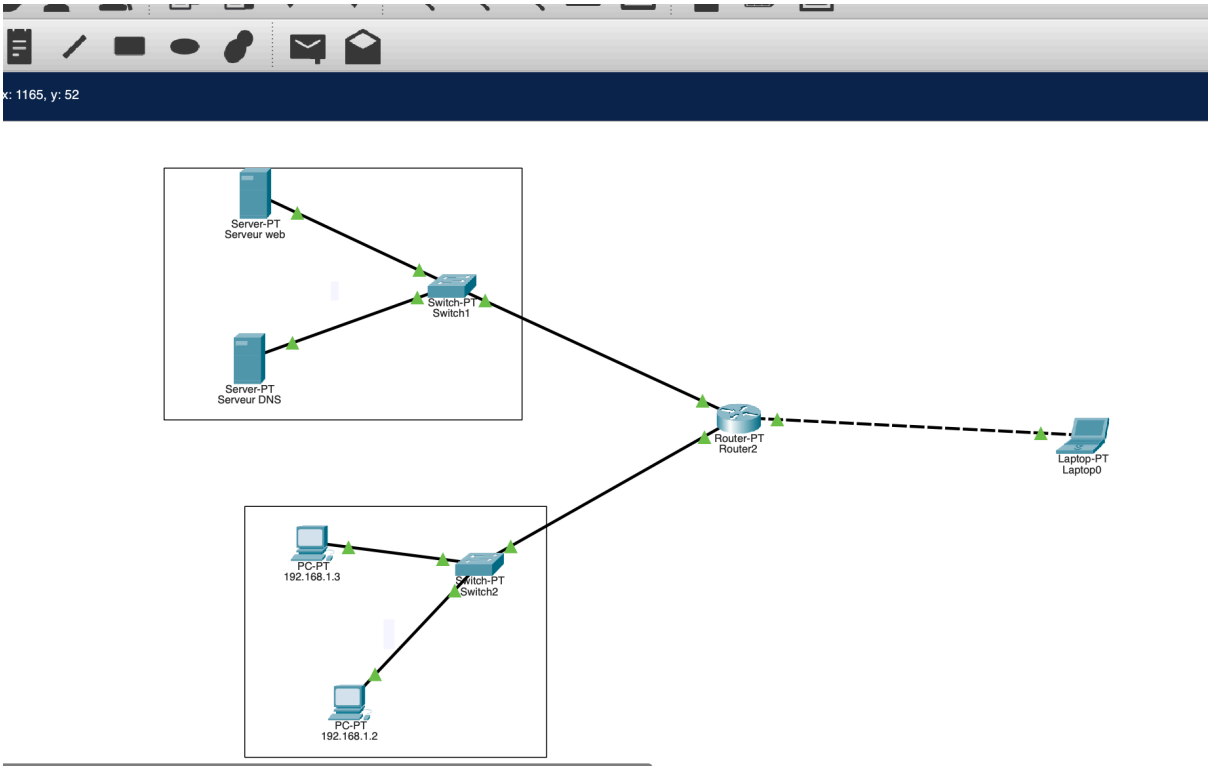
TP 4 bis - Sécurité réseaux

Logan TANN / Jean-Louis CHEN / LSI 1

Configuration du réseau

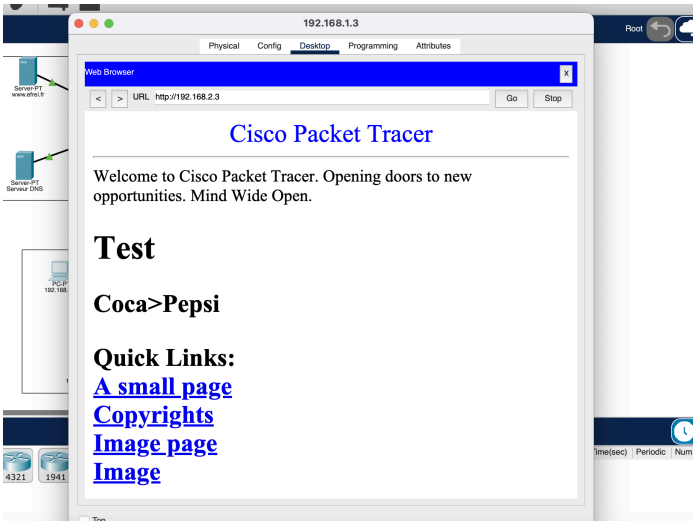
Nous avons configuré comme suit notre cisco packet tracer : une DMZ dans le sous réseau 192.168.2.X et un LAN dans 192.168.1.X



