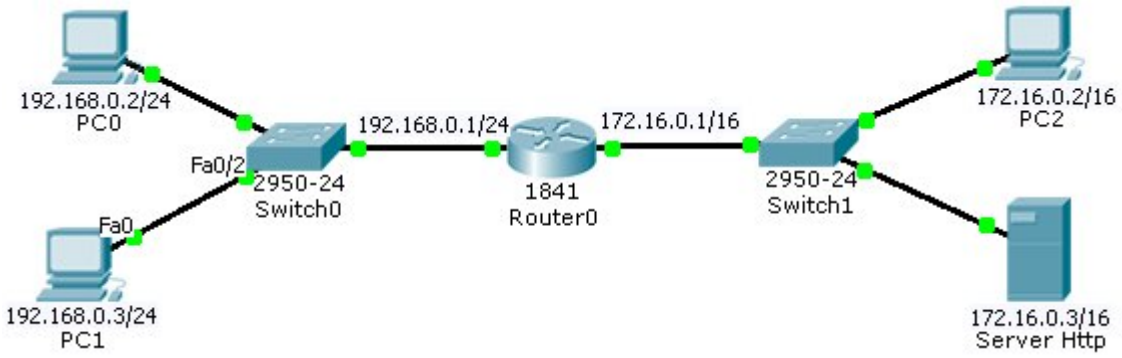
Centre Universitaire de Mila
departement MI
Master I I2A

TP 1: les ACLs

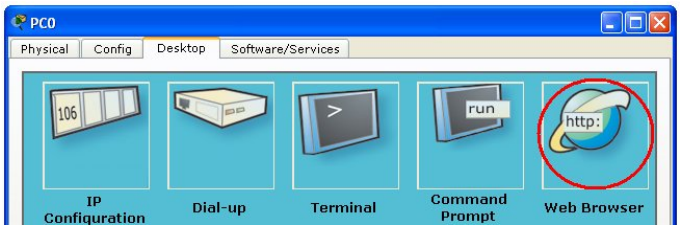
Exercice 1 : (Configuration de listes de contrôle d'accès standard)

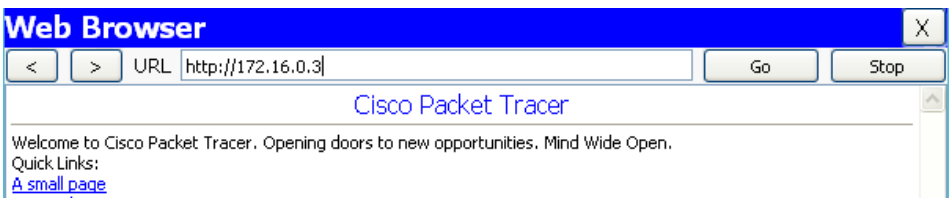
Soit le montage suivant :



A l'issue de ce TP, vous devez effectuer les tâches suivantes :

1. Configurer les adresses IP des machines.
2. Configurer les interfaces du routeur reliant les deux sous-réseaux.
3. Testez la connexion entre les différentes machines en utilisant la commande ***ping***.
4. Vérifier la connectivité avec le « ***serveur Http*** ». D'abord en utilisant la commande ***ping***, puis en accédant à une page web hébergée sur ce serveur.





5. Créer une *liste de contrôle d'accès standard* qui interdira l'accès au réseau 172.16.0.0/16 depuis le réseau 192.168.0.0/24.

```
Router(config)#access-list 10 deny 192.168.0.0 0.0.0.255
Router(config)#access-list 10 permit any
```

6. A quoi sert la deuxième instruction de la question (5.) ?
7. Essayez d'accéder au réseau 172.16.0.0/16 en envoyant des requêtes ***ping*** depuis le réseau 192.168.0.0/24. Ces requêtes *ping* ont-elles réussi ?
8. Appliquez l'ACL créée à la question (5.) à l'interface connectée au sous-réseau 172.16.0.0/16.

```
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip access-group 10 out
```

9. Reprendre la question (7.). Ces requêtes *ping* ont-elles réussi ?
10. Essayez d'accéder à la page Web hébergée sur le « ***serveur Http*** » depuis les machines **PC0**, **PC1** et **PC2**. Depuis quelles machines peut-on accéder au « ***serveur Http*** ».
11. Utilisez la commande **`#show access-lists`** pour afficher les ACLs créées sur le routeur.
12. Vérifier si l'ACL est bien Appliquée sur l'interface concernée. (*s'il s'agit par exemple de l'interface f0/1*) :

```
Router#show ip interface f0/1

...
Outgoing access list is 10
Inbound  access list is not set
```

13. Supprimer l'ACL 10 du routeur. (**`Router(config)#no access-list 10`**).
14. Désactiver l'ACL 10 de l'interface du routeur :

```
Router (config)#interface fastethernet 0/1
Router (config-if)#no ip access-group 10 out
```

