IUT - Nice Côte d'Azur Site de Sophia Antipolis
650 Routes des Colles
06560 Valbonne

SAÉ THALES n°21

Construire un réseau informatique pour une petite structure

Enseignant de la matière : Guillaume Urvoy-Keller & Michael Lance

Déroulé du projet :

- 6h de TP en salle 410 avec équipements physiques
- Avancement maison sous Packet Tracer

Objectif du projet :

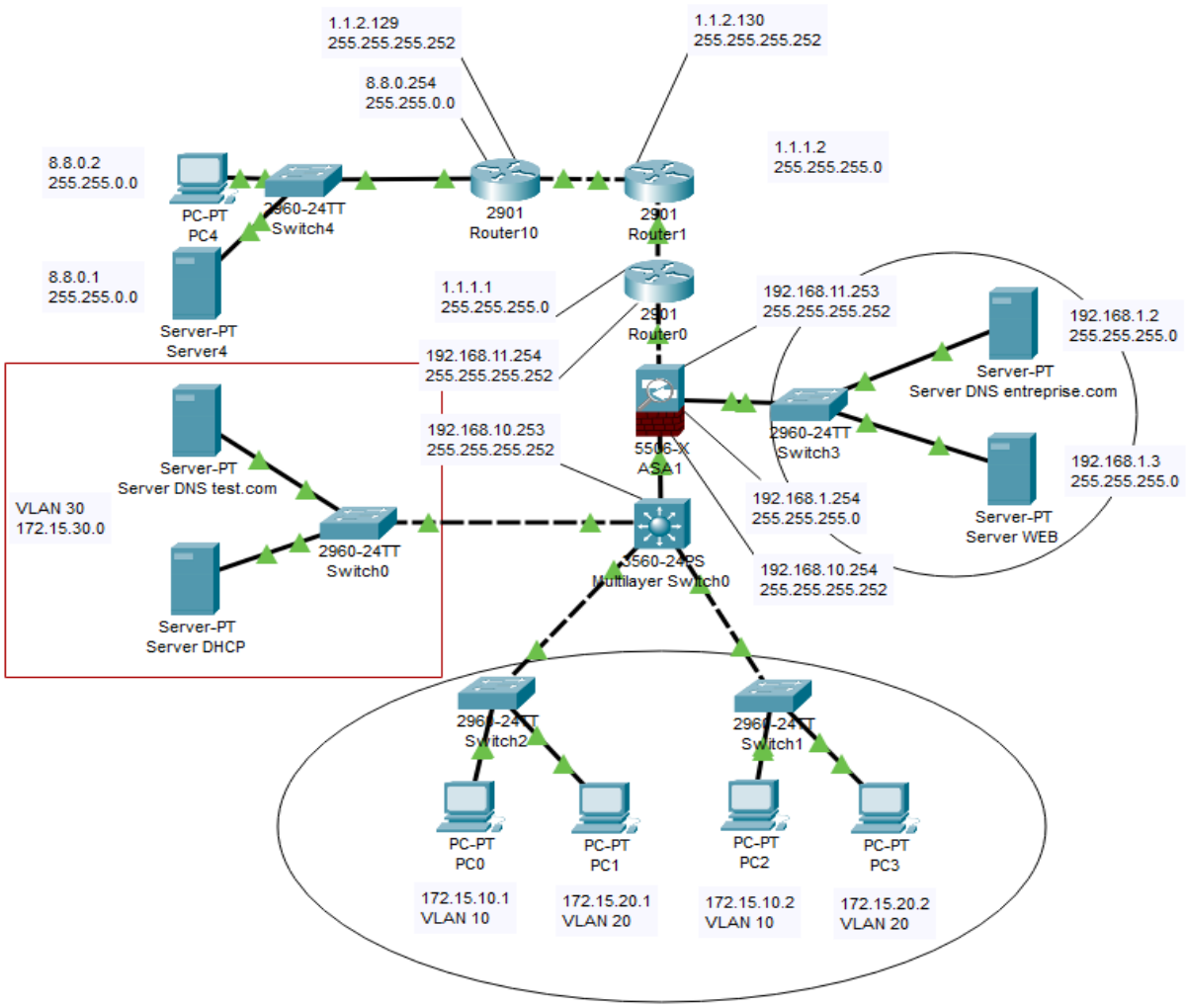
Réaliser un petit réseau d'entreprise qui correspond aux différents critères recherchés à savoir assurer une bonne connectivité des équipements ainsi qu'une sécurisation des données.