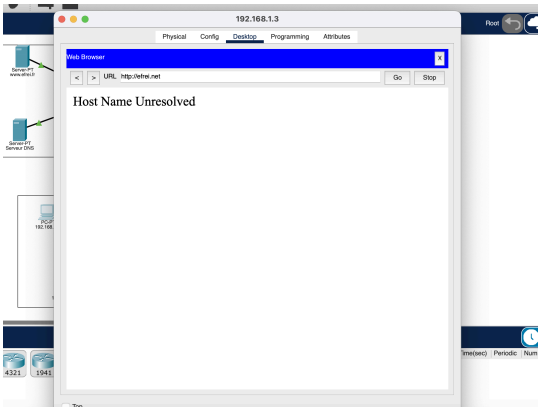
En plus des IPs, il ne faut pas oublier de configurer les gateways et aussi le serveur DNS pour la suite.

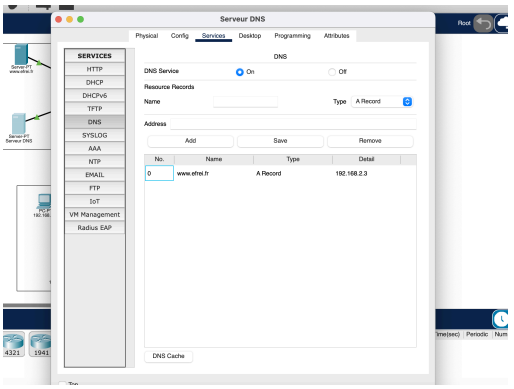
Serveur HTTP

Dans la configuration du serveur HTTP, on modifie le fichier index.html (coca > pepsi). En tapant l'adresse IP du serveur, nous obtenons le résultat suivant :



Lorsque nous tapons www.efrei.fr, nous n'avons pas la page web. C'est normal, car il faut associer le nom de domaine à l'IP de notre serveur web. Crééons un record A.





On remarque que ça fonctionne.

ACL

Permettre aux machines du LAN de pinger celles de la DMZ

Puisque lorsque nous crééons une ACL, la règle par défaut est DENY ALL, alors il suffit de créer les deux règles suivantes :

- Autoriser le ping echo du LAN vers la DMZ :
  OUT : access-list 103 permit icmp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 echo
- Autoriser le ping echo-reply de la DMZ vers la LAN
  IN : access-list 102 permit icmp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 echo-reply

```
Router(config)#access-list 101 permit icmp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config)#access-list 102 deny icmp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 echo

Router(config)#interf f0/0
Router(config-if)#ip access-group 102 out
Router(config-if)#ip access-group 101 in
```

Ping du LAN vers la DMZ : fonctionne

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time=33ms TTL=127

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 33ms, Average = 8ms
```

Ping de la DMZ vers le LAN : ne fonctionne pas (Ne pas ping l'IP du routeur 192.168.1.1, nous avons perdu plus d'une heure à cause de ça.)

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
```

Vérifier les accès

Source	→	Destination	Peut pinger ?
DMZ	→	DMZ	OUI
DMZ	→	Routeur	OUI
DMZ	→	LAN	NON
DMZ	→	EXT	OUI
LAN	→	DMZ	OUI
LAN	→	Routeur	NON
LAN	→	LAN	NON
LAN	→	EXT	NON
EXT	→	DMZ	OUI
EXT	→	Routeur	OUI
EXT	→	LAN	NON

Empêcher les machines ayant une IP impaire d'accéder au serveur DNS

Nombre impair : l'IP doit avoir le dernier bit à 1. Donc le masque pour la règle DENY est 0.0.0.254 avec correspondance sur le dernier bit (x.x.x.1).

```
access-list 104 deny udp 192.168.1.1 0.0.0.254 192.168.2.2 eq domain
```

Autoriser uniquement le HTTP depuis le LAN vers la DMZ

Nous nous inspirons de la commande précédente pour autoriser le http.
Il faut ajouter cette règle sur l'interface du routeur côté LAN en IN.

```
access-list 105 permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 80
```

Les machines du DMZ ne doivent pouvoir initier aucune connexion

Empêcher d'initier une connexion : bloquer IP.
Il faut ajouter cette règle sur l'interface du routeur côté DMZ en IN.

```
access-list 106 deny ip 192.168.2.0 0.0.0.255 any
```