web de PME2 s'affiche, ce qui valide le routage entre les deux PME via la zone Internet.



Depuis un PC du LAN de PME2, nous accédons au serveur HTTP de PME1. La page web de PME1 s'affiche correctement, confirmant la communication entre les entreprises.

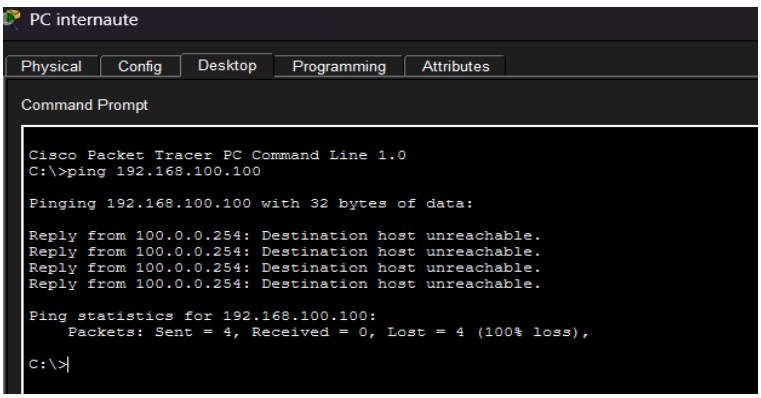


Tests de sécurité (ACL) :

Depuis un PC du LAN de PME2, nous tentons d'accéder au réseau ADMIN (192.168.120.x). La requête est bloquée par l'ACL 100, confirmant que le LAN, le WIFI et la DMZ ne peuvent pas atteindre le réseau d'administration. L'ACL permet d'observer la même chose pour le WIFI et la DMZ.

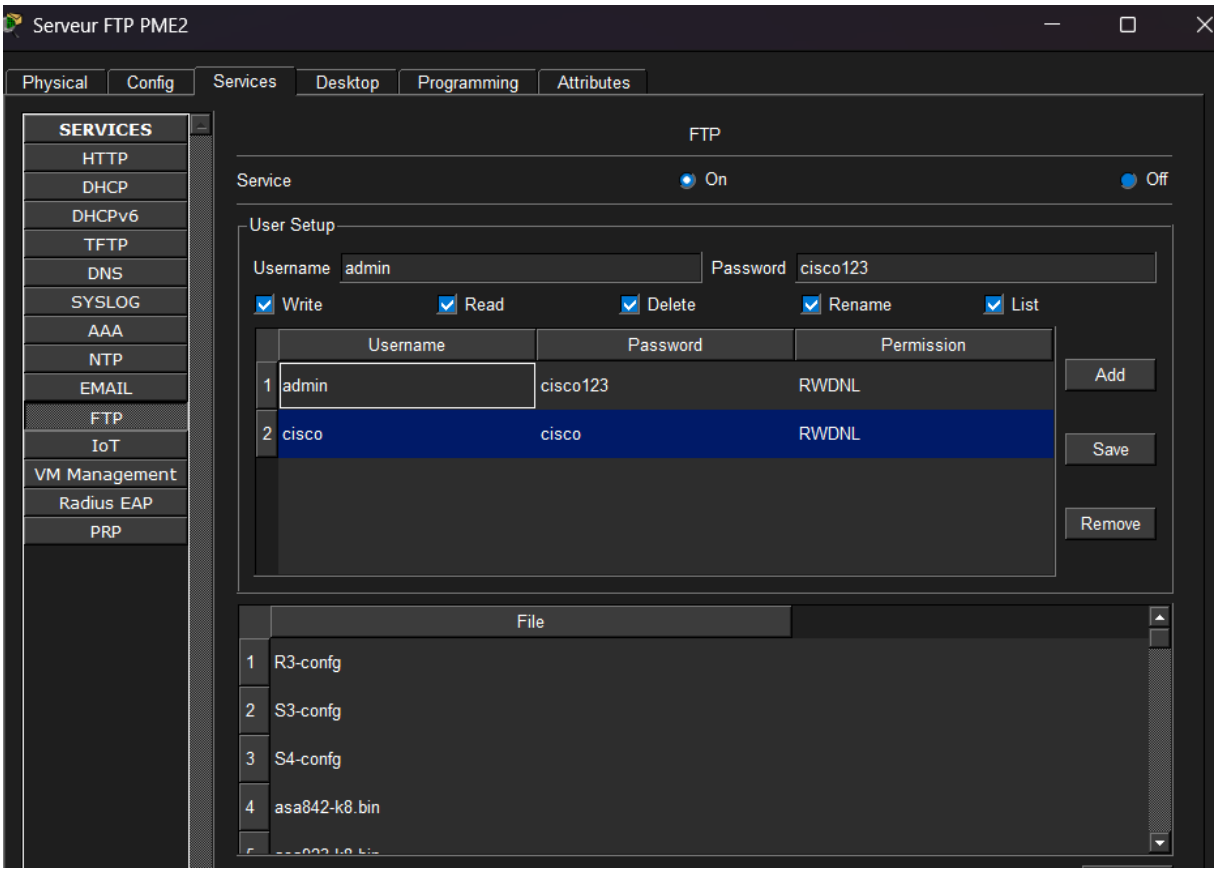
```
C:\>ping 192.168.120.10

Pinging 192.168.120.10 with 32 bytes of data:

Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.

Ping statistics for 192.168.120.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Depuis le PC internaute, nous tentons d'accéder au réseau LAN de PME2 (192.168.100.x). La requête est bloquée par l'ACL 101 appliquée sur l'interface Internet du routeur R3, confirmant que les réseaux privés internes sont bien protégés depuis Internet.



Tests de sauvegarde FTP :

Nous copions la configuration courante finale du routeur R3 et des switches S3 et S4 vers le serveur FTP (192.168.120.1). Les trois fichiers de configuration apparaissent bien dans la liste des fichiers du serveur FTP, confirmant que la sauvegarde fonctionne correctement.



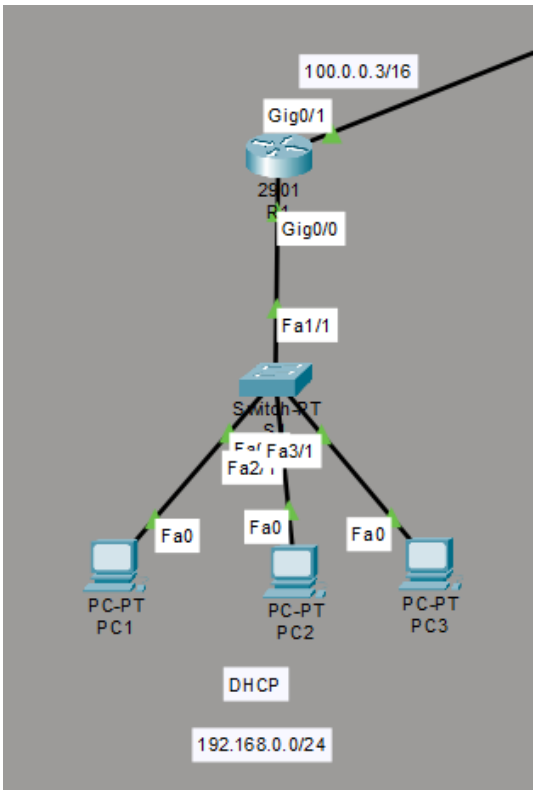
Détails :

1) TPE avec un seul LAN en IPv4 privées sans VLAN :

Pour ce réseau, nous avons besoin :

- 1 routeur, 1 switch, plusieurs stations
- IPv4 privées avec NAT
- Service DHCP pour les utilisateurs
- Aucun service hébergé dans le LAN

Tout d'abord, nous allons brancher les équipements. Nous connectons les stations au switch, puis le switch au routeur comme ci-dessous :



Nous renommons le routeur R1, le switch S1 et les PCs PC1, PC2 et PC3.

Nous avons choisi le réseau 192.168.0.0/24 comme référence.

Nous allons maintenant configurer la passerelle par défaut. Sur le routeur, nous allons passer en mode de configuration globale.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Puis, sur l'interface Gig0/0, nous attribuerons l'adresse 192.168.0.254 au routeur, qui servira de passerelle par défaut. Nous n'oublierons pas d'activer l'interface.

