SOMMAIRE

1 ACL Ipv4 standards

a) Configurer son nom d'hôte, désactivez la recherche DNS, activez le chiffrement des mots de passe.

```
r1(config)#no ip domain-lookup
r1(config)#enable secret
r1(config)#hostname r1
r1(config)#no ip domain-lookup
r1(config)#ser
r1(config)#service pass
r1(config)#service password-encryption
r1(config)#
```

b) Protéger l'accès enable avec le mot de passe class. Ajoutez l'utilisateur admin avec le mot de passe cisco. Configurez l'accès SSH avec l'utilisateur admin et la synchronisation des logs.

```
r1(config)#service password-encryption
r1(config)#enable secret class
r1(config)#user
r1(config)#username admin pass cisco
r1(config)#line vty 0 4
r1(config-line)#login local
r1(config-line)#exec
r1(config-line)#exec-timeout 5 0
r1(config-line)#logging syn
r1(config-line)#logging synchronous
r1(config-line)#
```

```
r1(config)#ip domain-
r1(config)#ip domain-name exupery.local
r1(config)#crypto key generate rsa
The name for the keys will be: r1.exupery.local
Choose the size of the key modulus in the range
  General Purpose Keys. Choosing a key modulus g
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be nor

r1(config)#line vty 0 4
*Mar 1 0:37:14.533: %SSH-5-ENABLED: SSH 1.99 has
r1(config-line)#login local
r1(config-line)#transport input ssh
r1(config-line)#^Z
r1#
```

c) Configurer les interfaces du routeur (G0/0, G0/1 et S0/0/0).

```
r1(config)#int g0/0
r1(config-if)#ip add 192.168.11.254 255.255.255.0
r1(config-if)#no shut

r1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
int g0/1
r1(config-if)#ip add 192.168.12.254 255.255.255.0
r1(config-if)#no shut

r1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
int s0/0/0
r1(config-if)#ip add 10.0.12.1 255.255.255.252
r1(config-if)#clo
r1(config-if)#clock rata
r1(config-if)#clock rate
r1(config-if)#clo
r1(config-if)#clock r
r1(config-if)#clock rate 64000
r1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
r1(config-if)#
```

2) Configurer le routeur R2 de manière analogue ainsi que les interfaces du routeur (L0, S0/0/0 et S0/0/1).

```
Router(config)#no ip
Router(config)#no ip do
Router(config)#no ip domain
Router(config)#no ip domain-lo
Router(config)#no ip domain-lookup
Router(config)#host r2
r2(config)#servic pass
r2(config)#servic password-encryption
r2(config)#ena secret class
r2(config)#username admin pass cisco
r2(config)#line vty 0 4
r2(config-line)#login local
r2(config-line)#exec
r2(config-line)#exec-timeout 5 0
r2(config-line)#logging syn
r2(config-line)#
```

```
r2(config)#ip domain-name exupery.local
r2(config)#crypto
r2(config)#crypto key genere
r2(config)#crypto key generq
r2(config)#crypto key gener
r2(config)#crypto key generate rsa
The name for the keys will be: r2.exupery.local
Choose the size of the key modulus in the range o
  General Purpose Keys. Choosing a key modulus gr
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-

r2(config)#line vty 0 4
*Mar 1 0:42:30.481: %SSH-5-ENABLED: SSH 1.99 has
r2(config-line)#login local
r2(config-line)#tran
r2(config-line)#transport input ssh
r2(config-line)#
```

```
r2(config)#int s0/0/0
r2(config-if)#ip add 10.0.23.1 255.255.255.252
r2(config-if)#no shut

r2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
int s0/0/0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed st
r2(config-if)#int s0/0/1
r2(config-if)#ip add 10.0.12.2 255.255.255.252
r2(config-if)#no shut

r2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

r2(config-if)#int s0/0/
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to
up
0
r2(config-if)#int s0/0/0
r2(config-if)#clock rate 64000
r2(config-if)#int l0

r2(config-if)#
%LINK-3-UPDOWN: Interface Loopback0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to
up

r2(config-if)#ip add 200.0.0.1 255.255.255.255
r2(config-if)#no shut
r2(config-if)#
```

