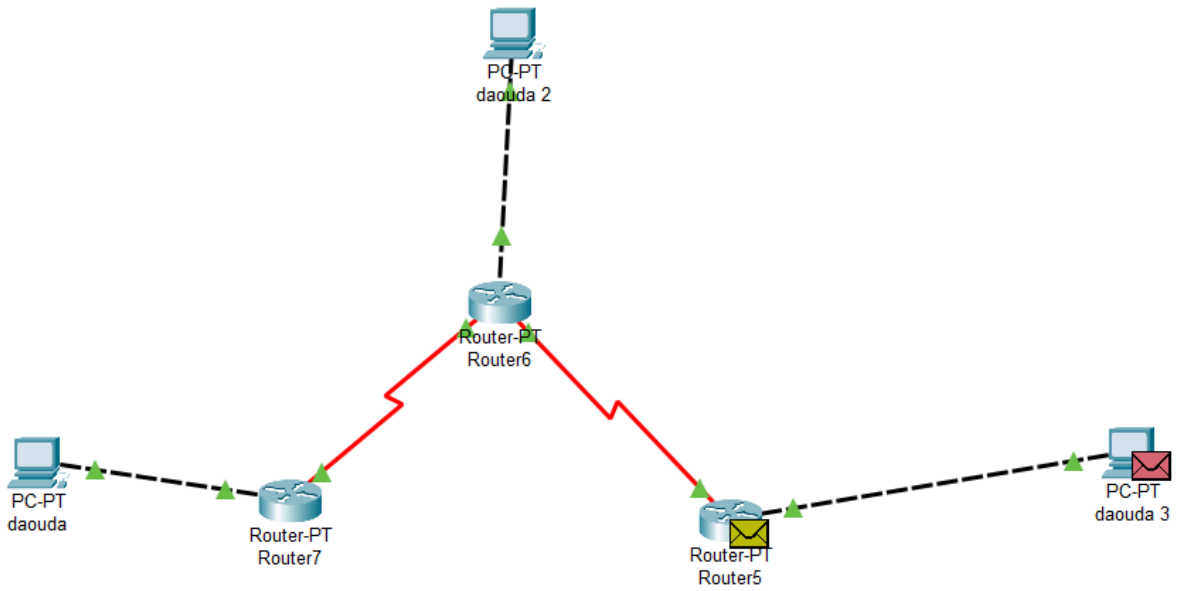
Rapport TP ACL Par Daouda David Coulibaly (IRIC1)

Introduction:

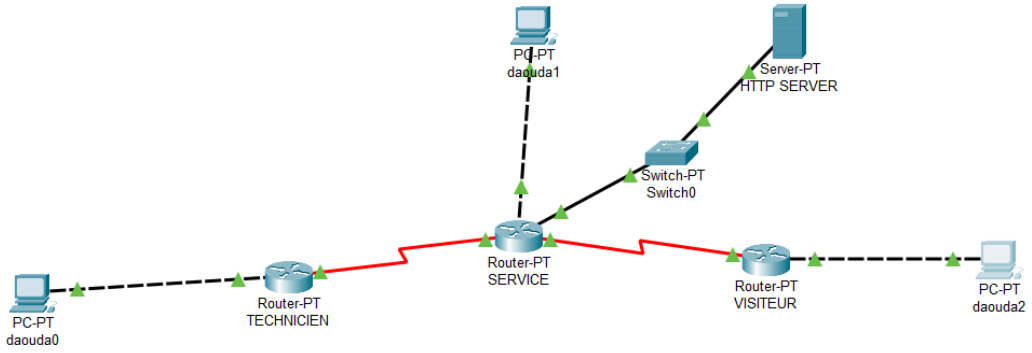
Bienvenue dans ce TP sur les listes de contrôle d'accès (ACL) avec Packet Tracer. Au cours de cet exercice, nous explorerons comment configurer et appliquer des ACL pour contrôler le flux de trafic sur les équipements réseau. Vous apprendrez à restreindre l'accès aux ressources en fonction des adresses IP, des protocoles et des ports. Préparez-vous à acquérir des compétences pratiques en sécurité réseau et à découvrir l'impact des ACL sur la gestion du trafic dans un environnement simulé.