```
Router(config)#interface Gig0/0
Router(config-if)#ip address 192.168.0.254 255.255.255.0
Router(config-if)#no shutdown
```

Ensuite, nous allons configurer le service DHCP. Sur le routeur, au sein du pool dédié au LAN1, nous déclarerons le réseau 192.168.0.0 avec le masque de sous-réseau 255.255.255.0. Enfin, nous renseignerons l'adresse IP 192.168.0.254 comme passerelle par défaut.

```
Router(config)#ip dhcp pool LAN1
Router(dhcp-config)#network 192.168.0.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.0.254
```

Nous allons à présent configurer le NAT, qui permet de remplacer l'adresse IP source privée par l'adresse IP publique de l'interface de sortie du routeur.

Pour ce faire, nous définissons d'abord l'interface interne (inside) et l'interface externe (outside) du réseau.

```
Router(config)#interface gig0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface gig0/1
Router(config-if)#ip nat outside
```

Puis, nous créons une liste de contrôle d'accès pour identifier et autoriser le flux de données provenant de notre réseau local 192.168.0.0/24.

```
Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
```

Enfin, nous activons le NAT en associant notre liste d'accès à l'interface de sortie (GigabitEthernet0/1).

```
Router(config)#ip nat inside source list 1 interface gig0/1 overload
```

Pour finir, nous configurons chaque PC en mode DHCP afin qu'ils récupèrent automatiquement leur adresse IP auprès du routeur.

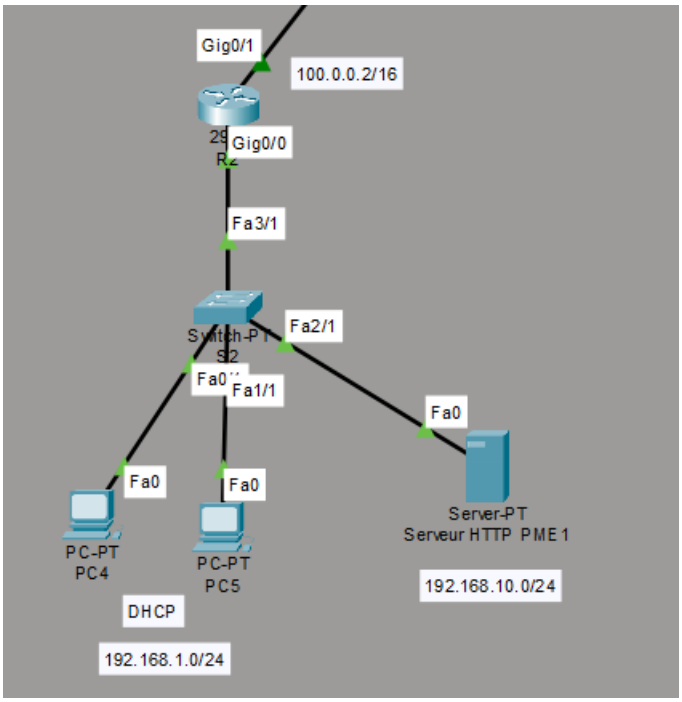
```
C:\>ipconfig /renew

   IP Address.....................: 192.168.0.1
   Subnet Mask....................: 255.255.255.0
   Default Gateway................: 192.168.0.254
   DNS Server.....................: 0.0.0.0
```

2) PME1 avec un LAN et DMZ, IPv4 et IPv6 :

Pour ce réseau, nous avons besoin :

- 1 routeur, 1 switch, plusieurs stations, 1 serveur
- 2 VLANs : LAN et DMZ
- LAN : IPv4 privées, DHCP, IPv6 publiques
- DMZ : IPv4 privées IPv6 publique, service http accessible de l'extérieur en IPv4 par port forwarding et en IPv6 par routage.

Tout d'abord, nous allons brancher les équipements. Nous connectons les stations et le serveur au switch, puis le switch au routeur comme ci-dessous :



Nous renommons le routeur R2, le switch S2 et les PCs PC4, PC5 et le serveur Server HTTP.

Nous avons choisi le réseau 192.168.1.0/24 pour le LAN et le réseau 192.168.10.0/24 pour la DMZ comme référence.

Puis, nous créons les deux zones isolées : le VLAN 1 pour le LAN (VLAN déjà présent par défaut sur le switch) et le VLAN 2 pour la DMZ."

Sur le switch, nous renommons le VLAN 2 en DMZ.

```
S2(config)#vlan 2
S2(config-vlan)#name DMZ
S2(config-vlan)#exit
```

Puis, nous attribuons le port où se trouve le serveur au VLAN 2.

```
S2(config)#int fa2/1
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 2
S2(config-if)#exit
```

Enfin, nous configurons l'interface connectée au routeur en mode TRUNK pour permettre au routeur de recevoir et d'acheminer le trafic des deux VLANs.

```
S2(config)#interface fa3/1
S2(config-if)#switchport mode trunk
```

Ensuite, sur le routeur, nous configurons la première sous-interface virtuelle (Gig0/0.1). Nous y activons l'encapsulation, qui permet au routeur de trier et de séparer le trafic des différents VLANs. Enfin, nous lui attribuons l'adresse IPv4 qui servira de passerelle par défaut pour le LAN, puis nous définissons cette interface comme appartenant à la zone interne du réseau.

```
Router(config)#int gig0/0.1
Router(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1, changed state to
up

Router(config-subif)#encapsulation dot1Q 1
Router(config-subif)#ip address 192.168.1.254 255.255.255.0
Router(config-subif)#ip nat inside
Router(config-subif)#exit
```

Par la suite, nous configurons la seconde sous-interface virtuelle du routeur (Gig0/0.2). De la même manière, nous y activons l'encapsulation afin d'isoler le trafic dédié au VLAN 2. Nous lui attribuons ensuite l'adresse IPv4 qui servira de passerelle par défaut pour la zone DMZ, puis nous définissons cette interface comme appartenant elle aussi à la zone interne (inside) du réseau.

```
Router(config)#int gig0/0.2
Router(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.2, changed state to
up

Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 192.168.10.254 255.255.255.0
Router(config-subif)#ip nat inside
Router(config-subif)#exit
```

Puis, nous créons une liste de contrôle d'accès pour identifier et autoriser le flux de données provenant de notre LAN1 192.168.1.0/24. Nous activons le NAT en associant notre liste d'accès à l'interface de sortie (GigabitEthernet0/1).

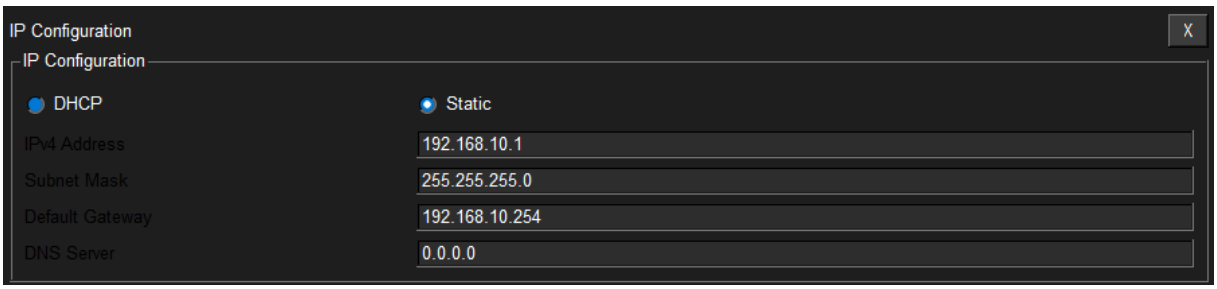
```
Router(config)#int gig0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat inside source list 1 interface gig0/1 overload
```

Ensuite, nous configurons le service DHCP. Sur le routeur, au sein du pool dédié au LAN 1, nous déclarons le réseau 192.168.1.0 avec le masque de sous-réseau 255.255.255.0. Enfin, nous renseignons l'adresse IP 192.168.1.254 comme passerelle par défaut.

```
Router(config)#ip dhcp pool LAN1
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.254
Router(dhcp-config)#exit
```

En revanche, nous n'activons pas de DHCP pour la DMZ (VLAN 2). Le serveur Web a besoin d'une adresse IP fixe pour rester toujours accessible, et cela évite qu'un appareil inconnu n'obtienne une adresse automatiquement dans cette zone sécurisée.

Pour le serveur Web, la configuration IP se fait directement depuis l'interface graphique de l'équipement dans Packet Tracer. Dans l'onglet Desktop > IP Configuration, nous cochons l'option Static et renseignons les paramètres suivants :



Nous allons maintenant configurer l'IPv6. Nous configurons les adresses IPv6 sur nos sous-interfaces virtuelles afin qu'elles servent de passerelles par défaut.