<u>Exercice 2 :</u> (Configuration des ACLs standards nommées)

Refaire toutes les questions de l'***Exercice 1*** en utilisant les ACLs standards nommées.

```
Router(config)#ip access-list standard monACL_sd
Router(config-std-nacl)#deny 192.168.0.0 0.0.0.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#int f0/1
Router(config-if)#ip access-group monACL_sd out
Router(config-if)#end
Router#show ip interface f0/1
...
Outgoing access list is monACL_sd
Inbound  access list is not set
```

Exercice 3 : (Configuration de listes de contrôle d'accès étendues)

Complétons la configuration du réseau illustré sur la figure de l'***Exercice 1***. L'objectif de cet exercice sera de configurer des ACLs étendue pour filtrer le trafic sur le routeur.

1. Effacer les ACLs créées précédemment sur le routeur.
2. Vérifier qu'aucune ACL n'est appliquée aux interfaces du routeur.
3. En utilisant les requêtes ***ping***, essayez la connectivité entre les différentes machines du réseau.
4. Vérifier l'accès au « ***serveur http*** » depuis le réseau 192.168.0.0/24.
5. Ecrire une ACL étendue qui n'autorise que la machine PC0 d'accéder aux pages web hébergées sur le ***serveur Http***.
6. Etablir une ACL étendue qui n'autorise que les machines du réseau 172.16.0.0/16 de pinger (protocole ***icmp***) les autres réseaux, et d'interdire les autres réseaux d'envoyer des requêtes *ping* aux machines ce réseau (utiliser l'option **`echo-replay`** du protocole ***icmp***).
7. Attribuer cette ACL à une interface du routeur selon le sens du trafic.
8. Proposer une ACL qui n'autorise qu'aux machines du réseau 172.16.0.0/16 d'ouvrir des sessions Telnet (port **23**), et qui interdit l'ouverture de session Telnet vers les machines de ce réseau.
9. Afficher les ACLs configurées sur le routeur.

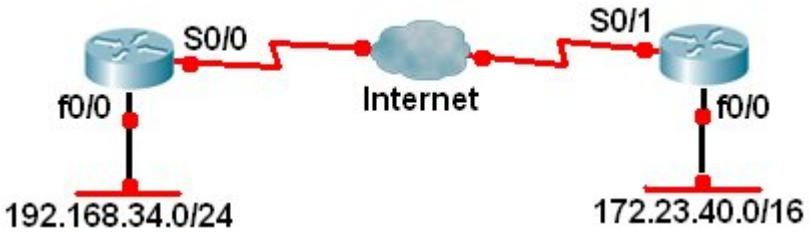
```
Router#show access-lists
Ou
Router#show running-config
```

Exercice 4 : (Configuration de listes de contrôle d'accès étendues nommées)

Effacer toutes les ACLs configurées sur le routeur, puis refaire toutes les questions de l'***Exercice 3*** en utilisant les ACLs étendues nommées.

Exercice 5 :

Soit le réseau suivant :



Sur le réseau interne 192.168.34.0/24. La machine 192.168.34.2 ne doit pas être accessible de l'extérieur.

1. Quelle ACL doit-on choisir :
   a. `access-list 101 deny tcp any host 192.168.34.2`
   b. `access-list 101 deny ip any 192.168.34.0 0.0.0.255`
   c. `access-list 101 deny ip any 192.168.34.2 255.255.255.255`
   d. `access-list 101 deny ip any host 192.168.34.2`
2. A quelle interface doit-on la définir ? Expliquer ?
   a. Sur l'interface S0/0 in
   b. Sur l'interface Fa0/0 in
   c. Sur l'interface S0/0 out
   d. Sur l'interface Fa0/0 out
3. Nous voulons restreindre tout accès SMTP (port 25) à la machine 192.168.34.200.
   A. Quelle ligne d'ACL doit-on choisir ?
      a. `access-list 101 permit tcp any host 192.168.34.200 eq 25`
      b. `access-list 101 deny tcp any 192.168.34.0 0.0.0.255 eq 25`
      c. `access-list 101 permit tcp host 192.168.34.200 any eq 25`
      d. `access-list 101 deny tcp any 192.168.34.200 0.0.0.255 eq 25`
   B. A quelle interface doit-on la définir ?
   C. Ecrire les commandes nécessaires pour positionner cette ACL à l'interface que vous avez choisie.
4. Supposons que la liste de contrôle d'accès suivante soit correctement appliquée à une interface de routeur,

```
Router(config)# access-list 165 deny tcp 192.168.34.0 0.0.0.255
172.23.0.0 0.0.255.255 eq telnet
Router(config)# access-list 165 permit ip any any
```

   a. Que fait-elle cette ACL?
   b. Expliquer le choix des masques génériques?