

# TP9 - Mise en place d'ACLs

---

## IV/ Configuration des interfaces des routeurs

**En vous référant à la table d'adressage, configurer les interfaces des routeurs en leur attribuant une adresse IP, un masque et en les activant**

**Question : Donner les commandes qui vous ont permis de configurer les interfaces des routeur**

R1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip address 10.1.0.1 255.255.0.0
R1(config-if)#NO SHUTDOWN

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R1(config-if)#exit
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

R2

```
R2(config)#interface GigabitEthernet0/0
R2(config-if)#no ip address
R2(config-if)#ip address 10.1.0.2 255.0.0.0
R2(config-if)#ip address 10.1.0.2 255.255.0.0
R2(config-if)#
R2(config-if)#exit
R2(config)#interface GigabitEthernet0/1
R2(config-if)#ip address 172.16.1.1 255.255.0.0
R2(config-if)#ip address 172.16.1.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R2(config-if)#exit
R2(config)#interface GigabitEthernet0/0
R2(config-if)#no shutdown
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R2(config-if)#exit
R2(config)#interface GigabitEthernet0/2
R2(config-if)#ip address 172.168.2.1 255.255.0.0
R2(config-if)#ip address 172.168.2.1 255.255.255.0
R2(config-if)#no shutdown
```

## V/ Configuration des terminaux

PC1

```
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2E0:F7FF:FE0A:A466
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.253
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                     192.168.1.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                     0.0.0.0
```

PC2

```
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::202:16FF:FEA7:CB9A
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.254
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                     192.168.1.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                     0.0.0.0
```

Serv1

```
Physical  Config  Services  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer SERVER Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::20A:F3FF:FE90:E44D
IPv6 Address.....: ::
IPv4 Address.....: 172.16.1.254
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                        172.16.1.1
```

Serv2

```
Physical  Config  Services  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer SERVER Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::2D0:97FF:FE73:5381
IPv6 Address.....: ::
IPv4 Address.....: 172.16.2.254
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                        172.16.2.1
```

**Question : Dans la configuration actuelle, un ping partant de PC1 peut-il arriver à PC2? Pourquoi ?**

Oui dans la configuration actuelle, le pc1 peut communiquer avec le pc2 car elles sont sur le même réseau local

**Question : Même question pour un ping entre PC1 et Serv1. Et Serv2. Pourquoi ?**

Non dans la configuration actuelle, un ping partant de PC1 ne peut pas atteindre Serv1 car eles sont sur des réseaux différents et que nous n'avons pas configurés les routeurs

**Créer des routes statiques par défaut pour faire communiquer tous les réseaux Question : Quelles commandes avez-vous tapé ?**

```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.0.2
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#write memory
Building configuration...
[OK]

R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 10.1.0.1
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#write memory
Building configuration...
[OK]
```

## Vérifier que les pings fonctionnent

De PC1 à Serv1

```
C:\>ping 172.16.1.254

Pinging 172.16.1.254 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 172.16.1.254: bytes=32 time<lms TTL=126
Reply from 172.16.1.254: bytes=32 time<lms TTL=126

Ping statistics for 172.16.1.254:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

De PC2 à Serv1

```
C:\>ping 172.16.1.254

Pinging 172.16.1.254 with 32 bytes of data:

Reply from 172.16.1.254: bytes=32 time<lms TTL=126
Reply from 172.16.1.254: bytes=32 time<lms TTL=126
Reply from 172.16.1.254: bytes=32 time<lms TTL=126
Reply from 172.16.1.254: bytes=32 time<lms TTL=126

Ping statistics for 172.16.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

## VI/ Les ACL standards

**Construire l'ACL numéro 1 avec une règle interdisant 192.168.1.0/24 de communiquer avec 172.16.2.0/24. Attention au routeur sur lequel vous mettez cette règle**

**Question : Quelles commandes avez-vous tapé ?**

```
R2(config)#access-list 1 deny 192.168.1.0 0.0.0.255  
R2(config)#access-list 1 permit any
```