```
Router(config)#int gig0/0.1
Router(config-subif)#ipv6 address 2001:1234:ABCD:1::1/64
Router(config-subif)#exit

Router(config)#int gig0/0.2
Router(config-subif)#ipv6 address 2001:1234:ABCD:10::1/64
Router(config-subif)#exit
```

Nous activons le routage IPv6 de manière globale sur le routeur pour qu'il puisse traiter et acheminer ce type de trafic correctement.

```
Router(config)#ipv6 unicast-routing
```

Nous attribuons une IPv4 publique à l'interface de sortie du routeur.

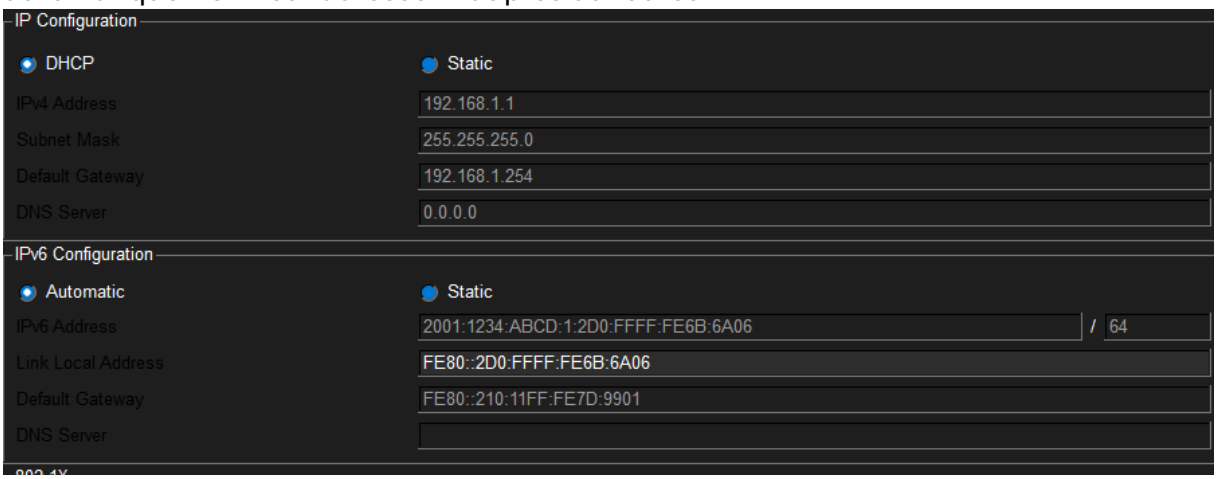
```
Router(config)#int gig0/1
Router(config-if)#ip address 203.0.113.1 255.255.255.0
Router(config-if)#no shutdown
```

Nous mettons en place une règle de NAT statique (redirection de port) :

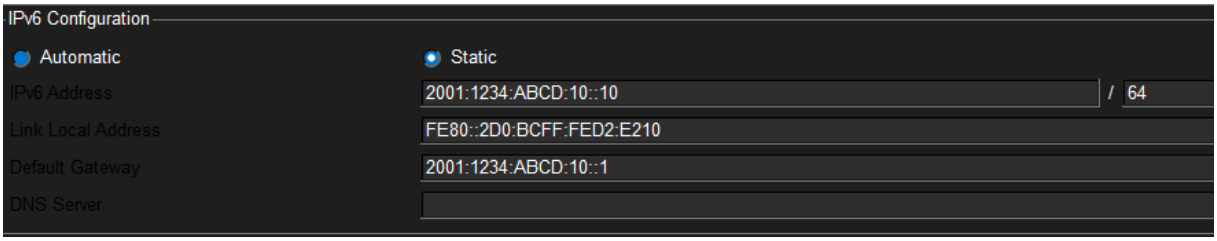
```
Router(config)#ip nat inside source static tcp 192.168.10.1 80 203.0.113.1 80
```

Cette commande redirige l'ensemble du trafic HTTP (port 80) arrivant sur l'interface publique du routeur (203.0.113.1) vers l'adresse IP privée du serveur Web (192.168.10.1). Cela permet aux utilisateurs externes de consulter le site sans avoir un accès direct au reste de notre réseau.

Pour finir, nous configurons chaque PC en mode DHCP afin qu'ils récupèrent automatiquement leur adresse IP auprès du routeur.



Nous configurons l'IPv6 en statique du serveur HTTP.



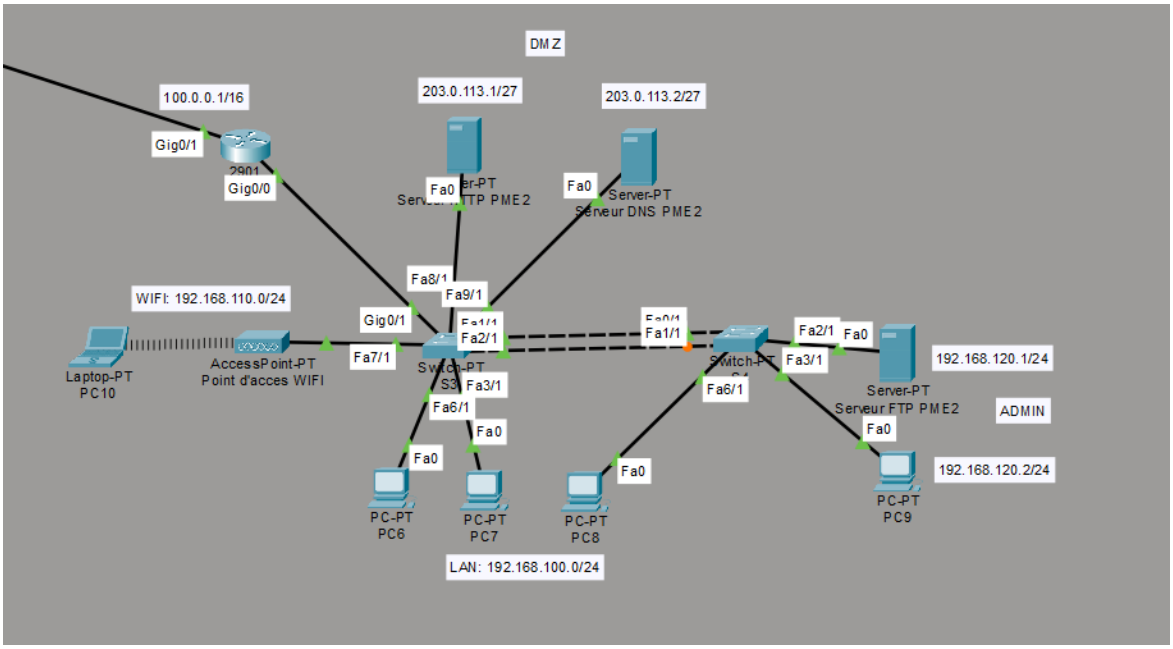
Nous testons la connectivité entre un pc et le serveur web avec l'adresse IPv6 du serveur web (ne pas oublier de mettre les crochets).

3) PME2 avec LAN en IPv4 privées et DMZ en IPv4 publiques :

Pour ce réseau, nous avons besoin :

- 1 routeur, plusieurs switches avec redondance, plusieurs stations, plusieurs serveurs
- 4 VLANs : LAN, WIFI, ADMIN et DMZ
- LAN et WIFI : IPv4 privées, DHCP
- ADMIN : IPv4 privées fixes (administration des actifs par SSH)
    - 1 PC d'administration
    - 1 serveur FTP pour sauvegarde configuration des actifs réseau
- DMZ : IPv4 publiques dans un sous-réseau /27 au maximum, annoncé par OSPF vers Internet, contenant au moins :
    - Serveur HTTP accessible de l'extérieur
    - Serveur DNS accessible de l'extérieur hébergeant la zone DNS de la PME, avec les redirections nécessaires
- Sécurisation pertinente par ACL

Tout d'abord, nous allons brancher les équipements comme ci-dessous.



Tout d'abord, nous allons configurer les switches. Sur le switch S3, nous créons les quatre VLANs nécessaires : le VLAN 10 nommé LAN, le VLAN 20 nommé WIFI, le VLAN 30 nommé ADMIN et le VLAN 40 nommé DMZ.