3) Configurer le routeur R3 de manière analogue ainsi que les interfaces du routeur (G0/0, G0/1 et S0/0/1).

```
Router(config)#hostname  r3
r3(config)#no ip domain-look
r3(config)#no ip domain-lookup
r3(config)#service pass
r3(config)#service password-encryption
r3(config)#ena secret class
r3(config)#username admin pass cisco
r3(config)#line vty 0 4
r3(config-line)#login local
r3(config-line)#exe
r3(config-line)#exec-timeout
% Incomplete command.
r3(config-line)#exec-timeout 5 0
r3(config-line)#logg
r3(config-line)#logg syn
r3(config-line)#
```

```
r3(config)#ip domain-name exupery.local
r3(config)#crpto key generate rsa modulus
                  ^
% Invalid input detected at '^' marker.

r3(config)#cripto key generate rsa
                  ^
% Invalid input detected at '^' marker.

r3(config)#crypto key generate rsa
The name for the keys will be: r3.exupery.loc
Choose the size of the key modulus in the ran
  General Purpose Keys. Choosing a key modulu
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be

r3(config)#line vty 0 4
*Mar 1 0:45:34.760: %SSH-5-ENABLED: SSH 1.99
r3(config-line)#login local
r3(config-line)#transport input ssh
r3(config-line)#
```

```
r3(config)#int s0/0/1
r3(config-if)#ip add 10.0.23.2 255.255.255.252
r3(config-if)#no shut
r3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed
state to up
int
    ^
% Invalid input detected at '^' marker.

r3(config-if)#int g0/0
r3(config-if)#ip add 192.168.21.254 255.255.255.0
r3(config-if)#no shut

r3(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

r3(config-if)#int g0/1
r3(config-if)#ip add 192.168.22.254
% Incomplete command.
r3(config-if)#ip add 192.168.22.254 255.255.255.0
r3(config-if)#no shut

r3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed stat

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthe
changed state to up
```

4) Configurer RIPv2 sur les routeurs R1, R2 et R3. Vérifiez leur table de routage

```
r1(config)#rou
r1(config)#router rip
r1(config-router)#vers 2
r1(config-router)#network 10.0.0.0
r1(config-router)#no auto-su
r1(config-router)#no auto-summary
r1(config-router)#network 192.168.12.0
r1(config-router)#network 192.168.11.0
r1(config-router)#^Z
r1#
```

```
r2(config)#route
r2(config)#router rip
 2(config-router)#ver 2
 2(config-router)#network 10.0.0.0
 2(config-router)#no sum
                   ^
```

```
r3(config)#rout rip
r3(config-router)#ver 2
r3(config-router)#no auto
r3(config-router)#no auto-summary
r3(config-router)#netwo
r3(config-router)#network 10.0.0.0
r3(config-router)#network 192.168.21.0
r3(config-router)#network 192.168.22.0
r3(config-router)#^Z
r3#
```

```
r1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.0.12.0/30 is directly connected, Serial0/0/0
L       10.0.12.1/32 is directly connected, Serial0/0/0
R       10.0.23.0/30 [120/1] via 10.0.12.2, 00:00:20, Serial0/0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/0
L       192.168.11.254/32 is directly connected, GigabitEthernet0/0
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/24 is directly connected, GigabitEthernet0/1
L       192.168.12.254/32 is directly connected, GigabitEthernet0/1
R    192.168.21.0/24 [120/2] via 10.0.12.2, 00:00:16, Serial0/0/0
R    192.168.22.0/24 [120/2] via 10.0.12.2, 00:00:12, Serial0/0/0

r1#
```

5)Vérifiez la connectivité. Tous les PC doivent pouvoir se joindre et doivent également pouvoir accéder en SSH aux trois routeurs (captures d'écran).

