TP15 : Listes de contrôle d’accès standards et étendues.

Sommaire :

1. ACL IPv4 standards :

- Question 2

```
R1#sh run
Building configuration...

Current configuration : 1044 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX152454TD
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
ip domain-name formation.local
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 192.168.11.254 255.255.255.0
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 ip address 192.168.12.254 255.255.255.0
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 10.0.12.1 255.255.255.252
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0
 password 7 0822455D0A16
 logging synchronous
!
line aux 0
!
line vty 0 4
 access-class ACCESS_SSH_ADMIN in
 password 7 0822455D0A16
 logging synchronous
 login
!
!
!
end
```

1ère étape: Configuration du routeur R1.

- Question 3

```
interface Loopback0
 ip address 200.0.0.1 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 10.0.23.1 255.255.255.252
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 ip address 10.0.12.2 255.255.255.252
 clock rate 2000000
 shutdown
!
```

1ère étape : Configuration du routeur R2.

- Question 4

```
interface GigabitEthernet0/0
 ip address 192.168.21.254 255.255.255.0
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 ip address 192.168.22.254 255.255.255.0
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 ip address 10.0.23.2 255.255.255.252
 clock rate 2000000
 shutdown
!
```

1ère étape : Configuration du routeur R3.

- Question 5

```
R1(config)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth 1000
R1(config-router)#network 192.168.11.0 0.0.0.255 area 0
R1(config-router)#network 192.168.12.0 0.0.0.255 area 0
R1(config-router)#network 10.0.12.0 0.0.0.3 area 0
R1(config-router)#passive-interface g0/0
R1(config-router)#passive-interface g0/1
R1(config-router)#exit
R1(config)#int g0/0
R1(config-if)#bandwidth 1000000
R1(config-if)#int g0/1
R1(config-if)#bandwidth 1000000
R1(config-if)#int s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#exit
R1(config)#exit
```

```
R2(config)#ip route 0.0.0.0 0.0.0.0 10
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#router ospf 1
R2(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
R2(config-router)#network 10.0.12.0 0.0.0.3 area 0
R2(config-router)#network 10.0.23.0 0.0.0.3 area 0
R2(config-router)#default-information originate
R2(config-router)#exit
R2(config)#int s0/0/0
R2(config-if)#bandwidth 128



R2(config-if)#int s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#exit
```

```
R3(config-router)#router ospf 1
R3(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
R3(config-router)#network 192.168.21.0 0.0.0.255 area 0
R3(config-router)#network 192.168.22.0 0.0.0.255 area 0
R3(config-router)#network 10.0.23.0 0.0.0.3 area 0
R3(config-router)#passive-interface g0/0
R3(config-router)#passive-interface g0/1
R3(config-router)#exit
R3(config)#int g0/0
R3(config-if)#bandwidth 1000000
R3(config-if)#int g0/1
R3(config-if)#bandwidth 1000000
R3(config-if)#int s0/0/0
R3(config-if)#bandwidth 128
R3(config-if)#exit
R3(config)#exit
```

1ère étape : Nous configurons sur les trois routeurs R1, R2 et R3 OSPFv2.

- Question 6

```
C:\>ping 192.168.12.1

Pinging 192.168.12.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.12.1: bytes=32 time=2ms TTL=125
Reply from 192.168.12.1: bytes=32 time=2ms TTL=125
Reply from 192.168.12.1: bytes=32 time=17ms TTL=125

Ping statistics for 192.168.12.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 17ms, Average = 7ms

C:\>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.11.1: bytes=32 time=2ms TTL=125
Reply from 192.168.11.1: bytes=32 time=17ms TTL=125
Reply from 192.168.11.1: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 17ms, Average = 7ms

C:\>ping 192.168.21.1

Pinging 192.168.21.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.21.1: bytes=32 time<1ms TTL=127
Reply from 192.168.21.1: bytes=32 time<1ms TTL=127
Reply from 192.168.21.1: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.21.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

1ère étape : Actuellement tout les PC peuvent se joindre, depuis PC22 nous effectuons un ping vers les autres PC afin de vérifier que les machines peuvent effectivement communiquer ensemble.

- Question 7

```
R3(config)#access-list 1 permit 192.168.11.0 0.0.0.255
R3(config)#access-list 1 permit 192.168.12.0 0.0.0.255
R3(config)#access-list 1 deny any
```