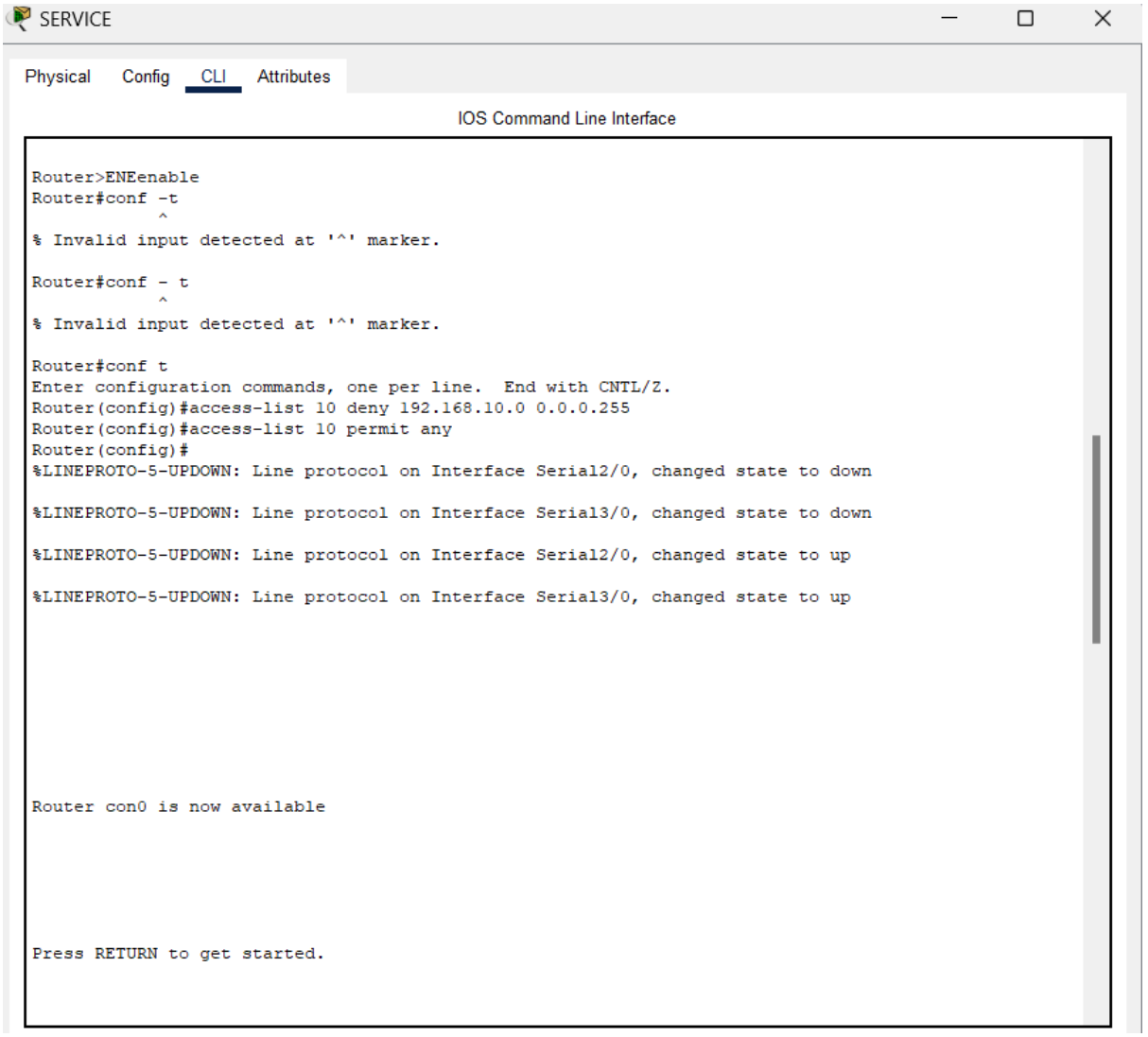
Premiere partie:

Objectif : On veut interdire le trafic des paquets du réseau Visiteur (192.168.10.0/24) au réseau Technicien (192.168.30.0/24). Les adresses des liens sont 192.168.40.0/24 entre les routeurs TECH et SERV et 192.168.50.0/24 entre les

routeurs SERV et VST.