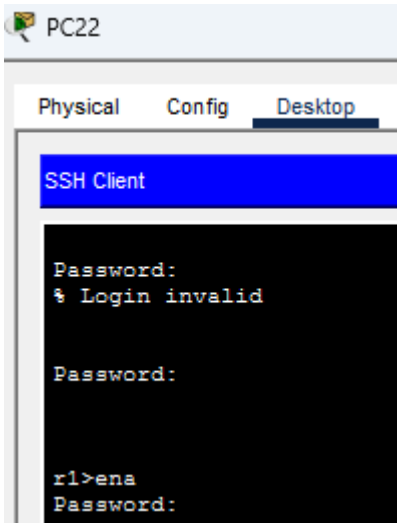
```
C:\>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.11.1: bytes=32 time<1ms TTL=127
Reply from 192.168.11.1: bytes=32 time<1ms TTL=127
Reply from 192.168.11.1: bytes=32 time<1ms TTL=127
Reply from 192.168.11.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

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=11ms TTL=125
Reply from 192.168.21.1: bytes=32 time=7ms TTL=125
Reply from 192.168.21.1: bytes=32 time=6ms TTL=125
Reply from 192.168.21.1: bytes=32 time=6ms 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 = 6ms, Maximum = 11ms, Average = 7ms

C:\>ping 192.168.22.1

Pinging 192.168.22.1 with 32 bytes of data:

Reply from 192.168.22.1: bytes=32 time=12ms TTL=125
Reply from 192.168.22.1: bytes=32 time=8ms TTL=125
Reply from 192.168.22.1: bytes=32 time=3ms TTL=125
Reply from 192.168.22.1: bytes=32 time=5ms TTL=125

Ping statistics for 192.168.22.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 12ms, Average = 7ms

C:\>
```

```
C:\>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.11.1: bytes=32 time=22ms TTL=125
Reply from 192.168.11.1: bytes=32 time=18ms TTL=125
Reply from 192.168.11.1: bytes=32 time=18ms TTL=125
Reply from 192.168.11.1: bytes=32 time=18ms TTL=125

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 22ms, Average = 19ms

C:\>ping 192.168.12.1

Pinging 192.168.12.1 with 32 bytes of data:

Reply from 192.168.12.1: bytes=32 time=23ms TTL=125
Reply from 192.168.12.1: bytes=32 time=10ms TTL=125
Reply from 192.168.12.1: bytes=32 time=2ms TTL=125
Reply from 192.168.12.1: bytes=32 time=5ms TTL=125

Ping statistics for 192.168.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 23ms, Average = 10ms

C:\>ping 192.168.22.1

Pinging 192.168.22.1 with 32 bytes of data:

Reply from 192.168.22.1: bytes=32 time<1ms TTL=127
Reply from 192.168.22.1: bytes=32 time<1ms TTL=127
Reply from 192.168.22.1: bytes=32 time<1ms TTL=127
Reply from 192.168.22.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.22.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.12.1

Pinging 192.168.12.1 with 32 bytes of data:

Reply from 192.168.12.1: bytes=32 time=35ms TTL=125
Reply from 192.168.12.1: bytes=32 time=2ms TTL=125
Reply from 192.168.12.1: bytes=32 time=5ms TTL=125
Reply from 192.168.12.1: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 35ms, Average = 11ms

C:\>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.11.1: bytes=32 time=16ms TTL=125
Reply from 192.168.11.1: bytes=32 time=12ms TTL=125
Reply from 192.168.11.1: bytes=32 time=9ms TTL=125
Reply from 192.168.11.1: bytes=32 time=5ms TTL=125

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 16ms, Average = 10ms

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<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
Reply from 192.168.21.1: bytes=32 time<1ms TTL=127

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

C:\>S
```

```
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<1ms TTL=127
Reply from 192.168.12.1: bytes=32 time<1ms TTL=127
Reply from 192.168.12.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.12.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.22.1

Pinging 192.168.22.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.22.1: bytes=32 time=7ms TTL=125
Reply from 192.168.22.1: bytes=32 time=5ms TTL=125
Reply from 192.168.22.1: bytes=32 time=5ms TTL=125

Ping statistics for 192.168.22.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 7ms, Average = 5ms

C:\>ping -c 2 192.168.22.1
Invalid Command.

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=22ms TTL=125
Reply from 192.168.21.1: bytes=32 time=5ms TTL=125
Reply from 192.168.21.1: bytes=32 time=5ms TTL=125

Ping statistics for 192.168.21.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 22ms, Average = 10ms

C:\>
```

Capture decran du pc22



Créer une liste de contrôle d'accès numérotée standard qui 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.

```
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)#ass
r3(config)#acc
r3(config)#access-list 1 deny any
r3(config)#int g0/0
r3(config-if)#ip acc
r3(config-if)#ip access-group 1 out
r3(config-if)#exit
r3(config)#
```