```
R3(config)#int g0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#exit
```

1ère étape : Nous plaçons une ACL le plus proche de la destination afin que celle-ci n'autorise l'accès au réseau 192.168.21.0/24 qu'aux hôtes des réseaux 192.168.11.0/24 et 192.168.12.0/24. La direction souhaite pouvoir connaître le nombre de tentatives refusées.

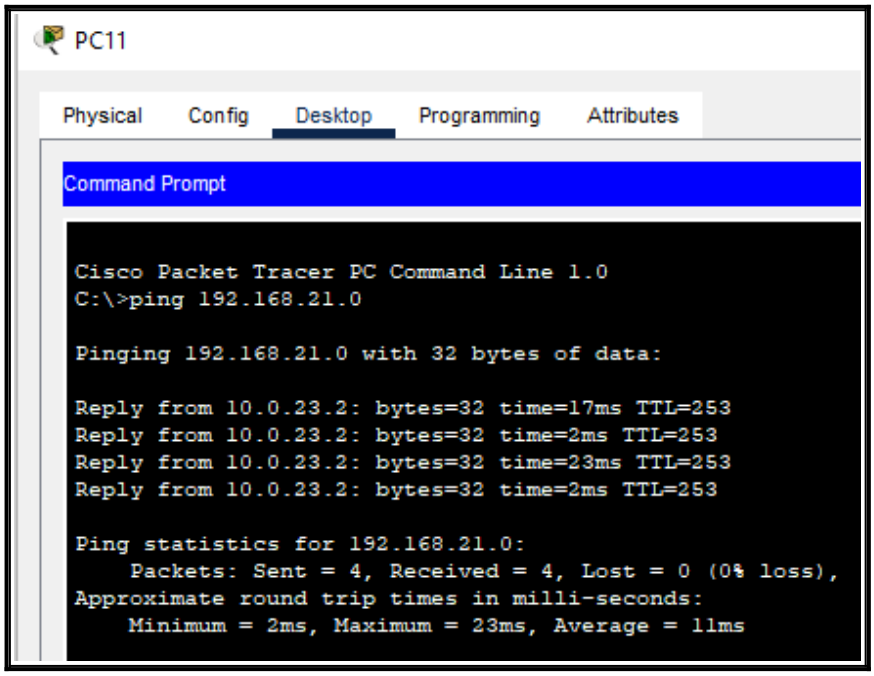
```
C:\>ping 192.168.21.1

Pinging 192.168.21.1 with 32 bytes of data:

Reply from 192.168.22.254: Destination host unreachable.
Reply from 192.168.22.254: Destination host unreachable.
Reply from 192.168.22.254: Destination host unreachable.
Reply from 192.168.22.254: Destination host unreachable.

Ping statistics for 192.168.21.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

2ème étape : Nous effectuons un ping depuis PC22 pour vérifier que le réseau demandé n'est plus accessible.

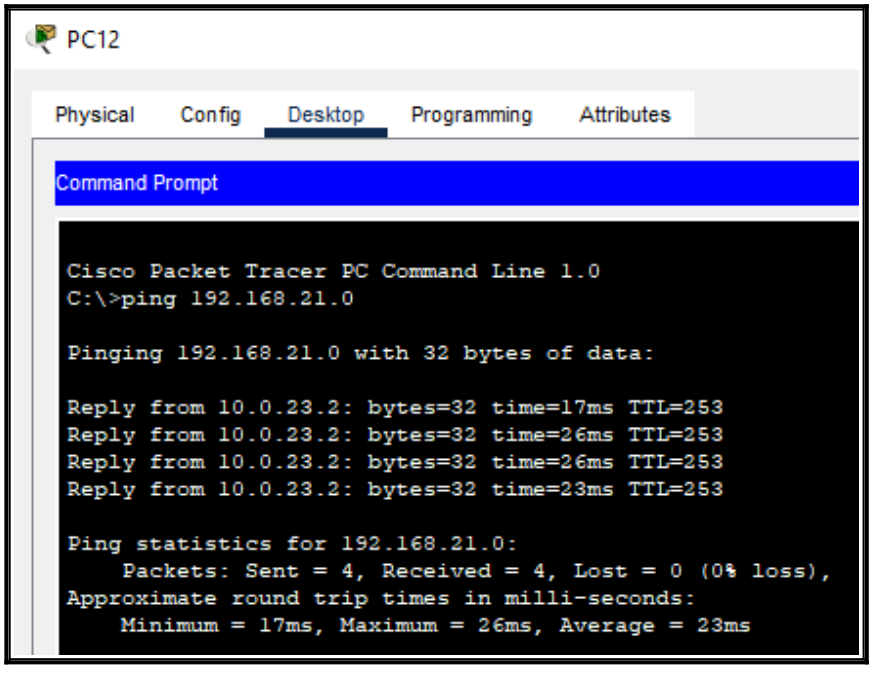
```
R3#sh access-lists
Standard IP access list 1
    10 permit 192.168.11.0 0.0.0.255
    20 permit 192.168.12.0 0.0.0.255
    30 deny any (4 match(es))
```

