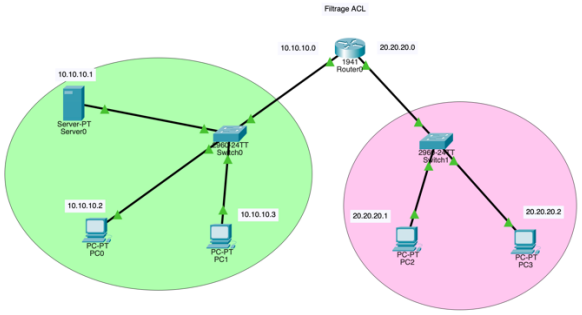
Filtrage ACL sur Cisco Packet Tracer

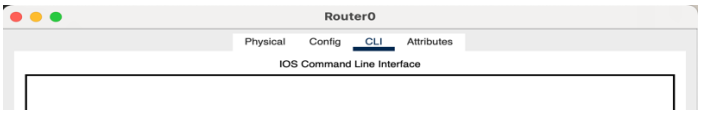
Une **ACL (Access Control List)** est un outil de sécurité réseau utilisé pour filtrer le trafic entrant ou sortant sur les interfaces d'un routeur. Elle permet de contrôler quels paquets sont autorisés ou bloqués en fonction de critères comme l'adresse IP source ou destination, le protocole utilisé (TCP, UDP, ICMP), ou encore le numéro de port. Les ACL sont essentielles pour renforcer la sécurité du réseau et limiter l'accès aux ressources sensibles.
Dans **Cisco Packet Tracer**, le filtrage par ACL est configuré sur les routeurs pour simuler des politiques de sécurité. On peut créer des **ACL standard**, qui filtrent uniquement selon l'adresse IP source, ou des **ACL étendues**, qui offrent un filtrage plus précis basé sur l'adresse source et destination, les protocoles, et les ports. Une fois définie, une ACL est appliquée à une interface dans une direction spécifique (*inbound* ou *outbound*), ce qui détermine à quel moment le trafic est filtré.
L'utilisation du filtrage ACL dans Cisco Packet Tracer permet de simuler un réseau sécurisé où l'accès aux services et aux segments du réseau peut être strictement contrôlé. Cela aide à mieux comprendre comment les pare-feux et les règles de filtrage fonctionnent dans un environnement réel, tout en illustrant l'importance de la sécurité dans la conception d'une infrastructure réseau.

Infrastructure



Cliquer sur le poste « PC3 », aller dans « Desktop », appuyer sur « Web Browser », puis marquer l'adresse IP sur serveur WEB 10.10.10.1 :

Aller dans le « Router0 », puis dans le « CLI » :

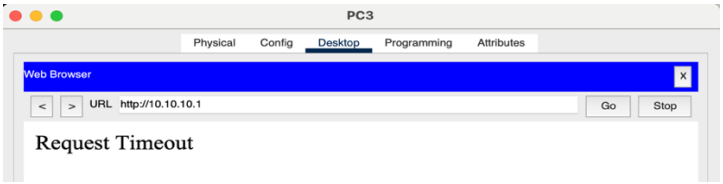


Puis marquer ces commandes pour restreindre l'accès et les communications au sein du réseau au poste « PC3 » (20.20.20.2) mais accorder aux autres un accès total :
CMD : enable
CMD : conf t
CMD : access-list ?
CMD : access-list 10 deny 20.20.20.2
CMD : access-list 10 permit any
CMD : int gigabitEthernet0/1
CMD : ip access-group 10 in
CMD : exit
CMD : exit

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
Router(config)#access-list 10 deny 20.20.20.2
Router(config)#access-list 10 permit any
Router(config)#
Router(config)#int gigabitEthernet0/1
Router(config-if)#ip access-group 10 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Tester que le poste « PC3 » n'a plus accès au serveur WEB :



Tester qu'un autre poste, par exemple le poste « PC2 » que lui a bien accès au serveur WEB :