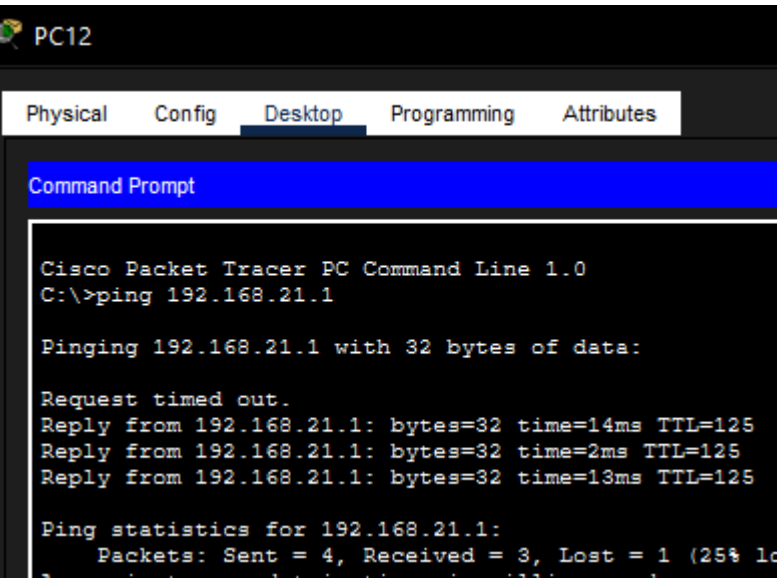
En conséquence, le réseau 192.168.21.0/24 ne doit plus être accessible depuis le PC22.

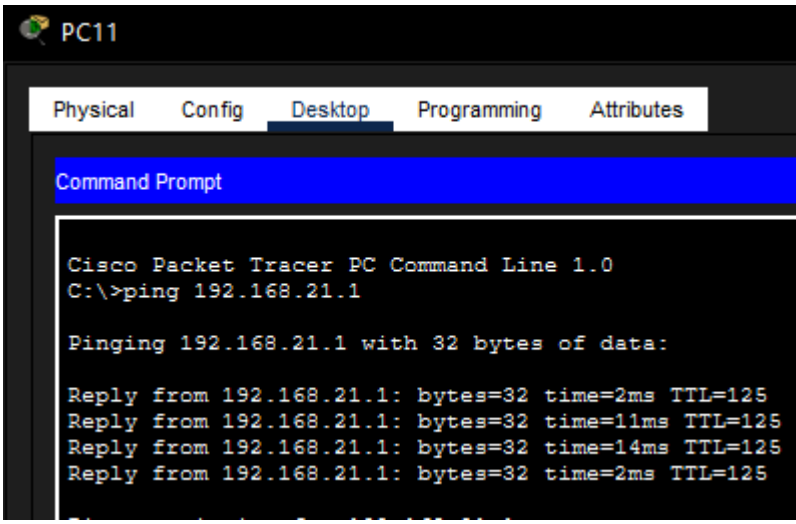
```
C:\>ping 192.168.21.1

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),

C:\>
```

```
r3(config)#^Z
r3#
%SYS-5-CONFIG_I: Configured from consol
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))

r3#
```

Grâce à l'ajout de la dernière ACL (deny any), il est possible de visualiser les tentatives refusées :

```
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

r3#
```





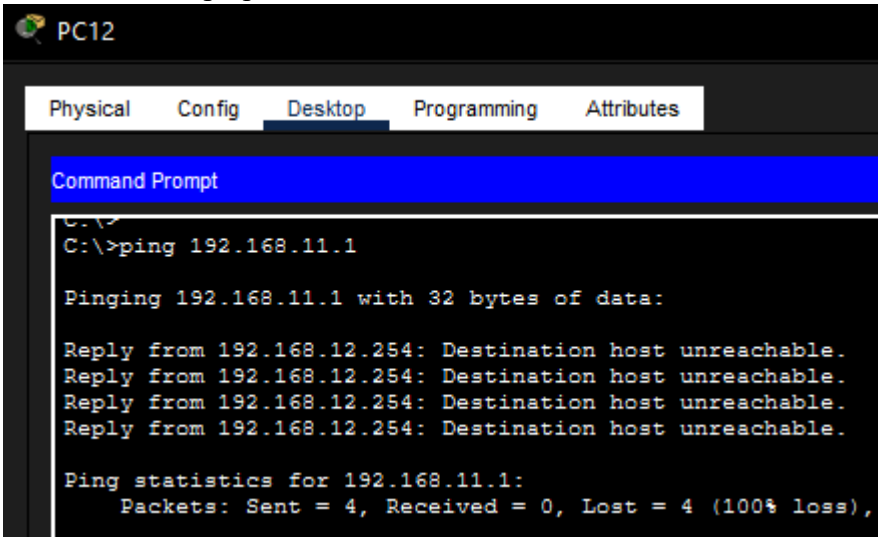
8. Créer une liste de contrôle d'accès standard nommée ACCESS_LAN11 qui n'autorise l'accès au réseau 192.168.11.0/24 qu'aux hôtes du réseau 192.168.22.0/24 ainsi qu'au PC21