### Appliquer la règle à la bonne interface

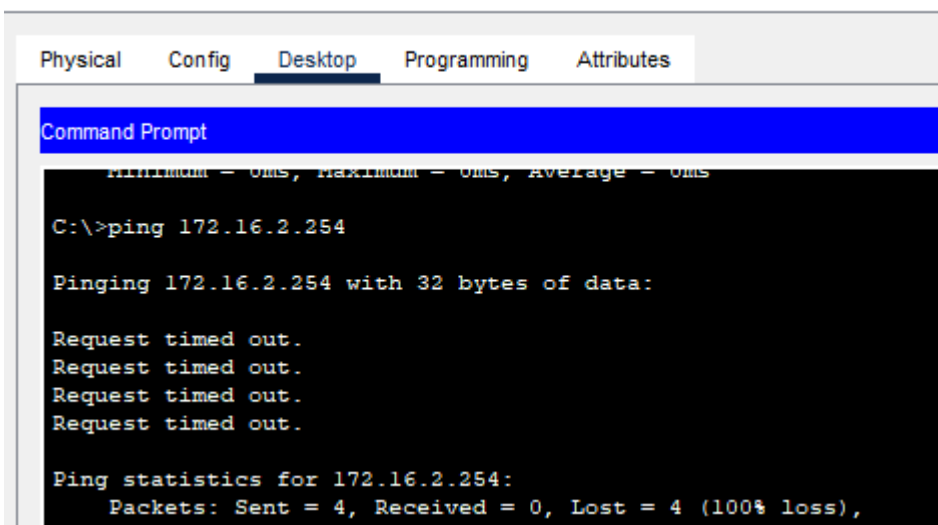
#### Question : Quelles commandes avez-vous tapé ?

```
R2(config)#access-list 1 deny 192.168.1.0 0.0.0.255  
R2(config)#access-list 1 permit any  
R2(config)#interface GigabitEthernet0/2  
R2(config-if)#ip access-group 1 out  
R2(config-if)#end
```

#### Question : En utilisant un ping depuis PC1, montrer que la règle est bien effective

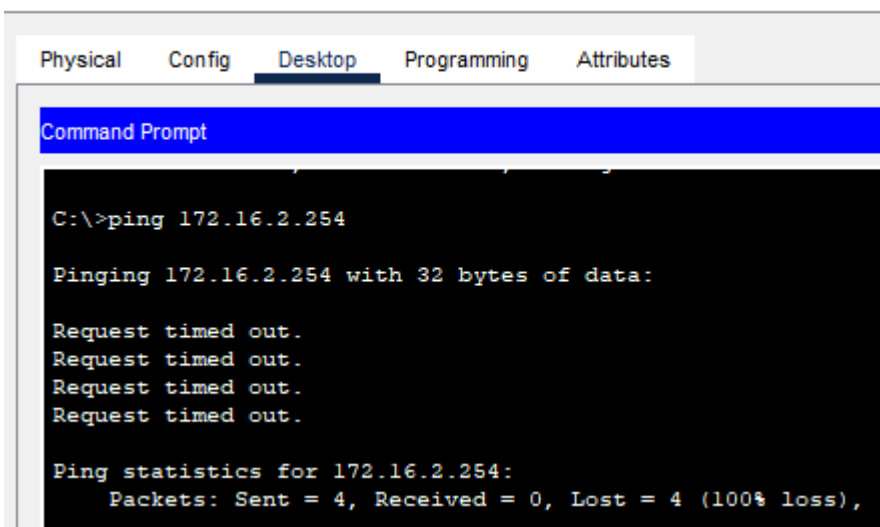
Normalement PC1 et donc PC2 ne devraient plus pouvoir communiquer avec Serv2

PC1



```
Physical  Config  Desktop  Programming  Attributes  
Command Prompt  
C:\>ping 172.16.2.254  
Pinging 172.16.2.254 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Ping statistics for 172.16.2.254:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC2



```
Physical  Config  Desktop  Programming  Attributes  
Command Prompt  
C:\>ping 172.16.2.254  
Pinging 172.16.2.254 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
Ping statistics for 172.16.2.254:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

#### Question : Dans l'état actuel, doit-on faire une règle pour permettre aux réseaux 192.168.1.0/24 et 172.16.1.0/24 de communiquer entre eux ? Pourquoi?