```
S3(config)#vlan 10
S3(config-vlan)#name LAN
S3(config-vlan)#exit
S3(config)#vlan 20
S3(config-vlan)#name WIFI
S3(config-vlan)#exit
S3(config)#vlan 30
S3(config-vlan)#name ADMIN
S3(config-vlan)#exit
S3(config)#vlan 40
S3(config-vlan)#name DMZ
S3(config-vlan)#exit
```

Nous configurons ensuite les interfaces du switch S3. L'interface connectée au routeur (Gig0/1) est configurée en mode trunk et autorise le passage des VLANs 10, 20, 30 et 40.

```
S3(config)#int gig0/1
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk allowed vlan 10,20,30,40
S3(config-if)#no shutdown
S3(config-if)#exit
```

Les interfaces FastEthernet1/1 et Fa2/1 sont également configurées en mode trunk avec les mêmes VLANs autorisés, afin d'assurer la redondance avec le second switch. Les ports d'accès sont ensuite affectés à leurs VLANs respectifs : fa3/1 et fa6/1 sont rattachés au VLAN 10 (LAN), fa7/1 au VLAN 20 (WIFI), et fa8/1 ainsi que fa9/1 au VLAN 40 (DMZ).

```
S3(config)#interface FastEthernet1/1
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk allowed vlan 10,20,30,40
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#int fa2/1
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk allowed vlan 10,20,30,40
S3(config-if)#no shutdown
S3(config-if)#int fa3/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 10
S3(config-if)#no shutdown
S3(config-if)#int fa6/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 10
S3(config-if)#no shutdown
S3(config-if)#exit

S3(config-if)#int fa7/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
S3(config-if)#no shutdown
S3(config-if)#int fa8/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#no shutdown
S3(config-if)#int fa9/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#no shutdown
S3(config-if)#exit
```

Sur le switch S4, nous créons de la même façon les quatre mêmes VLANs. Ses interfaces fa0/1 et fa1/1, qui assurent les liens de redondance avec S3, sont configurées en mode trunk et autorisent également les VLANs 10, 20, 30 et 40. Le port fa6/1 est affecté au VLAN 10 (LAN).

```
S4(config)#vlan 10
S4(config-vlan)#name LAN
S4(config-vlan)#exit
S4(config)#vlan 20
S4(config-vlan)#name WIFI
S4(config-vlan)#exit
S4(config)#vlan 30
S4(config-vlan)#name ADMIN
S4(config-vlan)#exit
S4(config)#vlan 40
S4(config-vlan)#name DMZ
S4(config-vlan)#exit
S4(config)#int fa0/1
S4(config-if)#switchport mode trunk
S4(config-if)#switchport trunk allowed vlan 10,20,30,40
S4(config-if)#no shutdown
S4(config-if)#int fa1/1
S4(config-if)#switchport mode trunk
S4(config-if)#switchport trunk allowed vlan 10,20,30,40
S4(config-if)#no shutdown
S4(config-if)#exit
S4(config)#int fa6/1
S4(config-if)#switchport mode access
S4(config-if)#switchport access vlan 10
S4(config-if)#no shutdown
S4(config-if)#exit
```

Les ports fa2/1 et fa3/1 de S4 sont affectés au VLAN 30 (ADMIN).

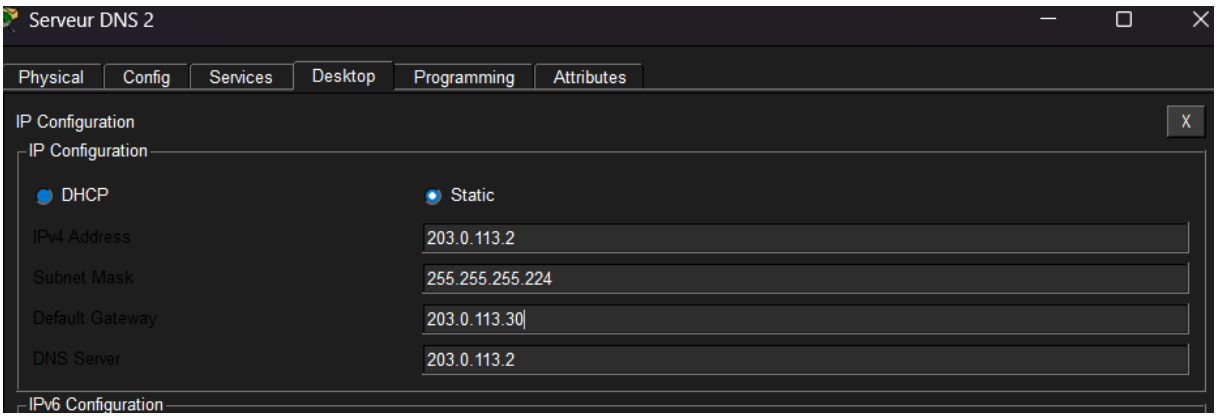
```
S4(config-if)#int fa2/1
S4(config-if)#switchport mode access
S4(config-if)#switchport access vlan 30
S4(config-if)#no shutdown
S4(config-if)#exit
S4(config)#int fa3/1
S4(config-if)#switchport mode access
S4(config-if)#switchport access vlan 30
S4(config-if)#no shutdown
S4(config-if)#exit
```

Nous passons ensuite à la configuration du routeur R3. Nous activons d'abord l'interface physique Gig0/0, puis nous créons quatre sous-interfaces virtuelles correspondant à chacun des VLANs.

Sur la sous-interface Gig0/0.10, nous activons l'encapsulation dot1Q pour le VLAN 10 et attribuons l'adresse 192.168.100.254/24, qui servira de passerelle par défaut pour le LAN. Sur Gig0/0.20, nous faisons de même pour le VLAN 20 (WIFI) avec l'adresse 192.168.110.254/24. Sur Gig0/0.30, nous configurons le VLAN 30 (ADMIN) avec l'adresse 192.168.120.254/24. Enfin, sur Gig0/0.40, nous configurons le VLAN 40 (DMZ) avec l'adresse publique 203.0.113.30/27, afin que les serveurs de la DMZ disposent d'adresses IP directement routables sur Internet.

```
R3(config)#int gig0/0
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R3(config-if)#exit
R3(config)#int gig0/0.10
R3(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.10, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up

R3(config-subif)#encapsulation dot1Q 10
R3(config-subif)#ip address 192.168.100.254 255.255.255.0
R3(config-subif)#no shutdown
R3(config-subif)#exit
R3(config)#int gig0/0.20
R3(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.20, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

R3(config-subif)#encapsulation dot1Q 20
R3(config-subif)#ip address 192.168.110.254 255.255.255.0
R3(config-subif)#no shutdown
R3(config-subif)#exit
R3(config)#int gig0/0.30
R3(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.30, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up

R3(config-subif)#encapsulation dot1Q 30
R3(config-subif)#ip address 192.168.120.254 255.255.255.0
R3(config-subif)#no shutdown
R3(config-subif)#exit
R3(config)#int gig0/0.40
R3(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0.40, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40, changed state to up

R3(config-subif)#encapsulation dot1Q 40
R3(config-subif)#ip address 203.0.113.30 255.255.255.224
R3(config-subif)#no shutdown
R3(config-subif)#exit
```

Nous configurons ensuite les adresses IP fixes de la DMZ. Pour le serveur DNS, nous lui attribuerons l'adresse 203.0.113.2 avec le masque 255.255.255.224 et la passerelle 203.0.113.30. Le serveur DNS pointe sur lui-même (203.0.113.2) puisqu'il héberge la zone DNS de la PME2.



Nous ferons pareil pour le serveur HTTP avec l'adresse 203.0.113.1 avec le masque 255.255.255.224, la passerelle 203.0.113.30 et le serveur DNS 203.0.113.2.

Nous ferons la même chose pour le serveur FTP avec l'adresse 192.168.120.1 avec le masque 255.255.255.0, la passerelle 192.168.120.254 et le serveur DNS 203.0.113.2. Ainsi que pour le PC ADMIN avec l'adresse 192.168.120.2 avec le masque 255.255.255.0, la passerelle 192.168.120.254 et le serveur DNS 203.0.113.2.

Nous configurons le DHCP sur le routeur. Nous commençons par exclure les adresses de passerelle afin qu'elles ne soient pas distribuées automatiquement : 192.168.100.254 pour le LAN et 192.168.110.254 pour le WIFI.