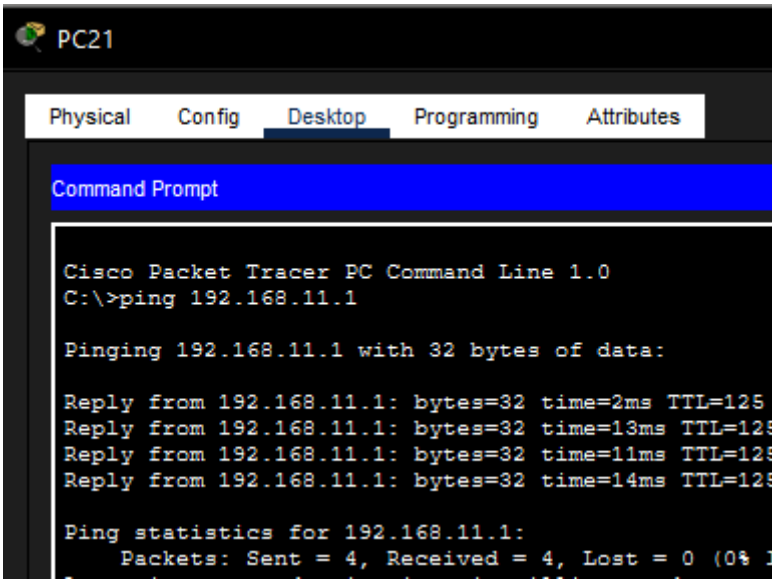
```
r1(config)#ip access
r1(config)#ip access
r1(config)#ip access-list stan
r1(config)#ip access-list standard acc
r1(config)#ip access-list standard ACCESS_LA?
WORD
r1(config)#ip access-list standard ACCESS_LAN11
r1(config-std-nacl)#permit 192.168.22.0 0.0.0.255
r1(config-std-nacl)#permit host 192.168.21.1
r1(config-std-nacl)#exit
r1(config)#int g0/0
r1(config-if)#ip acces
r1(config-if)#ip access-group  ACCESS_LAN11 out
r1(config-if)#exit
r1(config)#
```

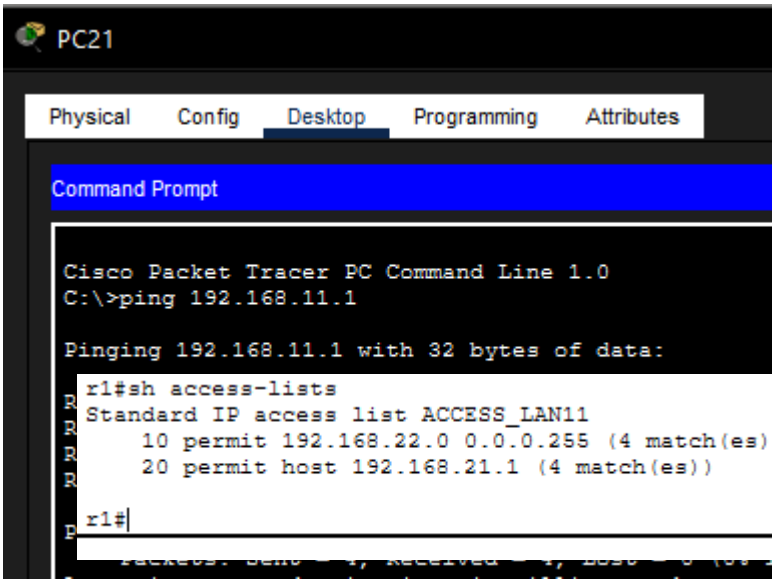
Il faut toujours indiquer le type d'ACL avec les listes nommées.Dans ce cas, seuls les compteurs concernant le trafic autorisé seront visibles :

```
sh acces
r1#sh access-lists
Standard IP access list ACCESS_LAN11
    10 permit 192.168.22.0 0.0.0.255
    20 permit host 192.168.21.1

r1#
```

un ping réussi à destination de PC11 a été effectué depuis PC21. Testez un ping depuis PC21, PC22 et PC12 et vérifiez le nombre de paquets autorisés à l'aide de la commande **sh access-lists**