3ème étape : Nous pouvons également désormais visualiser les tentatives refusées.

PC11 vers Réseau 21



PC12 vers Réseau 21



4ème étape : Nous vérifions que le réseau 21 est accessible pour PC11 et PC12.

- Question 8

```
R1(config)#ip access-list standard  ACCESS_LAN11
R1(config-std-nacl)#permit 192.168.22.0 0.0.0.255
R1(config-std-nacl)#permit host 192.168.21.1
R1(config-std-nacl)#exit
```

```
R1(config)#int g0/0
R1(config-if)#ip access-group ACCESS_LAN11 out
R1(config-if)#exit
```

1ère étape : Création d'une ACL concernant l'accès au réseau 192.168.22.0.

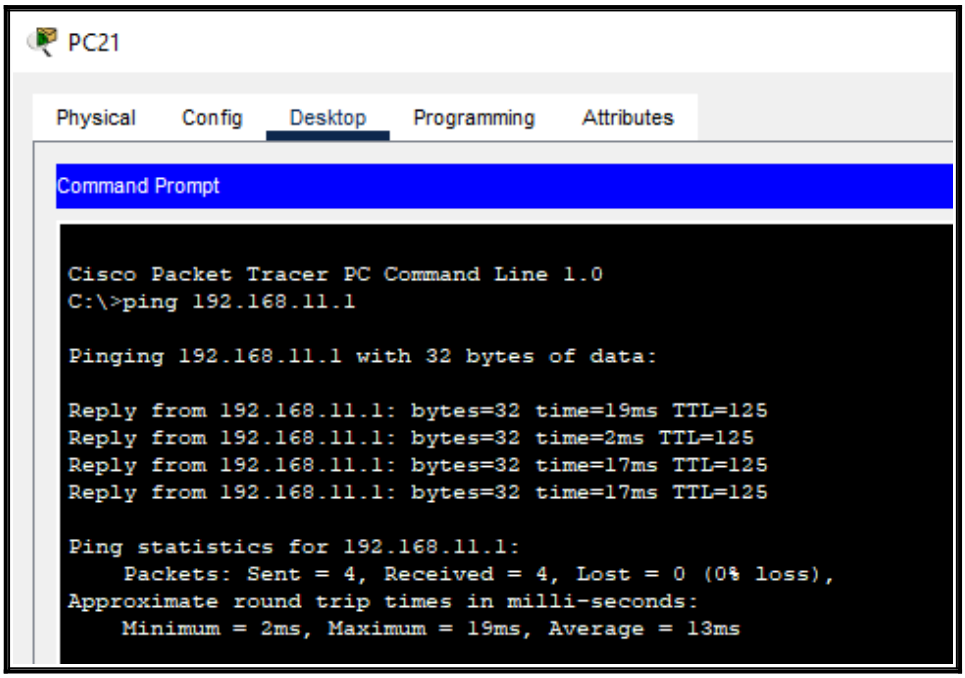
```
R1#sh access-lists
Standard IP access list ACCESS_LAN11
    10 permit 192.168.22.0 0.0.0.255 (4 match(es))
    20 permit host 192.168.21.1 (4 match(es))
```

2ème étape : Nous observons que seul le compteur concernant le trafic autorisé est visible.