Sommaire

Construction de la base du réseau

Plan d'adressage des équipements :

Screenshot PacketTracer de la topologie générale :



Bilan des adresses réseaux :

VLAN 10 : Réseau 172.15.10.0/24 (Mask 255.255.255.0)

- Ordinateurs configurés en .1 et .2
- Gateway (Switch Multilayer) configuré en .241

VLAN 20 : Réseau 172.15.20.0/24 (Mask 255.255.255.0)

- Ordinateurs configurés en .1 et .2
- Gateway (Switch Multilayer) configuré en .254

VLAN 30 : Réseau 172.15.30.0/24 (Mask 255.255.255.0)

- Serveur interne configuré en dhcp + dns en .2
- Gateway (Switch Multilayer) configuré en .254

Entre l'ASA et le Switch Multilayer : Réseau 192.168.10.252/30 (Mask 255.255.255.252)

- Interface de l'ASA configuré en .254
- Switch Multilayer en .253

Serveur WEB (DMZ) : Réseau 192.168.1.0/24 (Mask 255.255.255.0)

- Ordinateurs configurés en .2 et .3
- Gateway (Firewall ASA) configuré en .254

Entre l'ASA et le Routeur Entreprise : Réseau 192.168.11.252/30 (Mask 255.255.255.252)

- Interfaces de l'ASA et routeur configurés en .253 et .254

Serveur FAI (Fournisseur Internet) : Réseau 1.1.1.0/24 (Mask 255.255.255.0)

- Interfaces routeurs configurés en .1 et .2

Second Serveur FAI (Fournisseur Internet) : Réseau 1.1.2.128/30 (Mask 255.255.255.252)

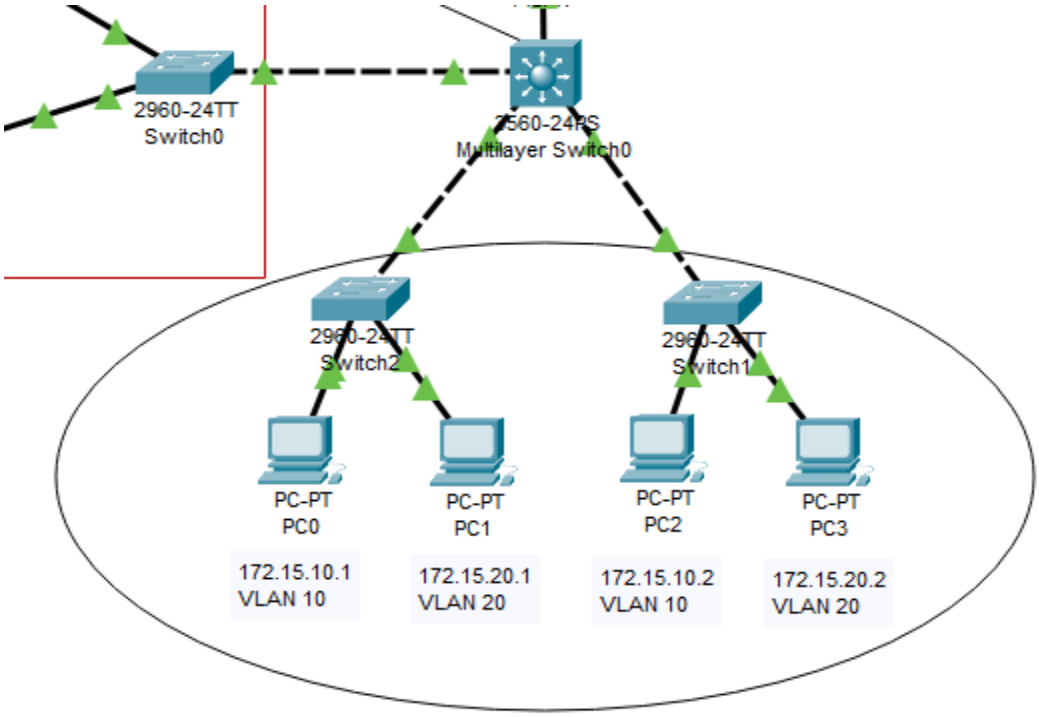
- Interfaces routeurs configurés en .1 et .2

Serveur externe : Réseau 8.8.0.0/16 (Mask 255.255.0.0)

- Interface routeur configuré en .254
- Serveur et ordinateur configurés en .1 et .2

Réalisation d'un réseau à base de Switchs :

Screenshot PacketTracer de la base du réseau :



Sur le schéma, 2 Switchs 2960 sont reliés à un Switch 3560 24PS (Multilayer), chacun des switchs sont reliés à 2 ordinateurs.

Ce réseau est basé sur les VLAN (Virtual local area network) pour connecter les machines entre elles.

Pour le moment, il n'y a que 2 VLANS ajoutés au switch Multilayer, la VLAN 10 et 20.