9. Modifier la liste de contrôle d'accès standard nommée ACCESS_LAN11 afin de permettre à tous
le réseau 192.168.21.0/24 (en plus du réseau 192.168.22.0/24) d'accéder au réseau 192.168.11.0/24. De plus, la direction souhaite également pouvoir connaître le nombre de tentatives refusées.

```
r1(config)#ip acc
r1(config)#ip access-list standard ACCES_LAN11
r1(config-std-nacl)#no 20 per
r1(config-std-nacl)#no 20 permi
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(config-std-nacl)#exit
r1(config)#^Z
r1#
%SYS-5-CONFIG_I: Configured from console by console
sh acc
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))
Standard IP access list ACCES_LAN11
    20 permit 192.168.21.0 0.0.0.255
    30 deny any

r1#
```

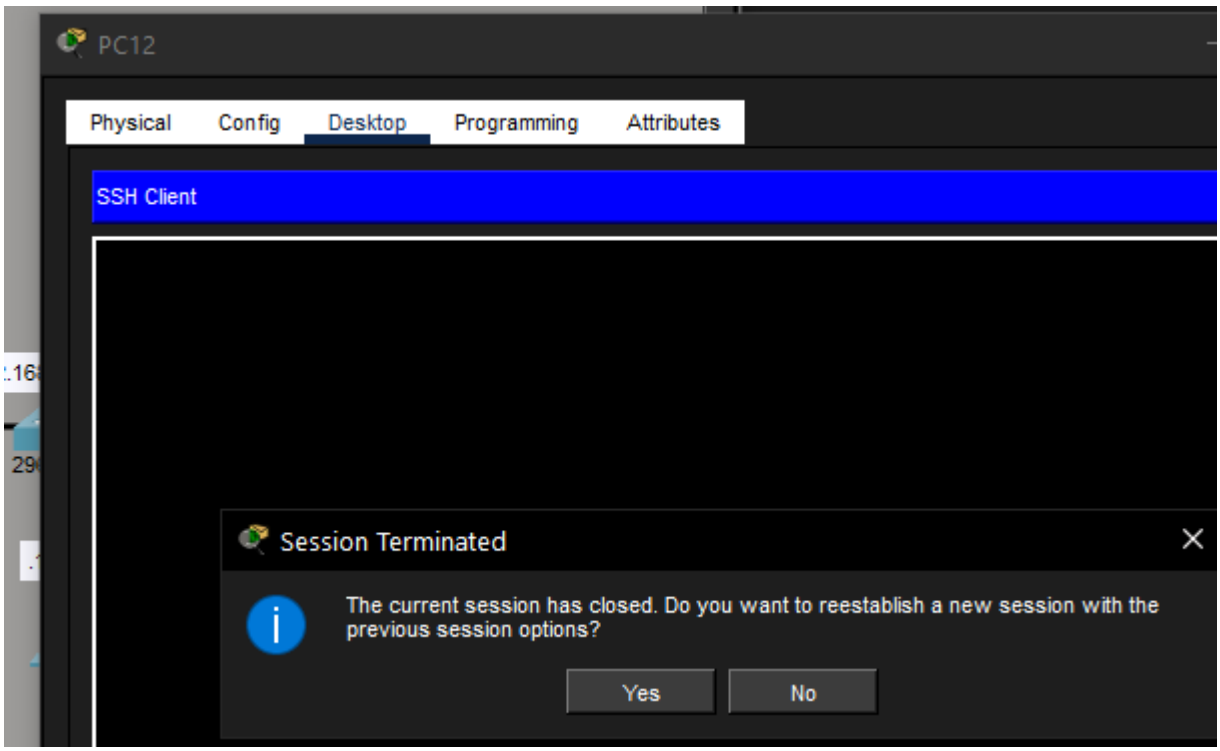
enfectuer un ping de PC11 depuis PC12 et vérifier le nombre de paquets refusés à l'aide de la