```
R3(config)#ip dhcp excluded-address 192.168.100.254
R3(config)#ip dhcp excluded-address 192.168.110.254
```

Nous créons ensuite les deux pools DHCP. Le pool LAN distribue des adresses sur le réseau 192.168.100.0/24 avec la passerelle 192.168.100.254 et le serveur DNS 203.0.113.2. Le pool WIFI distribue des adresses sur le réseau 192.168.110.0/24 avec la passerelle 192.168.110.254 et le même serveur DNS. La DMZ et le VLAN ADMIN ne disposent pas de DHCP : les serveurs et équipements d'administration utilisent des adresses IP fixes configurées juste avant.

```
R3(config)#ip dhcp pool LAN
R3(dhcp-config)#network 192.168.100.0 255.255.255.0
R3(dhcp-config)#default-router 192.168.100.254
R3(dhcp-config)#dns-server 203.0.113.2
R3(dhcp-config)#exit
R3(config)#ip dhcp pool WIFI
R3(dhcp-config)#network 192.168.110.0 255.255.255.0
R3(dhcp-config)#default-router 192.168.110.254
R3(dhcp-config)#dns-server 203.0.113.2
R3(dhcp-config)#exit
```

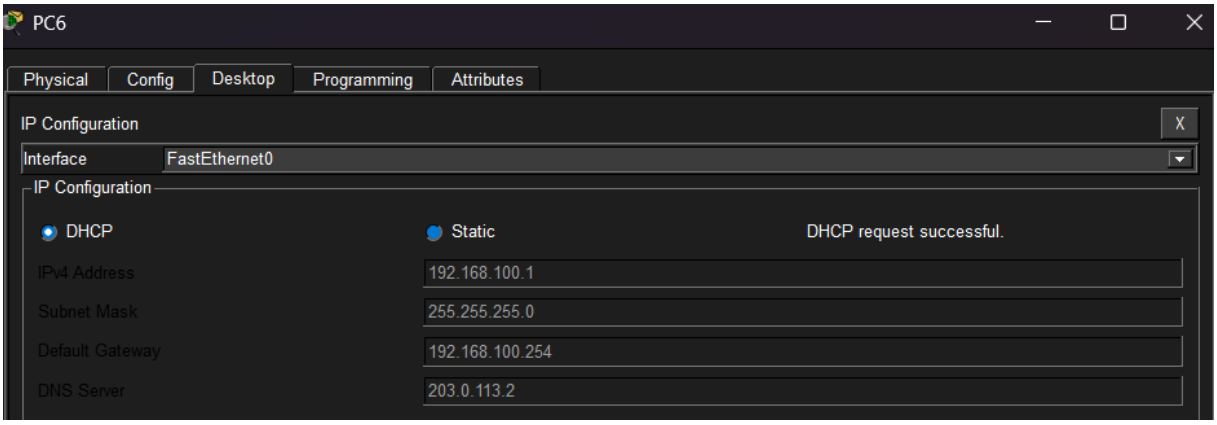
Une fois le routeur configuré, nous renseignons la passerelle par défaut sur les switches pour leur permettre d'être administrés à distance. Sur S3, nous définissons 192.168.120.254 (passerelle du VLAN ADMIN) comme route par défaut.

```
S3(config)#ip default-gateway 192.168.120.254
```

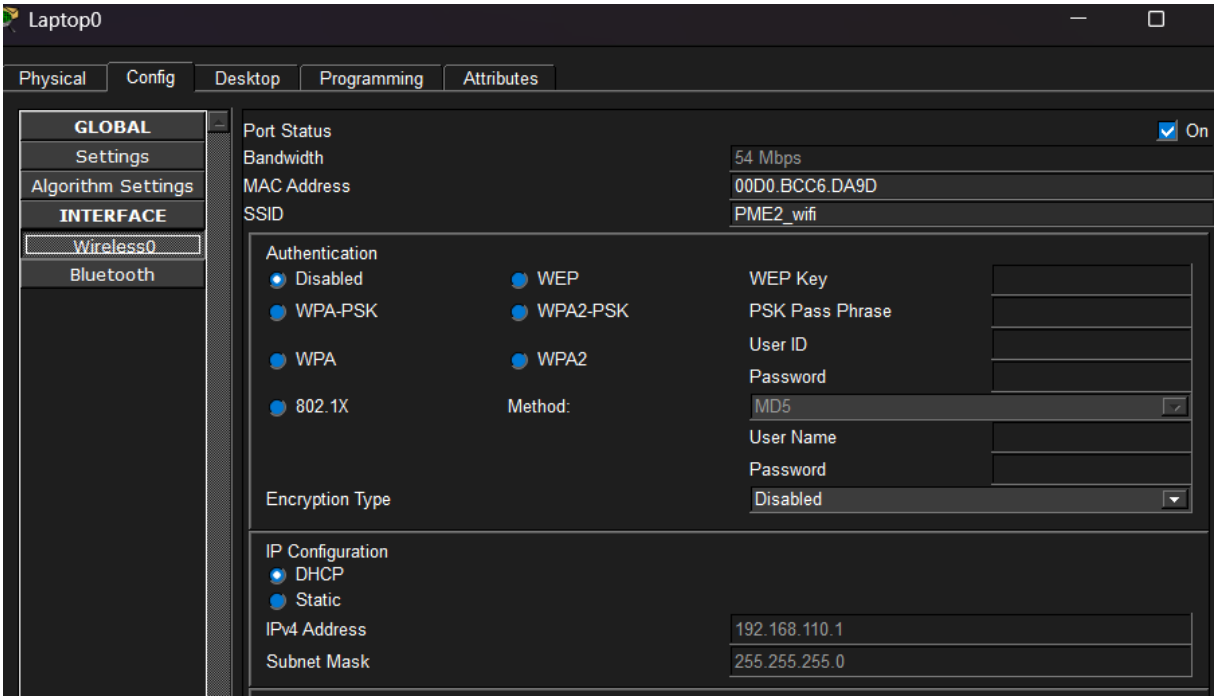
Nous faisons la même opération sur S4, en lui attribuant également 192.168.120.254 comme passerelle par défaut.