Commandes de configuration des équipements :

Switch Multilayer :

IOS Command Line Interface

```
MLS>en
MLS#conf t

– Ajout des VLANS –

MLS(config)#vlan 10
MLS(config-vlan)#vlan 20

– Configuration Trunk sur les interfaces –

MLS(config-vlan)#int f0/1
MLS(config-if)#switchport trunk encapsulation dot1q
MLS(config-if)#switchport mode trunk
MLS(config-if)#no shutdown
MLS(config-vlan)#int f0/2
MLS(config-if)#switchport trunk encapsulation dot1q
MLS(config-if)#switchport mode trunk
MLS(config-if)#no shutdown

– Ajout des adresses IPs aux VLANS –

MLS(config-if)#int vlan 10
MLS(config-if)#ip address 172.15.10.254 255.255.255.0
MLS(config-if)#no shutdown
MLS(config-if)#int vlan 20
MLS(config-if)#ip address 172.15.20.254 255.255.255.0
MLS(config-if)#no shutdown
MLS(config-if)#exit
MLS(config)#ip routing
```

Switchs 1 et 2 :

IOS Command Line Interface

```
Sw>en
Sw#conf t

– Ajout des VLANS –

MLS(config)#vlan 10
MLS(config-vlan)#vlan 20

– Configuration Trunk –

MLS(config-vlan)#int f0/3
MLS(config-if)#switchport mode trunk
MLS(config-if)#no shutdown

– Configuration des accès VLANS –

MLS(config-if)#int f0/2
MLS(config-if)#switchport mode access
MLS(config-if)#switchport access vlan 20
MLS(config-if)#no shutdown
MLS(config-if)#int f0/1
MLS(config-if)#switchport mode access
MLS(config-if)#switchport access vlan 10
MLS(config-if)#no shutdown
```

Sur les deux switchs, la configuration est la même car les PC des VLAN 10 et 20 sont dans les deux cas attribués sur les interfaces f0/1 et f0/2 pour faciliter la configuration.

Désormais il ne reste plus qu'à configurer l'ip des PC ainsi que la gateway en 172.15.x.254/24.

Tests de connectivité :

Désormais, nous allons effectuer des tests entre les VLANS ainsi qu'en leur sein pour vérifier si la configuration effectuée permet de ping toutes les machines.

Screenshots des différents ping effectués :

Nous effectuerons 2 pings par machine en prenant 2 équipements par exemple pour vérifier si elle peut atteindre le Switch Multilayer et communiquer avec l'autre VLAN.

PC 0 :

```
Pinging 172.15.10.254 with 32 bytes of data:

Reply from 172.15.10.254: bytes=32 time<1ms TTL=255
Reply from 172.15.10.254: bytes=32 time<1ms TTL=255
Reply from 172.15.10.254: bytes=32 time<1ms TTL=255
Reply from 172.15.10.254: bytes=32 time<1ms TTL=255

Ping statistics for 172.15.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.15.20.2

Pinging 172.15.20.2 with 32 bytes of data:

Request timed out.
Reply from 172.15.20.2: bytes=32 time<1ms TTL=127
Reply from 172.15.20.2: bytes=32 time<1ms TTL=127
Reply from 172.15.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.15.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Le ping est effectué avec succès du PC 0 jusqu'au switch multilayer sur la VLAN 1, la gateway est donc atteignable.

On peut également ping la VLAN 20 depuis le PC 0 ce qui prouve la connectivité entre les 2 VLANS.

PC 1 :

```
C:\>ping 172.15.10.254

Pinging 172.15.10.254 with 32 bytes of data:

Reply from 172.15.10.254: bytes=32 time<1ms TTL=255
Reply from 172.15.10.254: bytes=32 time<1ms TTL=255
Reply from 172.15.10.254: bytes=32 time<1ms TTL=255
Reply from 172.15.10.254: bytes=32 time<1ms TTL=255

Ping statistics for 172.15.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.15.10.2

Pinging 172.15.10.2 with 32 bytes of data:

Request timed out.
Reply from 172.15.10.2: bytes=32 time=1ms TTL=127
Reply from 172.15.10.2: bytes=32 time<1ms TTL=127
Reply from 172.15.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.15.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

On effectue des tests depuis le PC 1 faisant partie de la VLAN 2 pour vérifier si la connectivité entre les VLANS fonctionne correctement dans tout le réseau.

On remarque ici que l'on arrive à ping la gateway de la VLAN 10 ainsi que le PC 2 faisant partie de cette VLAN depuis le PC 1 qui est attribué à la VLAN 2.

Observation :

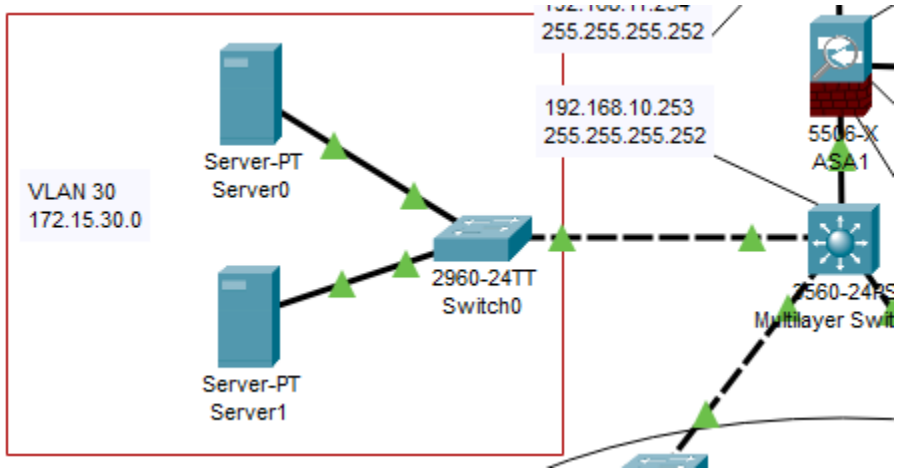
Pour permettre la connectivité des équipements en utilisant les VLANS, il faut définir un switch multilayer qui s'occupera d'effectuer la connectivité entre les différentes VLANS, si nous voulons effectuer un ping vers une machine appartenant à une autre VLAN, le paquet passera obligatoirement vers le switch multilayer pour ensuite rebrousser chemin jusqu'au destinataire.