- Application de l'ACL via le CLI du routeur visiteur.




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

Router(config-if)#interface Se2/0
Router(config-if)#ip access-group  10 out
Router(config-if)#
```

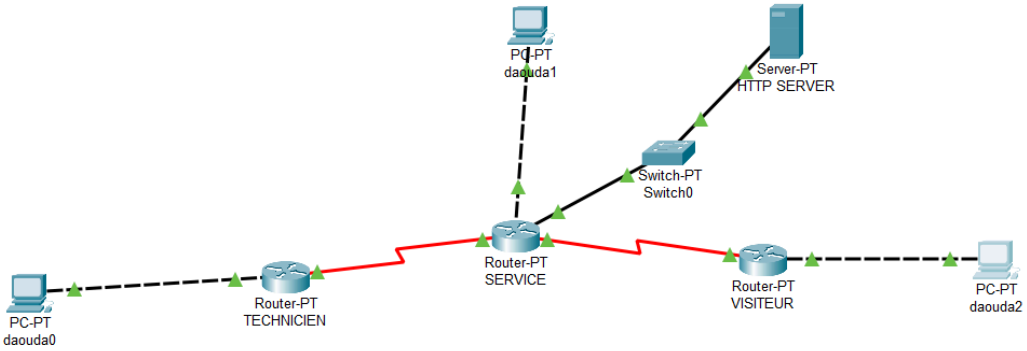
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	D
	Failed	HTTP...	daouda2	ICMP		0.000	N	16	(edit)	
	Failed	daouda2	daouda0	ICMP		0.000	N	17	(edit)	
	Successful	daouda2	daouda1	ICMP		0.000	N	18	(edit)	

- **On remarque que daouda 2 a pu se connecter a daouda 0 mais mais pas daouda 1 car l'acces lui a ete refuser par L'ACL**