```
S4(config)#ip default-gateway 192.168.120.254
```

Nous vérifions ensuite que les PC du LAN obtiennent bien une adresse IP en DHCP.



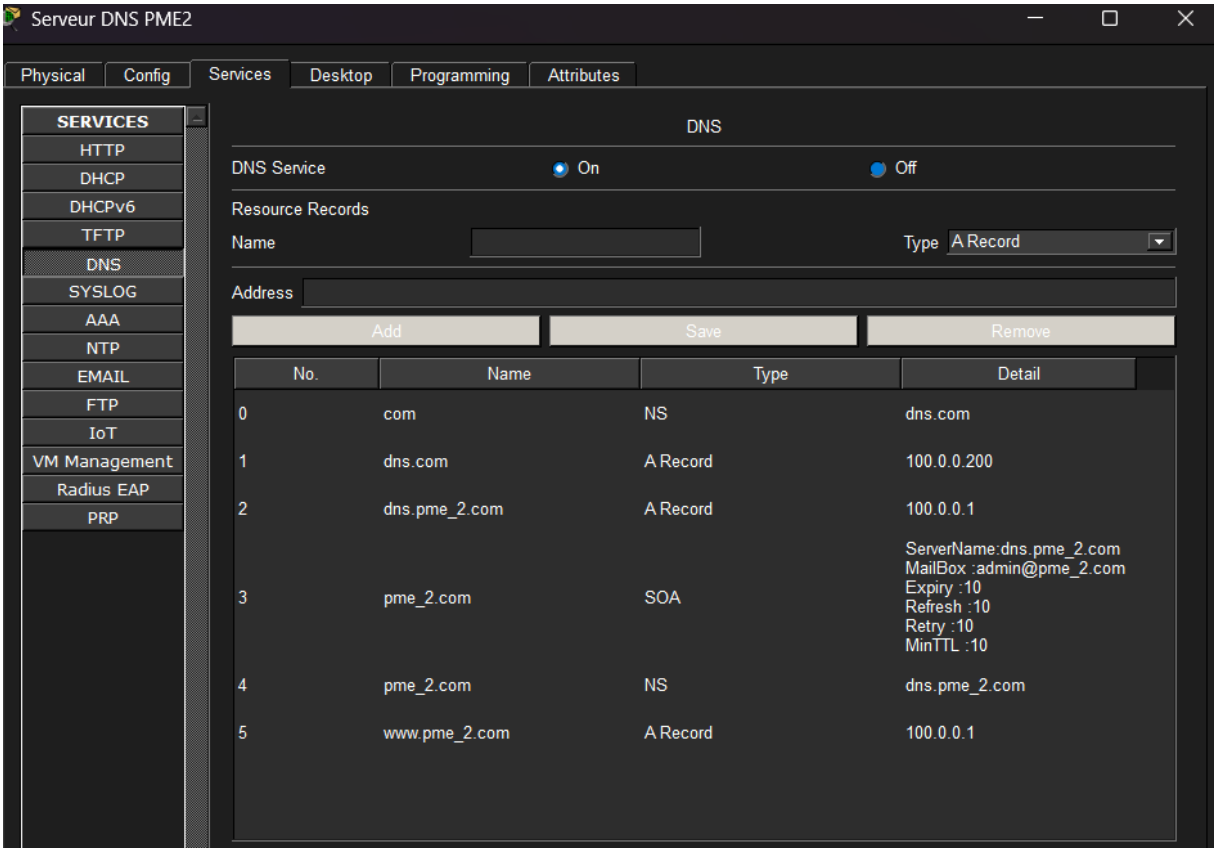
Pour la connexion Wi-Fi, nous configurons le point d'accès avec le SSID PME2_wifi. Sur le laptop, nous ajoutons d'abord un module réseau sans fil (WPC300N) dans l'onglet Physical, puis dans l'onglet « Config, Interface -> Wireless0 », nous renseignons le SSID PME2_wifi. Le laptop se connecte automatiquement au point d'accès et obtient l'adresse 192.168.110.1/24 via DHCP.



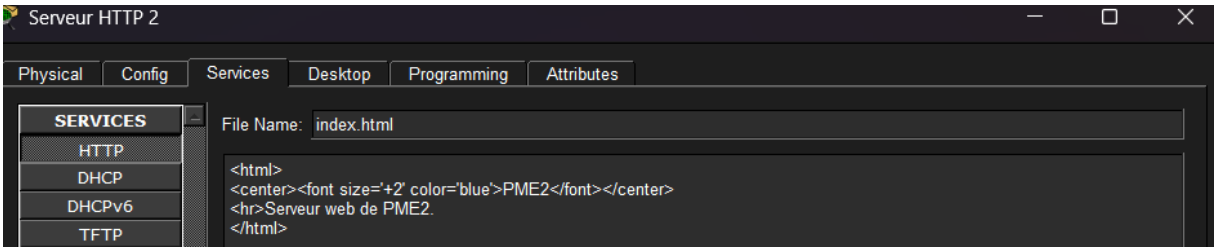
Nous configurons enfin le serveur DNS de la PME2. Dans l'onglet « Services – DNS », nous activons le service DNS et saisissons les enregistrements de la zone pme_2.com suivants :

- Un enregistrement NS pour com, pointant vers dns.com
- Un enregistrement A associant dns.com à 100.0.0.200
- Un enregistrement A associant dns.pme_2.com à 100.0.0.1
- Un enregistrement SOA pour pme_2.com, déclarant dns.pme_2.com comme serveur autoritaire de la zone
- Un enregistrement NS pour pme_2.com, pointant vers dns.pme_2.com

- Un enregistrement A associant www.pme_2.com à 100.0.0.1, soit l'adresse du serveur HTTP



Pour le serveur HTTP, la page d'accueil index.html est éditée directement depuis l'onglet « Services -> HTTP ». Nous y affichons un titre « PME2 » avec la mention « Serveur web de PME2 », pour confirmer que le site est bien hébergé et accessible via le nom de domaine www.pme_2.com.

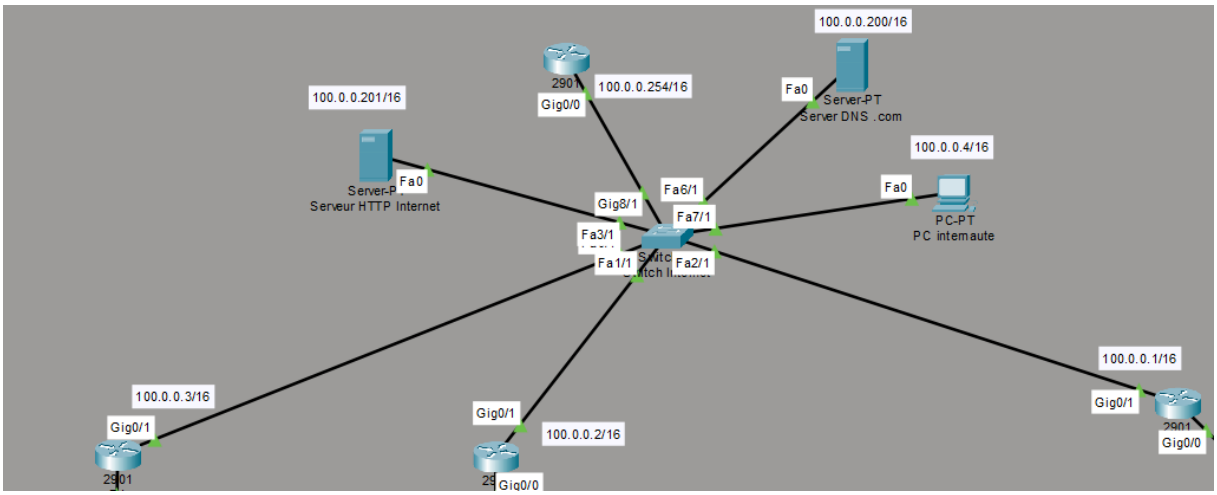


4) Zone Internet :

Pour ce réseau, nous avons besoin :

- Une zone « internet » avec IPv4 et IPv6 publiques permettant d'interconnecter les entreprises, contenant au minimum :
  - 1 routeur en IPv4 et IPv6 connaissant les routes utiles et servant de passerelle et de voisin OSPF pour les autres équipements de la zone
  - 1 serveur DNS principal « .com » avec les enregistrements et les délégations nécessaires pour les PME
  - 1 serveur http www.internet.com extérieur aux entreprises
  - 1 PC « internaute » extérieur aux entreprises

Tout d'abord, nous allons brancher les équipements aux switches ci-dessous :

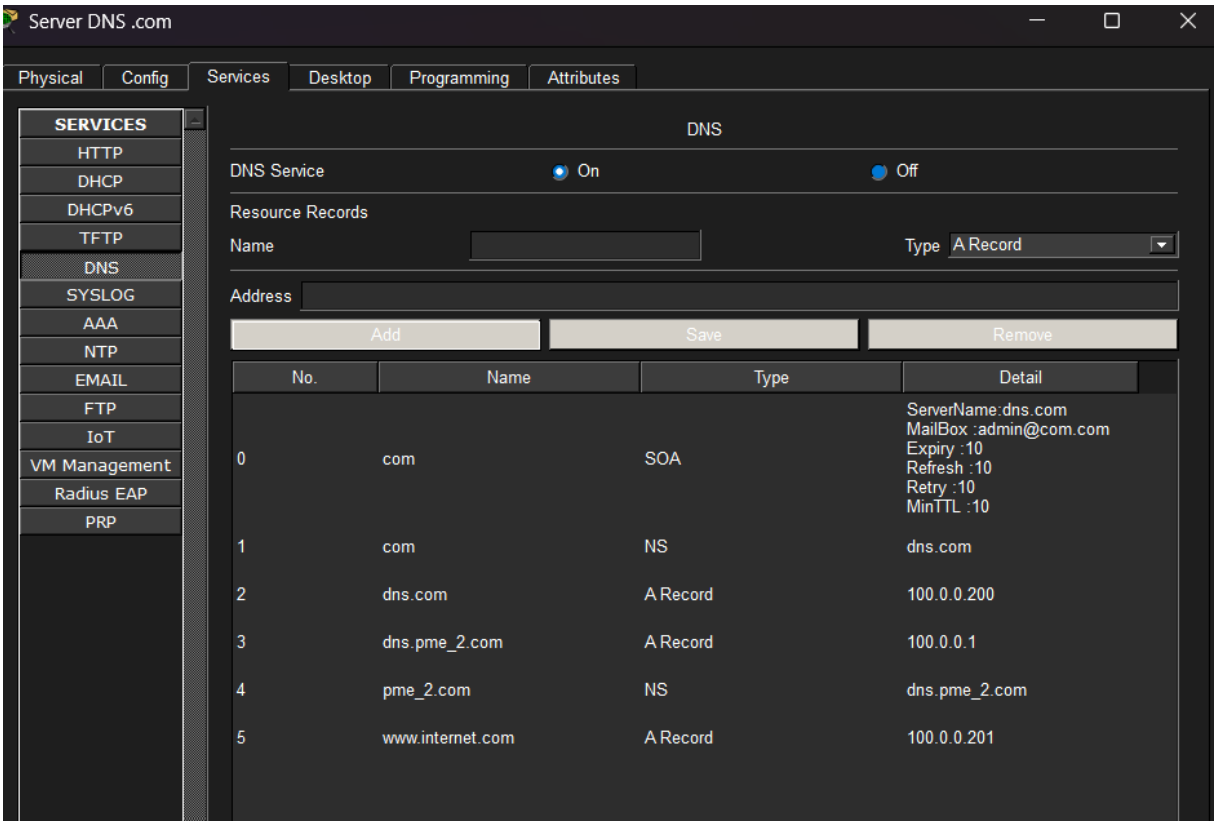


Nous activons les interfaces et leur attribuons des adresses IP publiques aux routeurs des PME et du TPE sur leur interface de sortie.

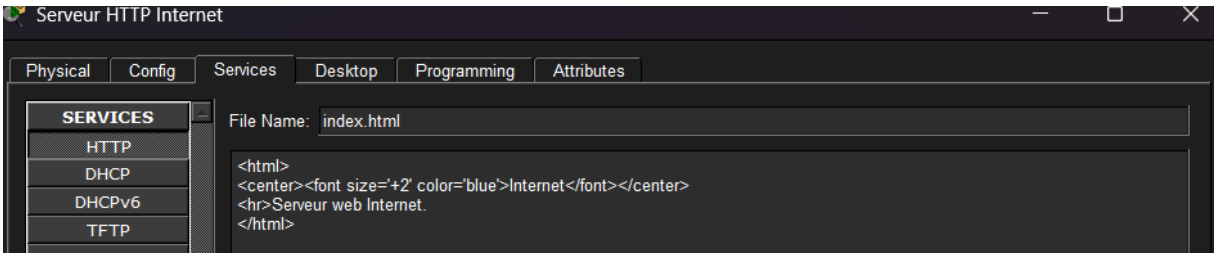
```
R1(config)#int gig0/1
R1(config-if)#ip address 100.0.0.3 255.255.0.0
R1(config-if)#no shutdown
```

Nous configurons ensuite le serveur DNS .com. Dans l'onglet « Services – DNS », nous activons le service DNS et saisissons les enregistrements suivants :

- Un enregistrement SOA pour com, déclarant dns.com comme serveur autoritaire
- Un enregistrement NS pour com, pointant vers dns.com
- Un enregistrement A associant dns.com à 100.0.0.200
- Des enregistrements NS et A pour chaque PME, permettant la délégation vers leurs serveurs DNS respectifs
- Un enregistrement A associant www.internet.com à 100.0.0.201



Nous configurons le serveur HTTP Internet. Dans l'onglet « Services – HTTP », nous activons le service et éditons le fichier index.html pour mentionner « Serveur web Internet ».



Nous configurons ensuite la route par défaut sur chaque routeur d'entreprise afin que tout trafic à destination d'Internet soit acheminé vers le routeur Internet (100.0.0.254).