Non, dans l'état actuel, il n'est pas nécessaire de créer une règle pour permettre aux réseaux 192.168.1.0/24 et 172.16.1.0/24 de communiquer entre eux car elle est déjà autorisée par défaut

**Dans l'ACL numéro 2, autoriser 192.168.1.0/24 de communiquer avec 172.16.1.0/24. Attention au routeur sur lequel vous mettez cette règle**

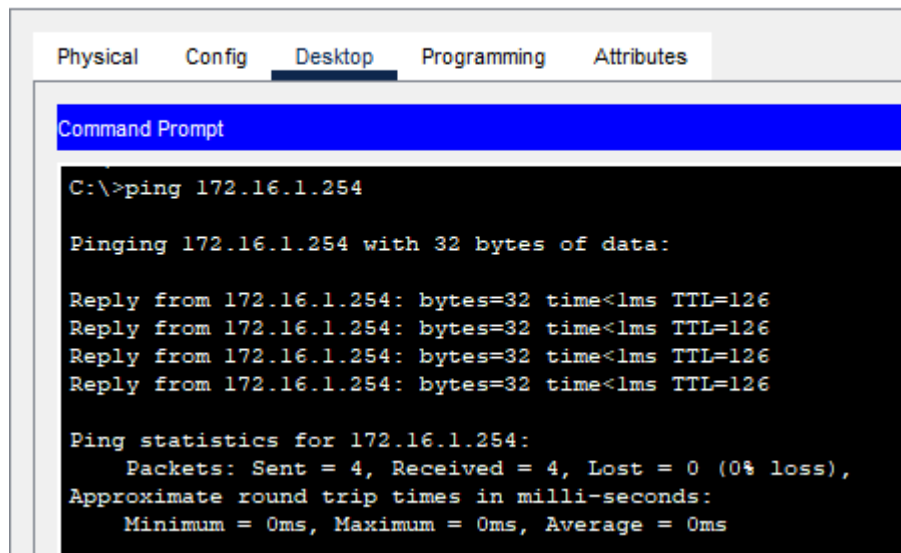
**Appliquer la règle à la bonne interface**

**Question : Quelles commandes avez-vous tapé ?**

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 2 permit 192.168.1.0 0.0.0.255
R2(config)#interface GigabitEthernet0/1
R2(config-if)#ip access-group 2 out
R2(config-if)#end
```

**Question : En utilisant un ping depuis PC2, montrer que la règle est bien effective, la communication est toujours permise entre le réseau 192.168.1.0/24 et le réseau 172.16.1.0/24**

PC2



The screenshot shows a Windows Command Prompt window titled 'Command Prompt' with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active. The command prompt shows the following output:

```
C:\>ping 172.16.1.254

Pinging 172.16.1.254 with 32 bytes of data:

Reply from 172.16.1.254: bytes=32 time<1ms TTL=126
Reply from 172.16.1.254: bytes=32 time<1ms TTL=126
Reply from 172.16.1.254: bytes=32 time<1ms TTL=126
Reply from 172.16.1.254: bytes=32 time<1ms TTL=126

Ping statistics for 172.16.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

**Question : Afficher les ACLs connues par le routeur R2. Vous montrerez le résultat et indiquerez la commande permettant d'afficher les règles**

```
R2#show access-lists
Standard IP access list 1
 10 deny 192.168.1.0 0.0.0.255
 20 permit any
Standard IP access list 2
 10 permit 192.168.1.0 0.0.0.255 (4 match(es))
```

**Question : Dans l'état actuel des chose, afin de bloquer le trafic entre les réseaux 172.16.1.0/24 et 172.16.2.0/24 est-il nécessaire d'établir une règle ?**

Dans l'état actuel, il n'est pas nécessaire de créer une règle supplémentaire pour bloquer le trafic entre les réseaux 172.16.1.0/24 et 172.16.2.0/24

**Dans l'ACL appropriée, attention à bien réfléchir ! Construire la règle bloquant tout le trafic**

**Question : Quelles commandes avez-vous tapé ?**


```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 3 deny any
R2(config)#end
```