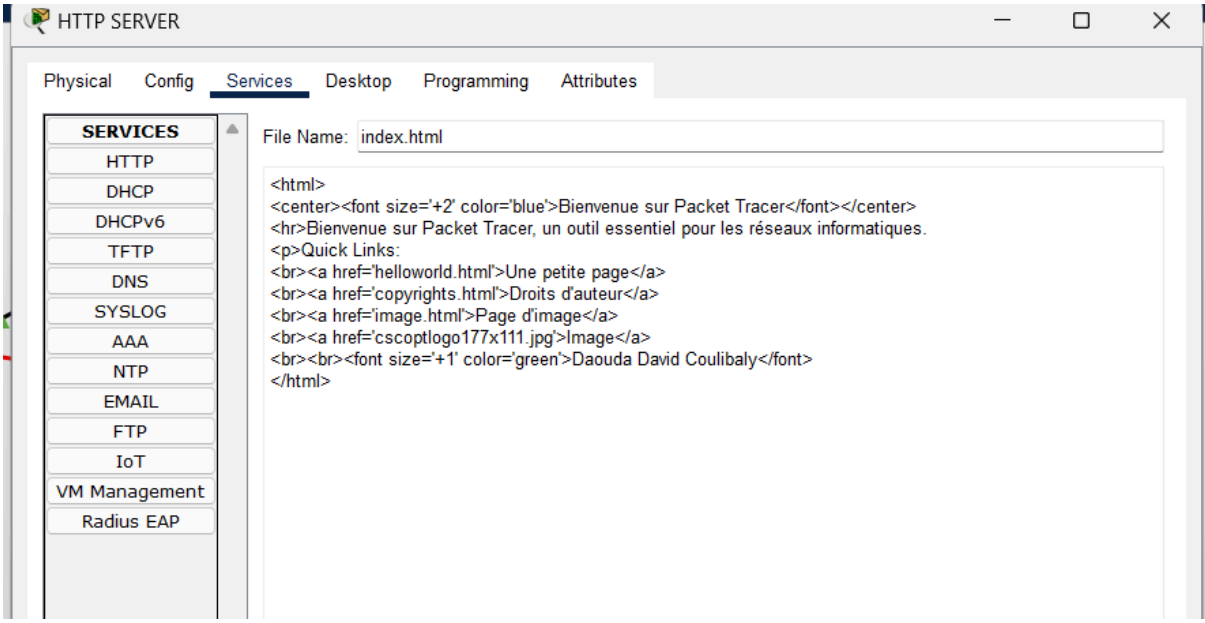
Deuxième partie:

Objectif : On veut interdire l'accés web d'un terminal du LAN VISITEUR au serveur HTTP branché au LAN SERVICE. On suppose l'adresse IP du serveur HTTP est 192.168.20.11 et celle du hôte qu'on veut lui interdire l'accès web est 192.168.10.10

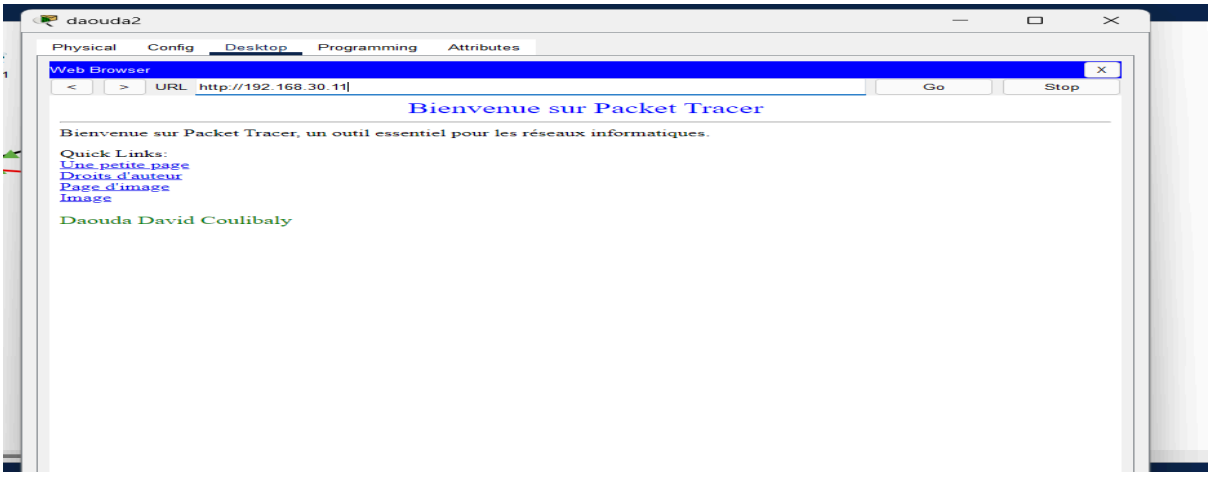
- **Considerons maintenant le serveur HTTP dans la typologie**



- **configurons la page HTML du serveur HTTP**

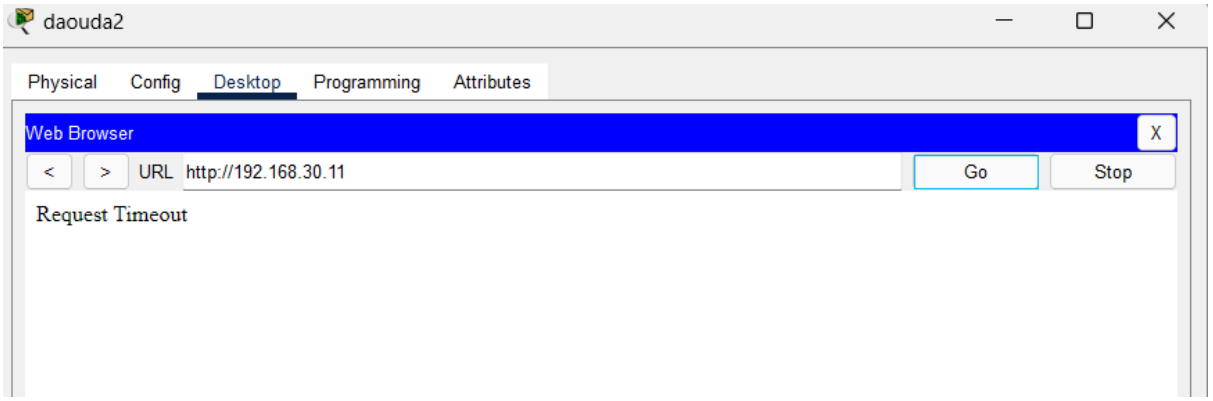


- **Visualisons la page HTTP via Daouda 2**



- **Maintenant usons de L'ACL pour lui interdire L'acces:**