```
R2(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.254
```

Pour le TPE, la configuration DNS est distribuée automatiquement aux postes clients via le service DHCP configuré sur le routeur, pointant vers le serveur DNS Internet (100.0.0.200).

```
R1(config)#ip dhcp pool LAN1
R1(dhcp-config)#dns-server 100.0.0.200
```

Nous mettons en place le protocole OSPF sur le routeur Internet ainsi que sur chaque routeur d'entreprise. OSPF permet aux routeurs d'échanger automatiquement leurs tables de routage et ainsi de connaître les routes vers chaque réseau. La configuration est identique sur tous les routeurs : on déclare le réseau 100.0.0.0/16 dans l'aire 0.

```
R4(config)#router ospf 1
R4(config-router)#router-id 1.1.1.1
R4(config-router)#network 100.0.0.0 0.0.255.255 area 0
```

Nous activons ensuite OSPF pour IPv6 sur le routeur PME1 afin d'annoncer ses réseaux IPv6 vers le routeur Internet.

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#router-id 3.3.3.3
R2(config-rtr)#int gig0/0.2
R2(config-subif)#ipv6 ospf 1 area 0
R2(config-subif)#int gig0/1
R2(config-if)#ipv6 ospf 1 area 0
```

De même, nous activons OSPFv3 sur le routeur Internet pour qu'il puisse recevoir et redistribuer les routes IPv6 des différentes entreprises.

```
R4(config)#int gig0/0
R4(config-if)#ipv6 ospf 1 area 0
```

Nous configurons ensuite le NAT sur le routeur PME2. Nous définissons d'abord les interfaces internes (inside) pour les VLANs LAN, WIFI, ADMIN et DMZ, et l'interface externe (outside) sur GigabitEthernet0/1. Nous créons ensuite l'ACL 99 qui identifie les adresses privées à translater, et nous activons le NAT overload (PAT) en associant cette ACL à l'interface de sortie. Enfin, nous mettons en place les redirections de ports pour le serveur HTTP (port 80) et le serveur DNS (port 53) de la DMZ.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int gig0/0.10
R3(config-subif)#ip nat inside
R3(config-subif)#exit
R3(config)#int gig0/0.20
R3(config-subif)#ip nat inside
R3(config-subif)#exit
R3(config)#int gig0/0.30
R3(config-subif)#ip nat inside
R3(config-subif)#exit
R3(config)#int gig0/0.40
R3(config-subif)#ip nat inside
R3(config-subif)#exit
R3(config)#int gig0/1
R3(config-if)#ip nat outside
R3(config-if)#exit
R3(config)#access-list 99 permit 192.168.100.0 0.0.0.255
R3(config)#access-list 99 permit 192.168.110.0 0.0.0.255
R3(config)#access-list 99 permit 192.168.120.0 0.0.0.255
R3(config)#ip nat inside source list 99 interface gig0/1 overload

R3(config)#ip nat inside source static tcp 203.0.113.1 80 100.0.0.1 80
R3(config)#ip nat inside source static tcp 203.0.113.2 80 100.0.0.1 80
R3(config)#ip nat inside source static udp 203.0.113.2 53 100.0.0.1 53
```

Nous vérifions que le PC11 (internaute) peut accéder au serveur HTTP de PME2 via son adresse publique. Depuis le navigateur web du PC11, nous accédons à l'adresse 100.0.0.1 et la page d'accueil de PME2 s'affiche correctement.

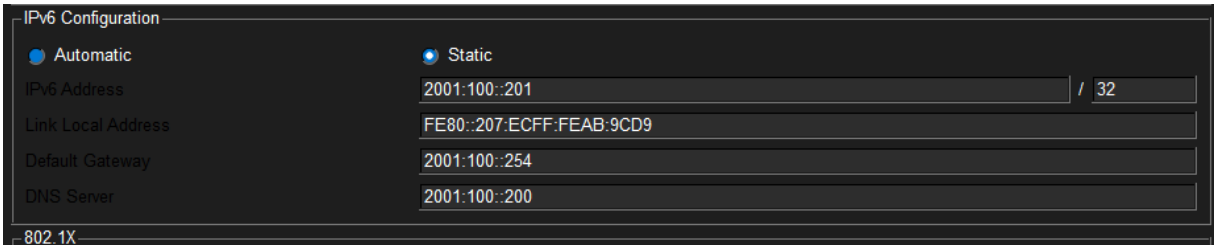
La configuration NAT de PME1 est similaire : une redirection de port achemine le trafic HTTP arrivant sur l'interface publique (100.0.0.2) vers le serveur HTTP interne de PME1 (192.168.10.1).

```
R2(config)#ip nat inside source static tcp 192.168.10.1 80 100.0.0.2 80
```

Nous configurons les adresses IPv6 sur l'interface de sortie du routeur PME1 (GigabitEthernet0/1). L'adresse 2001:100::2/32 est attribuée, permettant à PME1 d'être joignable en IPv6 depuis la zone Internet.