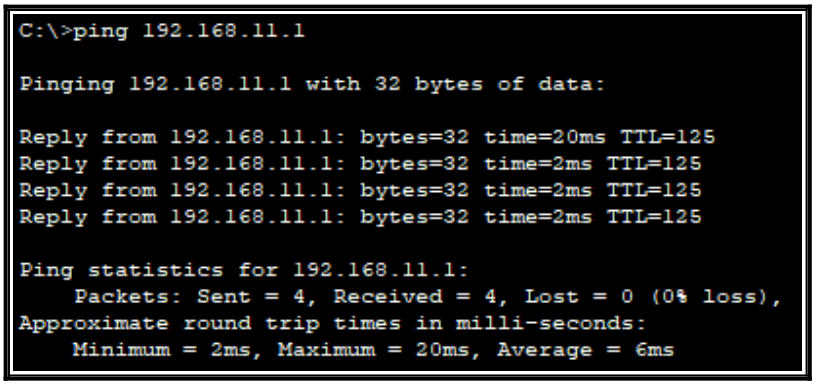
PC12 vers PC11

```
C:\>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.12.254: Destination host unreachable.
Reply from 192.168.12.254: Destination host unreachable.
Reply from 192.168.12.254: Destination host unreachable.
Reply from 192.168.12.254: Destination host unreachable.

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC21 vers PC11



PC22 vers PC11



3ème étape : Nous effectuons différent ping afin de vérifier si l'ACL est bien en place.

- Question 9

```
R1(config)#ip access-list standard ACCESS_LAN11
R1(config-std-nacl)#no 20 permit host 192.168.21.1
R1(config-std-nacl)#20 permit 192.168.21.0 0.0.0.255
R1(config-std-nacl)#30 deny any
```

```
R1#sh access-lists
Standard IP access list ACCESS_LAN11
    10 permit 192.168.22.0 0.0.0.255 (4 match(es))
    20 permit 192.168.21.0 0.0.0.255
    30 deny any
```

1ère étape : Création d'une ACL concernant le réseau 192.168.21.0 .

```
C:\>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.12.254: Destination host unreachable.
Reply from 192.168.12.254: Destination host unreachable.
Reply from 192.168.12.254: Destination host unreachable.
Reply from 192.168.12.254: Destination host unreachable.

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

2ème étape : Nous effectuons un ping de PC11 depuis PC12.

```
R1#sh access-lists
Standard IP access list ACCESS_LAN11
    10 permit 192.168.22.0 0.0.0.255 (4 match(es))
    20 permit 192.168.21.0 0.0.0.255
    30 deny any (4 match(es))
```

3ème étape : Nous observons les tentatives refusées.

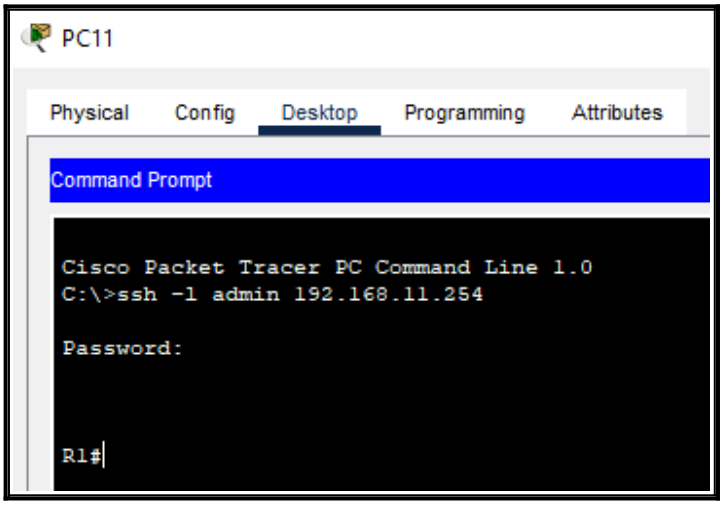
- Question 10

```
R1(config)#ip access-list standard ACCESS_SSH_ADMIN
R1(config-std-nacl)#permit 192.168.11.0 0.0.0.255
```

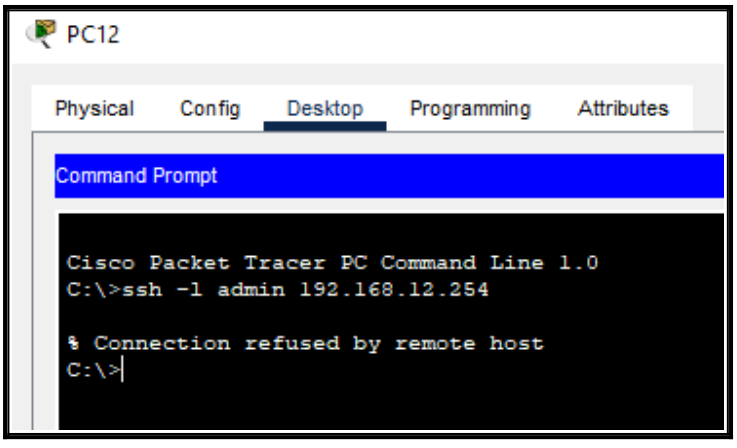
```
R1(config-std-nacl)#line vty 0 4
R1(config-line)#access-class ACCESS_SSH_ADMIN in
R1(config-line)#exit
```