```
Router(config)#access-list 111 deny tcp host 192.168.10.2 host 192.168.30.11 eq www
Router(config)#access-list 111 permit ip any any
Router(config)#interface Se2/0
Router(config-if)#ip access-group 111 out
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
```

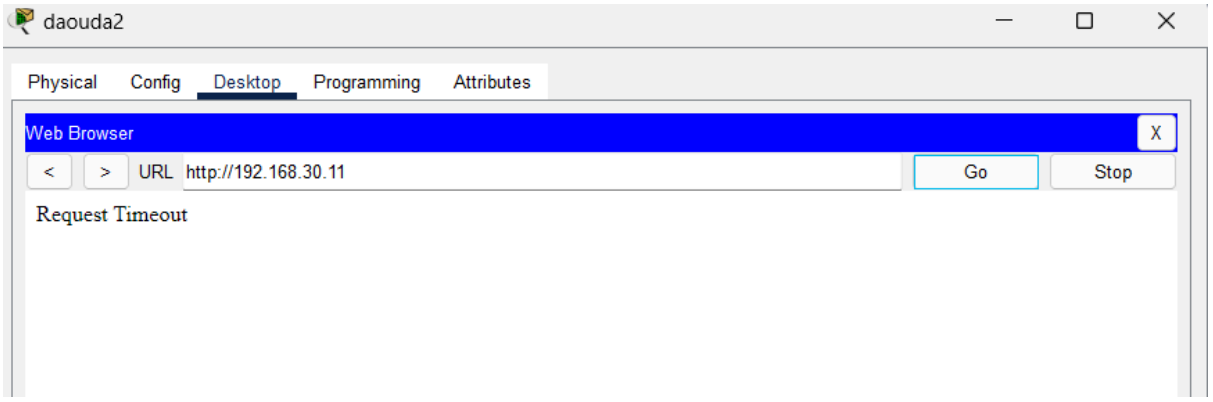


Troisieme partie:

Objectif : On veut interdire l'acces web d'un terminal du LAN Visiteur au serveur HTTP branché au LAN Service. On suppose l'adresse IP du serveur HTTP est 192.168.20.11 et celle du hôte qu'on veut lui interdire l'accès web est 192.168.10.10.

- **On procede de la mme facon que pour la deuxieme partie**

```
Router(config)#access-list 111 deny tcp host 192.168.10.2 host 192.168.30.11 eq www
Router(config)#access-list 111 permit ip any any
Router(config)#interface Se2/0
Router(config-if)#ip access-group 111 out
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
```



- **Utilisation de la commande Show ACL**

```
Router#show access-list lll
Extended IP access list lll
    deny tcp host 192.168.10.2 host 192.168.30.11 eq www (12 match(es))
    permit ip any any

Router#
```

Conclusion:

Bienvenue dans ce TP sur les listes de contrôle d'accès (ACL) avec Packet Tracer. Au cours de cet exercice, vous avez appris à configurer et à appliquer des ACL pour contrôler le flux de trafic sur les équipements réseau. En utilisant des adresses IP, des protocoles et des ports, vous avez restreint l'accès aux ressources réseau. Félicitations pour avoir acquis des compétences pratiques en sécurité réseau et pour avoir compris l'impact des ACL sur la gestion du trafic dans un environnement simulé. Continuez à explorer et à pratiquer pour renforcer vos connaissances dans ce domaine crucial de la gestion réseau.