On définit le mode trunk sur les interfaces entre switch/multilayer afin d'autoriser plusieurs VLANS à passer sur le même câble et on ajoute l'accès aux VLANS sur les interfaces switch/ordinateur pour assurer la connectivité.

Ajout du DHCP et de l'ASA

Configuration du serveur DHCP en VLAN :

Screenshot PacketTracer du serveur DHCP + l'ASA (Firewall) :



Nous allons configurer la VLAN 30 en dhcp, l'interface VLAN 30 du MLS aura pour adresse ip 172.15.30.254 et le serveur dns 172.15.30.2 qui sera situé dans la machine Server0. Nous allons donc configurer les interfaces de façon à activer le trunk/access afin de pouvoir communiquer avec les VLANS 10 et 20.

Nous allons définir une adresse ip sur le MLS en désactivant le switchport pour le relier à l'ASA sur le réseau 192.168.10.252/30.

Commandes de configuration des équipements :

Switch Multilayer :

IOS Command Line Interface

```
MLS>en
MLS#conf t

– Configuration IP sur MLS –

MLS(conf)#int f0/4
MLS(conf-if)#no switchport
MLS(conf-if)#ip add 192.168.10.253 255.255.255.252

– Configuration de la VLAN 30 et du DHCP –

MLS(conf-if)#int f0/3
MLS(conf-if)#switchport trunk encapsulation dot1q
MLS(conf-if)#switchport mode trunk
MLS(conf-if)#int vlan 30
MLS(conf-if)#ip add 172.15.30.254 255.255.255.0
MLS(conf-if)#ip helper-address 172.15.30.2
MLS(conf-if)#ex
MLS(conf)#ip dhcp excluded-address 172.15.30.254 172.15.30.2
MLS(conf)#ip dhcp pool VLAN30
MLS(dhcp-conf)#network 172.15.30.0 255.255.255.0
MLS(dhcp-conf)#dns-server 172.15.30.2
MLS(dhcp-conf)#default 172.15.30.254
MLS(dhcp-conf)#ex
MLS(cong)#ip name-server 172.15.30.2
```

Le trunk n'étant pas nécessaire ici car une seul VLAN circule sur cette interface, nous avons exclu les ip déjà utilisés et configuré le dhcp sur le réseau 172.15.30.0/24.

Switch 3 :

IOS Command Line Interface

```
Switch>en
Switch#conf t

– Configuration du DHCP pour les serveurs –

Switch(conf)#ip dhcp excluded-address 172.15.30.254 172.15.30.2
Switch(conf)#ip dhcp pool VLAN30
Switch(dhcp-conf)#network 172.15.30.0 255.255.255.0
Switch(dhcp-conf)#default 172.15.30.254
Switch(dhcp-conf)#dns-server 172.15.30.2

– Activation Trunk et accès VLANS –

Switch(dhcp-conf)#ex
Switch(cong)#ip name-server 172.15.30.2
Switch(conf)#vlan 30
Switch(conf-vlan)#vlan 10
Switch(conf-vlan)#vlan 20
Switch(conf-vlan)#int f0/3
Switch(conf-if)#switchport mode trunk
Switch(conf-if)#int 0/2
Switch(conf-if)#switchport mode access
Switch(conf-if)#switchport access vlan 30
Switch(conf-if)#int 0/1
Switch(conf-if)#switchport mode access
Switch(conf-if)#switchport access vlan 30
```

Sur le switch du serveur dhcp, nous avons configuré un pool dhcp afin de pouvoir attribuer une adresse ip de façon automatique sur le serveur dhcp de la VLAN 30.

Nous avons défini le serveur dhcp en 172.15.30.0 en excluant l'adresse ip 172.15.30.254 et .2 car sont sont les ip de l'interface VLAN 30 MLS ainsi que du serveur DNS.

Tests de connectivité :

Nous allons voir si la VLAN 30 configuré en dhcp peut être ping par les VLANS 10 et 20 réalisés précédemment et si nous pouvons atteindre le serveur dns avec le nom de domaine test.com.

Screenshots des différents ping effectués :

Nous effectuerons un ping depuis la VLAN 10 jusqu'au serveur dns pour vérifier si la configuration est correcte et par la même occasion, un ping depuis le VLAN 30 jusqu'à la VLAN 20 sera réalisé pour justifier le bon fonctionnement dans les deux sens.