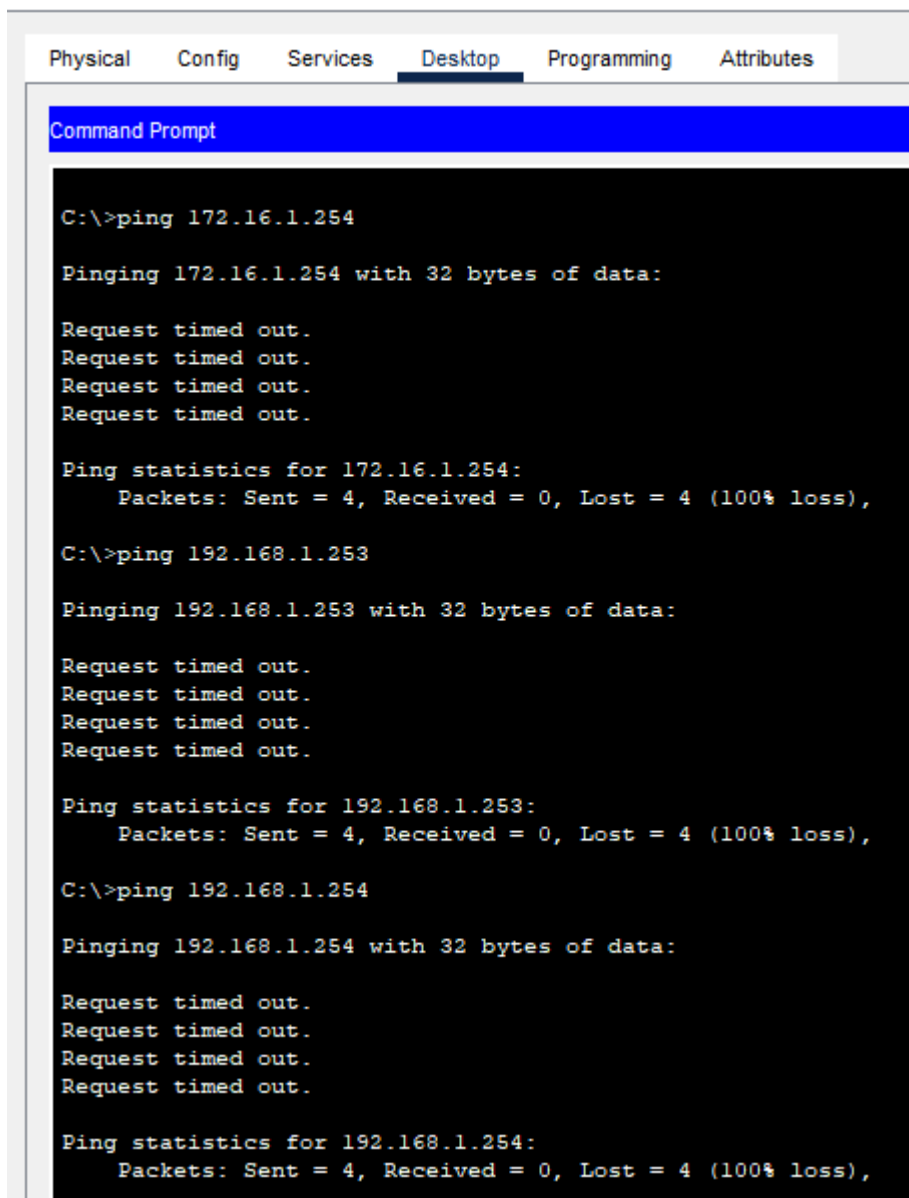
### Appliquer la règle à la bonne interface

#### Question : Quelles commandes avez-vous tapé ?

```
R2(config)#interface GigabitEthernet0/1
R2(config-if)#ip access-group 3 out
R2(config-if)#end
```

#### Question : En utilisant un ping depuis Serv2, montrer que la règle est bien effective

 Serv2



#### Question : En utilisant un ping depuis PC2, vérifier que le trafic est toujours permis entre 192.168.1.0/24 et 172.16.1.0/24