1ère étape: Création d'une ACL concernant la connexion SSH sur le routeur R1.

Connexion SSH PC11 vers R1



Connexion SSH PC12 vers R1

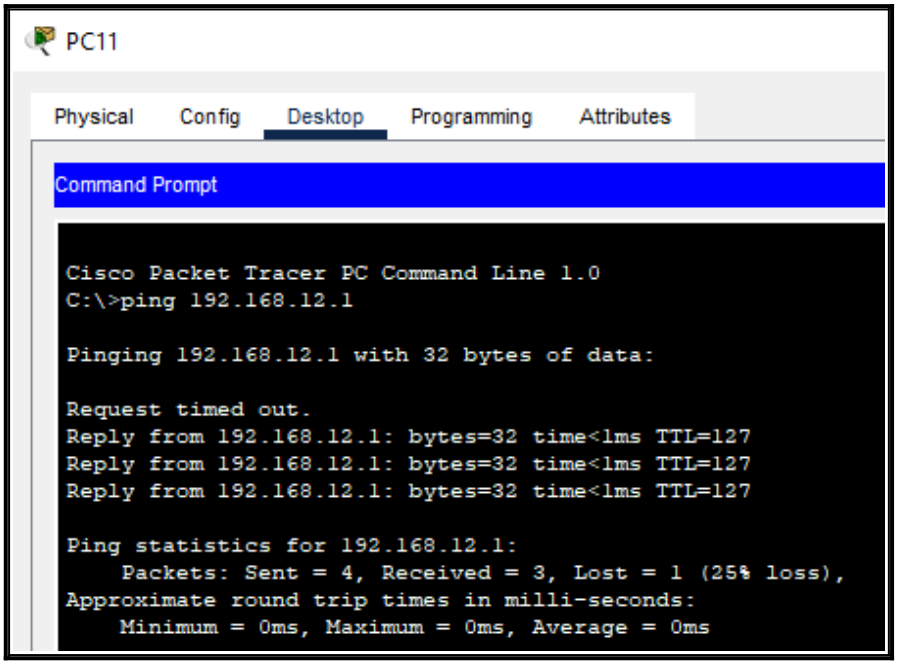


2ème étape : On constate donc que seul PC11 à l'accès en connexion SSH au routeur R1.

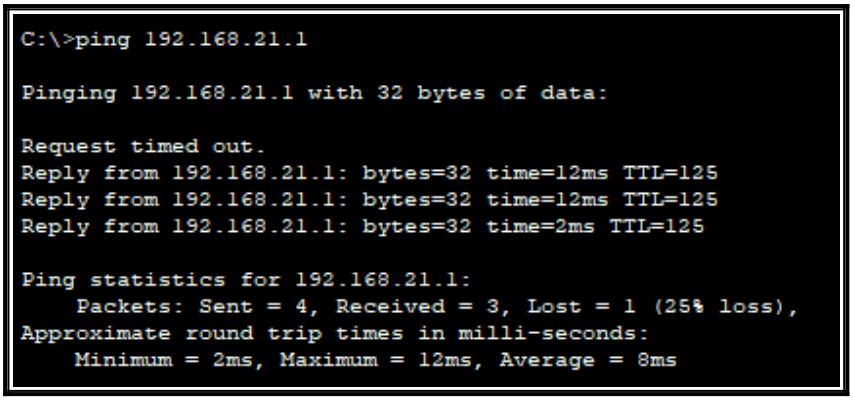
2. ACL IPv4 étendues :