On configure le dns 172.15.30.2 sur les ordinateurs du réseau 172.15.0.0/12 afin de pouvoir ping test.com.

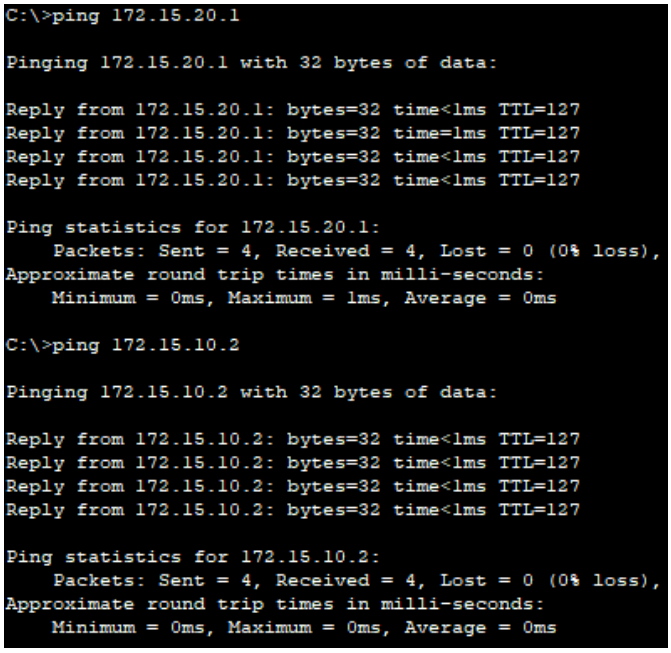
PC 0 :

```
C:\>ping test.com

Pinging 172.15.30.2 with 32 bytes of data:

Reply from 172.15.30.2: bytes=32 time<1ms TTL=127
Reply from 172.15.30.2: bytes=32 time<1ms TTL=127
Reply from 172.15.30.2: bytes=32 time<1ms TTL=127
Reply from 172.15.30.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.15.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>nslookup test.com

Server:  [172.15.30.2]
Address:  172.15.30.2

Non-authoritative answer:
Name:    test.com
Address:  172.15.30.2
```

L'ordinateur 0 sur le réseau 172.15.10.0 est capable de ping le serveur DNS.

Cela signifie que le switch multilayer est capable de rediriger les requêtes entre les différentes VLANS.

Serveur DHCP :



Le ping fonctionne bel et bien de la VLAN 30 jusqu'à la VLAN 20 et de même avec la VLAN 10.

La connectivité entre toutes les VLANS est donc prouvée et le dhcp configuré sur le serveur fonctionne parfaitement car elle attribue automatiquement son serveur dns ainsi que sa gateway.

Observation :

Afin de rendre le réseau plus simple, on aurait pu mettre les VLANS 10 et 20 en dhcp sur afin d'attribuer automatiquement le serveur dns 172.15.30.2 sur les machines au lieu de devoir le configurer manuellement. Nous avons configuré les ip-address ainsi que helper-address en 172.15.30.2 afin de rediriger les requêtes dns vers cette adresse ip.

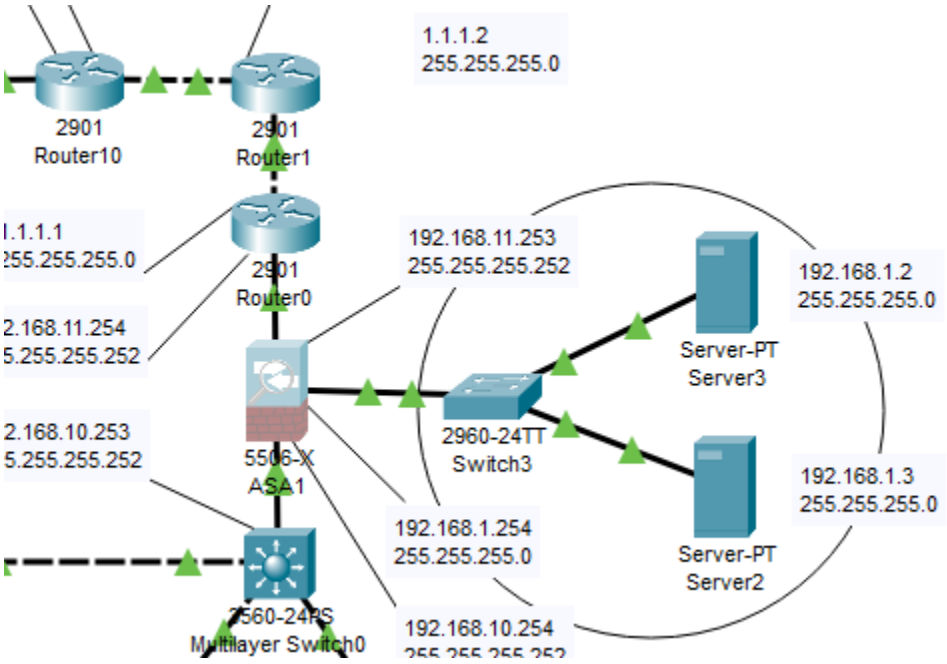
Les helper-address n'étant utiles que si nous définissons les ordinateurs en dhcp, dans le cas inverse, leur présence n'altère pas le fonctionnement du réseau.