```
R2(config)#int gig0/1
R2(config-if)#ipv6 address 2001:100::2/32
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#ipv6 unicast-routing
```

Nous attribuons des adresses IPv6 à tous les équipements de la zone Internet : le serveur HTTP (2001:100::201/32), le serveur DNS .com (2001:100::200/32) et le PC11 (2001:100::4/32). Le routeur Internet dispose de l'adresse 2001:100::254/32.



Nous mettons en place des règles de filtrage ACL sur le routeur R3 de PME2. La première ACL (ACL 100) interdit l'accès au VLAN ADMIN depuis tous les autres réseaux (LAN, WIFI, DMZ et Internet). Cette ACL est appliquée en sortie sur l'interface GigabitEthernet0/0.30 afin de filtrer tout trafic cherchant à atteindre le réseau 192.168.120.0/24.

```
R3(config)#access-list 100 deny ip 192.168.100.0 0.0.0.255 192.168.120.0 0.0.0.255
R3(config)#access-list 100 deny ip 192.168.110.0 0.0.0.255 192.168.120.0 0.0.0.255
R3(config)#access-list 100 deny ip 203.0.113.0 0.0.0.31 192.168.120.0 0.0.0.255
R3(config)#access-list 100 deny ip any 192.168.120.0 0.0.0.255
R3(config)#access-list 100 permit ip any any
```

La seconde ACL (ACL 101) est appliquée en entrée sur l'interface GigabitEthernet0/1 (côté Internet). Elle autorise uniquement le trafic HTTP vers le serveur HTTP de la DMZ et le trafic DNS vers le serveur DNS de la DMZ, et bloque tout accès depuis Internet vers les réseaux privés internes.

```
R3(config)#access-list 101 permit tcp any host 203.0.113.1 eq 80
R3(config)#access-list 101 permit udp any host 203.0.113.2 eq 53
R3(config)#access-list 101 permit tcp any host 203.0.113.2 eq 53
R3(config)#access-list 101 deny ip any 192.168.100.0 0.0.0.255
R3(config)#access-list 101 deny ip any 192.168.110.0 0.0.0.255
R3(config)#access-list 101 deny ip any 192.168.120.0 0.0.0.255
R3(config)#access-list 101 permit ip any any
```

Nous ajoutons également la DMZ (203.0.113.0/27) dans l'ACL 99 du NAT. En effet, dans Packet Tracer, même si les adresses de la DMZ sont publiques, le routeur doit les inclure dans le NAT pour que les serveurs de la DMZ puissent initier des connexions vers Internet (notamment pour

les requêtes DNS vers le serveur .com). C'est la seule solution fonctionnelle dans Packet Tracer pour ce cas particulier.

```
R3(config)#access-list 99 permit 203.0.113.0 0.0.0.31
```

Nous appliquons ensuite les ACL sur les interfaces correspondantes du routeur.

```
R3(config)#int gig0/0.30
R3(config-subif)#ip access-group 100 in
R3(config-subif)#exit
R3(config)#int gig0/1
R3(config-if)#ip access-group 101 in
```

Sur PME1, une ACL similaire est configurée pour sécuriser l'accès aux ressources internes.

```
R2(config)#access-list 1 permit 192.168.10.0 0.0.0.255
```

Nous sécurisons l'accès au routeur R3 par SSH. Nous configurons le nom de domaine, générons les clés RSA, activons SSH version 2 et créons un utilisateur local « **admin** » avec comme mot de passe « **admin123** ». L'ACL 10 restreint les connexions SSH au seul réseau ADMIN (192.168.120.0/24).

```
R3(config)#hostnam R3
R3(config)#ip domain-name pme_2.local
R3(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: R3.pme_2.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 11:30:42.630: %SSH-5-ENABLED: SSH 1.99 has been enabled
R3(config)#username admin privilege 15 secret admin123
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#login local
R3(config-line)#transport input ssh
```

La même configuration SSH est appliquée sur le switch S4 (et de manière identique sur S3). Une interface VLAN 30 est créée sur chaque switch pour lui attribuer une adresse IP d'administration dans le réseau ADMIN.

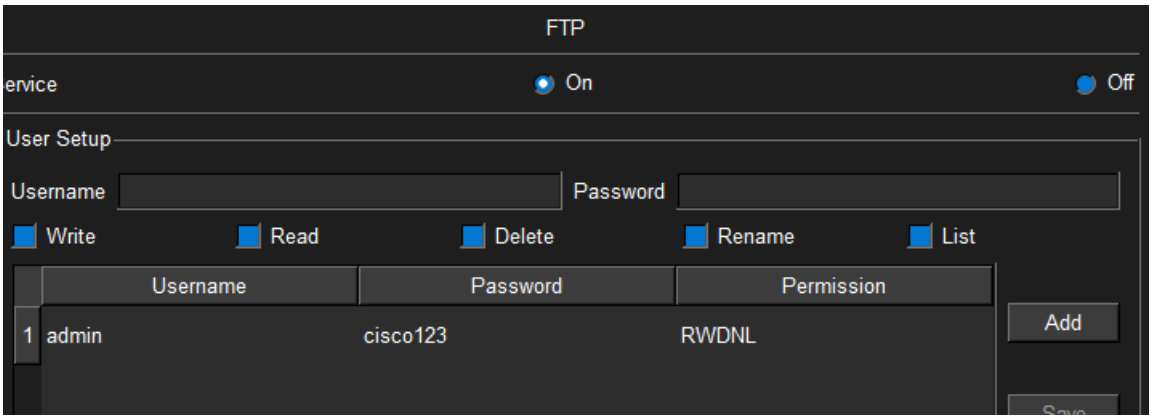
```
S4(config)#int vlan 30
S4(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

S4(config-if)#ip address 192.168.120.4 255.255.255.0
S4(config-if)#no shutdown
S4(config-if)#exit
S4(config)#hostname S4
S4(config)#ip domain-name pme_2.local
S4(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: S4.pme_2.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 11:24:17.259: %SSH-5-ENABLED: SSH 1.99 has been enabled
S4(config)#username admin privilege 15 secret admin123
S4(config)#line vty 0 4
S4(config-line)#access-class 10 in
S4(config-line)#login local
S4(config-line)#transport input ssh
```

```
S3(config)#int vlan 30
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

S3(config-if)#ip address 192.168.120.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#access-list 10 permit 192.168.120.0 0.0.0.255
S3(config)#hostname S3
S3(config)#ip domain-name pme_2.local
S3(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S3.pme_2.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 11:0:44.238: %SSH-5-ENABLED: SSH 1.99 has been enabled
S3(config)#username admin privilege 15 secret admin 123
S3(config)#line vty 0 4
S3(config-line)#access-class 10 in
S3(config-line)#login local
S3(config-line)#transport input ssh
```

Nous vérifions depuis le PC ADMIN (192.168.120.2) que la connexion SSH fonctionne bien vers le routeur R3, le switch S3 et le switch S4.

```
C:\>ssh -l admin 192.168.120.254

Password:



R3#exit

[Connection to 192.168.120.254 closed by foreign host]
C:\>ssh -l admin 192.168.120.3

Password:



S3#exit

[Connection to 192.168.120.3 closed by foreign host]
C:\>ssh -l admin 192.168.120.4

Password:



S4#exit
```

Nous configurons le serveur FTP (Server FTP PME2, 192.168.120.1). Dans l'onglet « Services – FTP », nous activons le service et créons un compte utilisateur « **admin** » avec comme mot de passe « **cisco123** ».



Sur le routeur R3, nous renseignons les identifiants FTP puis copions la configuration courante vers le serveur FTP.

```
R3(config)#ip ftp username admin
R3(config)#ip ftp password cisco123
R3(config)#ip domain-name pme_2

R3#copy running-config ftp
Address or name of remote host []? 192.168.120.1
Destination filename [R3-confg]?

Writing running-config...
[OK - 2495 bytes]

2495 bytes copied in 0.052 secs (47000 bytes/sec)
```

Nous effectuons la même opération sur les switches S3 et S4. Nous vérifions ensuite sur le serveur FTP que les fichiers de configuration des trois équipements sont bien présents.

CONCLUSION :

Ce projet nous a permis de concevoir et de mettre en œuvre un réseau d'entreprise complet sur Cisco Packet Tracer. Nous avons configuré les équipements de chaque entreprise en appliquant les règles demandées dans le cahier des charges telles que le NAT, le DHCP, les VLANs, OSPF, les ACL et SSH, en justifiant chacun de nos choix techniques. Les tests réalisés ont validé le bon fonctionnement de l'ensemble des configurations et le respect du cahier des charges. Ce projet nous a permis de mettre en pratique les notions vues en cours et d'approfondir notre compréhension des réseaux d'entreprise.