- Question 6

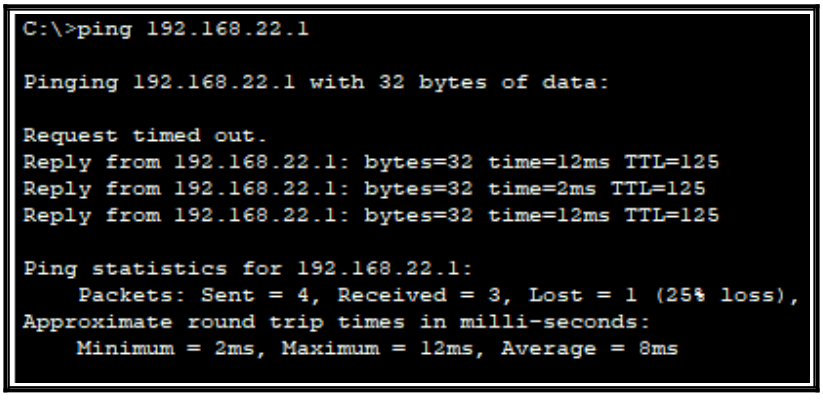
PC11 vers PC12



PC11 vers PC21



PC11 vers PC22



1ère étape : Nous testons différents ping après avoir configuré la topologie, on observe que tout les PC peuvent communiquer entre eux.

- Question 7

```
R1(config)#access-list 111 permit ip 192.168.11.0 0.0.0.255 192.168.21.0 0.0.0.255
R1(config)#access-list 111 deny ip any any
```

```
R1(config)#access-list 112 permit ip 192.168.12.0 0.0.0.255 192.168.21.0 0.0.0.255
R1(config)#access-list 112 deny ip any any
```

```
R1(config)#interface g0/0
R1(config-if)#ip access-group 111 in
```

```
R1(config-if)#int g0/1
R1(config-if)#ip access-group 112 in
```

1ère étape : Création de deux ACL placées respectivement sur les interfaces G0/0 et G0/1 de R1 en entrée, concernant les réseaux 192.168.11.0 et 192.168.12.0 .

PC11 vers PC21

```
C:\>ping 192.168.21.1

Pinging 192.168.21.1 with 32 bytes of data:

Reply from 192.168.21.1: bytes=32 time=10ms TTL=125
Reply from 192.168.21.1: bytes=32 time=4ms TTL=125
Reply from 192.168.21.1: bytes=32 time=4ms TTL=125
Reply from 192.168.21.1: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.21.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 5ms
```

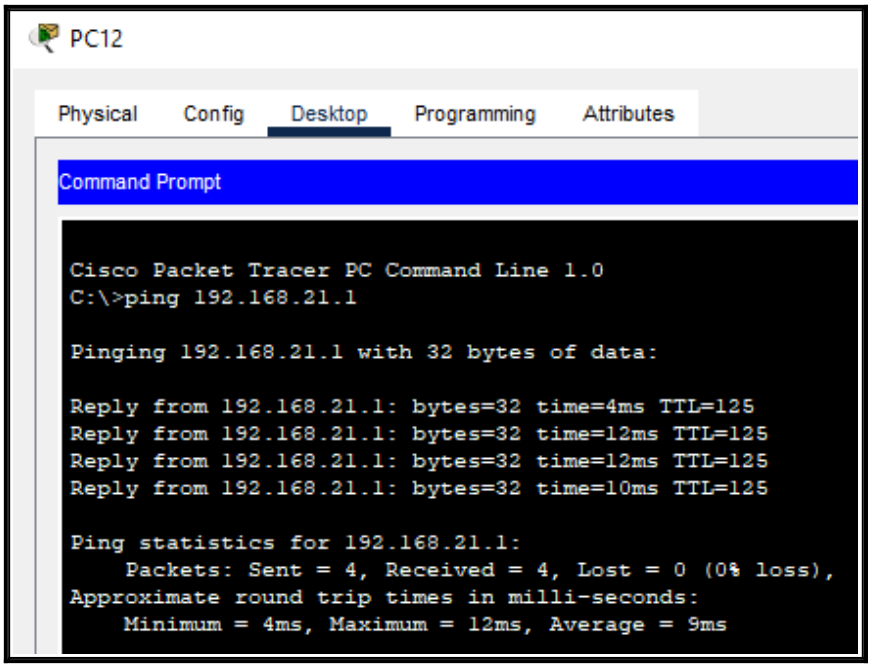
PC11 vers PC22

```
C:\>ping 192.168.22.1

Pinging 192.168.22.1 with 32 bytes of data:

Reply from 192.168.11.254: Destination host unreachable.
Reply from 192.168.11.254: Destination host unreachable.
Reply from 192.168.11.254: Destination host unreachable.
Reply from 192.168.11.254: Destination host unreachable.

Ping statistics for 192.168.22.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC11 vers SRV01

```
C:\>ping 200.0.0.2

Pinging 200.0.0.2 with 32 bytes of data:

Reply from 192.168.11.254: Destination host unreachable.
Reply from 192.168.11.254: Destination host unreachable.
Reply from 192.168.11.254: Destination host unreachable.
Reply from 192.168.11.254: Destination host unreachable.