En conclusion, la configuration réalisée nous permet de ping test.com et assure une bonne connectivité des équipements.

Ajout de la DMZ et du FAI :

Configuration pare-feu + routage externe :

Screenshot PacketTracer du serveur DMZ et des routeurs extérieurs :



Le serveur DMZ sera configuré sur l'adresse ip 192.168.1.0/24 et sera relié au Firewall qui lui-même assurera la connectivité avec les routeurs extérieurs (notamment la FAI) pour accéder à Internet.

Commandes de configuration des équipements :

Firewall ASA :

IOS Command Line Interface

```
ASA>en
ASA#conf t

– Configuration IP sur l'ASA –

ASA(conf)#int g1/1
ASA(conf-if)#ip add 192.168.10.254 255.255.255.252
ASA(conf-if)#nameif inside
ASA(conf-if)#int g1/2
ASA(conf-if)#ip add 192.168.11.253 255.255.255.252
ASA(conf-if)#nameif outside
ASA(conf-if)#int g1/3
ASA(conf-if)#ip add 192.168.1.254 255.255.255.0
ASA(conf-if)#nameif dmz
ASA(conf-if)#security-level 50
```

Nous avons commencé par configurer les adresses IPs sur les interfaces correspondantes ainsi que le security-level.

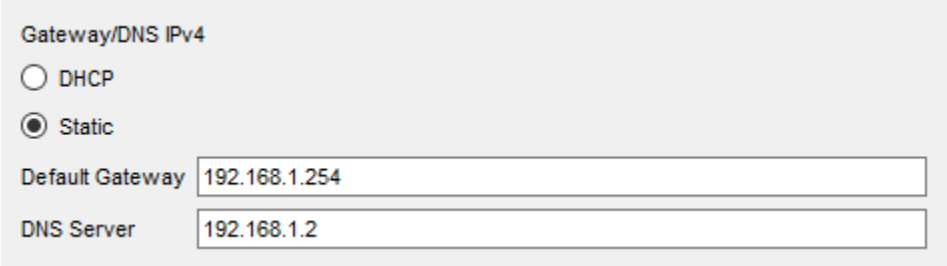
Les paquets passant dans le Firewall peuvent circuler d'un security-level plus élevé vers un plus faible. Dans le cas inverse, il faudra modifier le service global d'inspection du Firewall afin d'autoriser les paquets icmp à revenir vers la source. Cela nous permettra notamment de ping le réseau 192.168.1.0/24 depuis les VLANS 10, 20 et 30.

Par défaut, le security-level sur inside est défini à 100 et 0 sur l'outside.

Serveur DNS :

Config | INTERFACE FastEthernet0

Config | GLOBAL Settings



Services | SERVICES DNS

0	entreprise.com	A Record	192.168.1.2
1	entreprise.com	CNAME	www.entreprise.com
2	entreprise.com	NS	www.entreprise.com

On reproduit la même configuration sur l'autre serveur du réseau en changeant l'ip en 192.168.1.3 et sans configurer le paramètre dns.

Firewall ASA :

IOS Command Line Interface

```
– Configuration des routes –

ASA(conf)#route outside 0.0.0.0 0.0.0.0 192.168.11.254
ASA(conf)#route inside 172.15.0.0 255.255.0.0 195.168.10.253

– Configuration des ACL pour les ports 80 et 443 –

ASA(conf)#access-list OUTSIDE_DMZ extended permit tcp any any eq www
ASA(conf)#access-list OUTSIDE_DMZ extended permit tcp any any eq 443
ASA(conf)#access-list OUTSIDE_DMZ extended permit icmp any any

– Ajout de l'ACL sur l'interface extérieur de l'ASA –

ASA(conf)#access-group OUTSIDE_DMZ in interface outside

– Définition d'objet pour le réseau DMZ –

ASA(conf)#object network DMZ_WebServer
ASA(conf)#host 192.168.1.3
ASA(conf)#nat (dmz,outside) static 192.168.11.253
```

Avec ces commandes de configuration, on définit des routes pour assurer la connectivité du Firewall aux réseaux locaux et extérieurs.

Tous les paquets venant depuis l'extérieur du réseau doivent uniquement être de type icmp ou tcp sur les ports 80 et 443 pour passer le routeur d'entreprise. Dans le cas inverse, ces paquets seront rejetés.

Pour finir, on définit une classe d'objet en indiquant l'hôte du réseau ainsi que les interfaces affectées suivi de l'ip de l'interface d'où proviennent les paquets.

Firewall ASA :

IOS Command Line Interface

```
– Modification de la class-map / police –

ASA(conf)#class-map inspection_default
ASA(conf-cmap)#match default-inspection-traffic
ASA(conf-cmap)# exit
ASA(conf)#policy-map global_policy
ASA(conf-pmap)# class inspection_default
ASA(conf-pmap-c)#inspect icmp
ASA(conf-pmap-c)#ex
ASA(conf)#service-policy global_policy global
```

Désormais, lorsque l'on ping l'ip 192.168.1.3 depuis une ordinateur du réseau 172.15.0.0/12, on reçoit une réponse prouvant ainsi que le ping fonctionne correctement.

Même si on configure une ACL qui autorise les paquets du réseau 172.15.0.0/12 à passer, il faut modifier la police d'inspection des paquets afin d'autoriser les paquets icmp à revenir vers le source.

Il ne faut pas oublier de configurer des routes depuis le MLS afin d'assurer la connectivité avec le Firewall et la DMZ.

On les ajoute de la forme suivante :

```
MLS(conf)#ip route 192.168.1.0 255.255.255.0 192.168.10.254
MLS(conf)#ip route 192.168.10.0 255.255.255.252 f0/4
```

Router 0 :

IOS Command Line Interface

```
– Configuration NAT dynamique –

Router(conf)#access-list 1 permit 172.15.0.0 0.0.255.255
Router(conf)#access-list 1 deny any
Router(conf)#ip nat inside source list 1 interface g0/1 overload

– Configuration des routes –

Router(conf)#ip route 1.1.2.128 255.255.255.252 1.1.1.2
Router(conf)#ip route 8.8.0.0 255.255.0.0 1.1.2.129
Router(conf)#ip route 192.168.10.252 255.255.255.252 192.168.11.253
Router(conf)#ip route 192.168.1.0 255.255.255.0 192.168.11.253
Router(conf)#ip route 172.15.0.0 255.255.0.0 192.168.10.253

– Configuration des IPs sur les interfaces –

Router(conf)#int g0/0
Router(conf-if)#ip add 192.168.11.254 255.255.255.252
Router(conf-if)#int g0/1
Router(conf-if)#ip add 1.1.1.1 255.255.255.0
```

Nous autorisons les paquets provenant du réseau local 172.15.0.0/12 à sortir par le routeur d'entreprise. On configure un NAT dynamique afin de changer l'ip du réseau local en ip de l'interface pour qu'elle puisse être reconnue dans le réseau global.

Des routes statiques sont configurées afin d'assurer la connectivité du routeur avec le réseau intérieur ainsi que les routeurs extérieurs.

Pour les configurer, on définit l'ip du réseau auquel on veut accéder, le masque du réseau en question, et l'ip de l'interface vers laquelle on y accède.

Nous avons configuré les adresses IP des routeurs en statiques afin de ne pas altérer les routes configurées entre les routeurs.

Pour configurer les ips en eigrp on peut exécuter les commandes de la forme suivante :

```
#router eigrp x (x nombre entier naturel > 0 )
#network x.x.x.x 0.0.0.255
```

Observation :

Le Firewall a pour objectif d'empêcher les paquets extérieurs d'accéder à la DMZ s' ils ne sont pas de type icmp ou tcp.

Le réseau local lui peut ping l'extérieur en changeant temporairement son IP pour que le réseau extérieur puisse reconnaître la source.

Dû à cette configuration réalisée, on peut désormais ping le routeur d'entreprise via un ordinateur des VLANS 10 et 20 mais cela ne fonctionne pas dans le sens inverse tout simple grâce au security-level défini dans le Firewall.

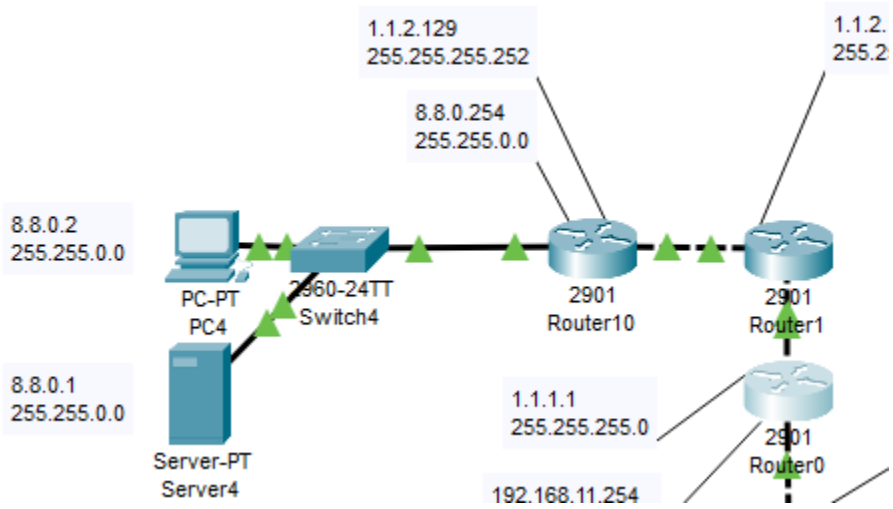
Cependant, nous avons remarqué une anomalie avec le service global d'inspection du Firewall car lorsque l'on redémarre le fichier .pkt, la configuration change automatiquement pour s'adapter. Mais après modification, le ping de la DMZ depuis le réseau local ne fonctionne plus.