Ping statistics for 200.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC12 vers PC21



2ème étape : Nous effectuons nos tests afin de vérifier que les ACL fonctionnent correctement.

- Question 8

```
R3(config)#ip access-list extended WEB
R3(config-ext-nacl)#permit icmp 192.168.22.0 0.0.0.255 any echo
R3(config-ext-nacl)#permit tcp 192.168.22.0 0.0.0.255 any eq www
R3(config-ext-nacl)#permit tcp 192.168.22.0 0.0.0.255 any eq 443
```

```
R3(config)#int g0/1
R3(config-if)#ip access-group WEB in
```

1ère étape : Création d'une ACL placée soit sur l'interface S0/0/1 de R3 en sortie soit sur l'interface G0/1 de R3 en entrée.

- Question 9

```
R3(config)#ip access-list extended WEB_RETOUR
R3(config-ext-nacl)#permit tcp any 192.168.22.0 0.0.0.255 established
R3(config-ext-nacl)#exit
```

```
R3(config)#int g0/1
R3(config-if)#ip access-group WEB_RETOUR out
R3(config-if)#exit
```

1ère étape : Création d'une ACL concernant le réseau 192.168.22.0 permettant les échanges concerner par le protocole de transport TCP.

```
R3#sh access-lists
Extended IP access list WEB
    10 permit icmp 192.168.22.0 0.0.0.255 any echo
    20 permit tcp 192.168.22.0 0.0.0.255 any eq www
    30 permit tcp 192.168.22.0 0.0.0.255 any eq 443
Extended IP access list WEB_RETOUR
    10 permit tcp any 192.168.22.0 0.0.0.255 established
```

```
R3#sh ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.22.254/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is WEB_RETOUR
  Inbound  access list is WEB
```

2ème étape : Nous vérifions à la fois les ACL présentes ainsi que celles liées à l'interface f0/1 dur routeur R3.

```
R3(config)#ip access-list extended WEB_RETOUR
R3(config-ext-nacl)#20 deny ip any any
R3(config-ext-nacl)#exit
```

3ème étape : Modification de la liste d'accès.

```
C:\>ping 200.0.0.2

Pinging 200.0.0.2 with 32 bytes of data:

Reply from 192.168.22.254: Destination host unreachable.
Reply from 192.168.22.254: Destination host unreachable.
Reply from 192.168.22.254: Destination host unreachable.
Reply from 192.168.22.254: Destination host unreachable.

Ping statistics for 200.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

4ème étape : Ping effectuer depuis PC22, on constate que la requête ICMP ne passe pas.

```
R3(config)#ip access-list extended WEB_RETOUR
R3(config-ext-nacl)#15 permit icmp any 192.168.22.0 0.0.0.255 echo-reply
```

5ème étape : Nouvelle ACL permettant cette fois-ci le passage des requêtes ICMP.

```
R3#sh access-lists WEB_RETOUR
Extended IP access list WEB_RETOUR
    permit tcp any 192.168.22.0 0.0.0.255 established
    permit icmp any 192.168.22.0 0.0.0.255 echo-reply (4 match(es))
    deny ip any any
```

6ème étape : Après un nouveau test de ping, nous observons que la requête ICMP à bien fonctionnée.

- Question 10

```
R3(config-ext-nacl)#ip access-list extended WEB
R3(config-ext-nacl)#permit tcp 192.168.22.0 0.0.0.255 any eq pop3
R3(config-ext-nacl)#deny ip any any
```

1ère étape : La demande d'autorisation du protocole POP3 pour le réseau 192.168.22.0/24 n'est en contradiction avec aucune commande précédente de la liste de contrôle d'accès WEB, nous modifions donc pour cela l'ACL WEB. Enfin, il convient d'ajouter un refus explicite en fin de liste pour comptabiliser toutes les tentatives refusées.