Pour assurer le bon fonctionnement du réseau, nous devons donc à chaque fois reconfigurer entièrement la police d'inspection des paquets pour laisser les paquets icmp revenir à la source.

Ajout du réseau public et de l'interconnexion :

Configuration du réseau statique / FAI :

Screenshot PacketTracer des routeurs extérieurs :



Les configurations réalisées seront effectuées en statique car on part du principe qu'elles seront gérés par le fournisseur d'internet (FAI).

On définit une adresse IP sur chaque interface ainsi que des routes statiques pour pouvoir ping n'importe quel routeur depuis n'importe quelle machine.

Commandes de configuration des équipements :

Router 1 :

IOS Command Line Interface

```
Router(conf)#int g0/0
Router(conf-if)#ip add 1.1.2.130 255.255.255.252
Router(conf-if)#int g0/1
Router(conf-if)#ip add 1.1.1.2 255.255.255.252
Router(conf-if)#ex
Router(conf)#ip route 8.8.0.0 255.255.0.0 1.1.2.129
Router(conf)#ip route 192.168.1.0 255.255.255.0 192.168.11.253
Router(conf)#ip route 192.168.11.252 255.255.255.252 1.1.1.1
```

Router 10 :

IOS Command Line Interface

```
Router(conf)#int g0/0
Router(conf-if)#ip add 8.8.0.254 255.255.0.0
Router(conf-if)#int g0/1
Router(conf-if)#ip add 1.1.2.129 255.255.255.252
Router(conf-if)#ex
Router(conf)#ip route 1.1.1.0 255.255.255.0 1.1.2.130
Router(conf)#ip route 192.168.1.0 255.255.255.0 192.168.11.253
Router(conf)#ip route 192.168.11.252 255.255.255.252 1.1.1.1
```

On configure l'adresse IP 8.8.0.2/12 sur l'ordinateur ainsi que 8.8.0.1/12 sur le serveur externe et on peut désormais effectuer des tests de connectivité au sein de notre topologie.

Tests finaux de connectivité :

Nous allons effectuer un ping depuis les VLANS du réseau local vers l'extérieur pour vérifier si le NAT dynamique fonctionne correctement et nous testerons également de ping la DMZ.

PC 1 :

```
C:\>ping 8.8.0.2

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=1ms TTL=123
Reply from 8.8.0.2: bytes=32 time<1ms 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 = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

On remarque que l'on arrive à ping l'ordinateur du serveur extérieur depuis la VLAN 20 en 172.15.20.0/24.

De plus, la DMZ sur le réseau 192.168.1.0/24 est également accessible.

Cela prouve donc que l'on peut traduire les adresses ip du réseau local et que l'on peut ping l'extérieur.

Nous allons maintenant effectuer un test de connexion depuis l'extérieur entre les routeurs pour assurer leur connectivité et nous vérifierons que le réseau local 172.15.0.0/12 est inaccessible pour les machines sur le réseau extérieur.

PC 4 :

```
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=124
Reply from 192.168.1.2: bytes=32 time<1ms TTL=124
Reply from 192.168.1.2: bytes=32 time=2ms TTL=124
Reply from 192.168.1.2: bytes=32 time<1ms TTL=124

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:

Reply from 1.1.1.1: bytes=32 time<1ms TTL=253
Reply from 1.1.1.1: bytes=32 time=1ms TTL=253
Reply from 1.1.1.1: bytes=32 time<1ms TTL=253
Reply from 1.1.1.1: bytes=32 time<1ms TTL=253

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 172.1.10.1

Pinging 172.1.10.1 with 32 bytes of data:

Reply from 8.8.0.254: Destination host unreachable.
```

Le ping fonctionne sur le routeur extérieur notamment avec l'ip 1.1.1.1 prouvant ainsi la connectivité des équipements extérieurs.

Si l'on effectue un ping vers la zone démilitarisée nommée DMZ, on voit bien que le ping passe à travers le Firewall.

Cependant, si l'on veut ping le réseau local 172.15.0.0/12, le Firewall empêche l'accès tout simplement dû au security-level plus élevé.

Conclusion :

Cette SAE nous a permis de découvrir la configuration d'un Firewall qui est un élément essentiel pour le réseau en entreprise. On a pu simuler un serveur interne uniquement pour les clients locaux et un serveur DMZ accessible depuis l'extérieur.

Pour améliorer notre configuration, on pourrait faire en sorte de ping le nom de domaine entreprise.com depuis l'extérieur du réseau au lieu de ping l'ip de ce nom de domaine 192.168.1.2. Cependant, le nom de domaine est uniquement reconnu dans la DMZ et cela nécessite une configuration plus aboutie pour permettre au nom de domaine d'être reconnu.