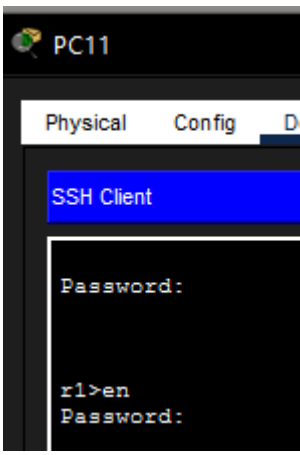
```
C:\>ping 192.168.11.1

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
```

```
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))
Standard IP access list ACCES_LAN11
    20 permit 192.168.21.0 0.0.0.255
    30 deny any

r1#
```

10. Créer une liste de contrôle d'accès standard nommée ACCESS_SSH_ADMIN permettant de sécuriser les ports VTY des routeurs en n'autorisant que les accès SSH depuis le réseau 192.168.11.0/24.

```
r1(config)#ip acc
r1(config)#ip access-list starndard ACCESS_SSH_ADMIN
                                    ^
% Invalid input detected at '^' marker.

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
r1(config)#
```





2. ACL IPv4 étendues

5. Configurer OSPFv2 sur les routeurs R1, R2 et R3. Vérifiez leur table de routage.

```
r1(config)# router ospf 1
r1(config-router)#auto
r1(config-router)#auto-cost reference
r1(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent
r1(config-router)#netwo
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)#pass
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)#bans
r1(config-if)#band
r1(config-if)#bandwidth 1000000
r1(config-if)#int g0/1
r1(config-if)#bandwidth 1000000
r1(config-if)#int 0/0/0
                  ^
% Invalid input detected at '^' marker.

r1(config-if)#int s0/0/0
r1(config-if)#band
r1(config-if)#bandwidth 128
r1(config-if)#exit
r1(config)#
```

La configuration OSPF de R2 est la suivante :

```
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 g0/0
%Default route without gateway, if not a point-to-point inter
r2(config)#router ospf 1
r2(config-router)#auto
r2(config-router)#auto-cost raf
r2(config-router)#auto-cost refere
r2(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent acros
r2(config-router)#network 10.0.12.0 0.0.0.3 area 0
r2(config-router)#network 10.0.12.0 0.0.0.3 area 0
00:26:13: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.12.254 on Se
r2(config-router)#network 10.0.23.0 0.0.0.3 area 0
r2(config-router)#de
r2(config-router)#default-information ori
r2(config-router)#default-information originate
r2(config-router)#exi
r2(config)#int s0/0/0
r2(config-if)#ba
r2(config-if)#bandwidth 128
r2(config-if)#int s0/0/1
r2(config-if)#bandwidth 128
r2(config-if)#exit
r2(config)#
```

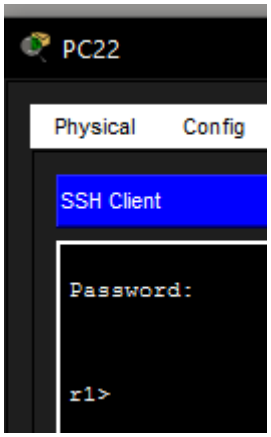
La configuration OSPF de R3 est la suivante :

```
r3(config)#router ospf 1
r3(config-router)#auto
r3(config-router)#auto-cost ren
r3(config-router)#auto-cost ref
r3(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consiste
r3(config-router)#network 192.168.21.0 0.0.0.255 area
r3(config-router)#network 192.168.22.0 0.0.0.255 area
r3(config-router)#network 10.0.23.0 0.0.0.3 area 0
r3(config-router)#passive
r3(config-router)#passive-interface
00:30:04: %OSPF-5-ADJCHG: Process 1, Nbr 200.0.0.1 on
Loading Done
g0/0
r3(config-router)#passive-interface g0/1
r3(config-router)#passive-interface g0/1
r3(config-router)#exit
r3(config)#int
r3(config)#interface g0/0/
                          ^
% Invalid input detected at '^' marker.

r3(config)#interface g0/0
r3(config-if)#band
r3(config-if)#bandwidth 1000000
r3(config-if)#interface g0/1
r3(config-if)#bandwidth 1000000
r3(config-if)#interface s0/0/1
r3(config-if)#bandwidth 128
r3(config-if)#exit
r3(config)#
```

Depuis R3, les réseaux de R1, la liaison R1-R2 et la route par défaut devraient maintenant être appris via OSPF :

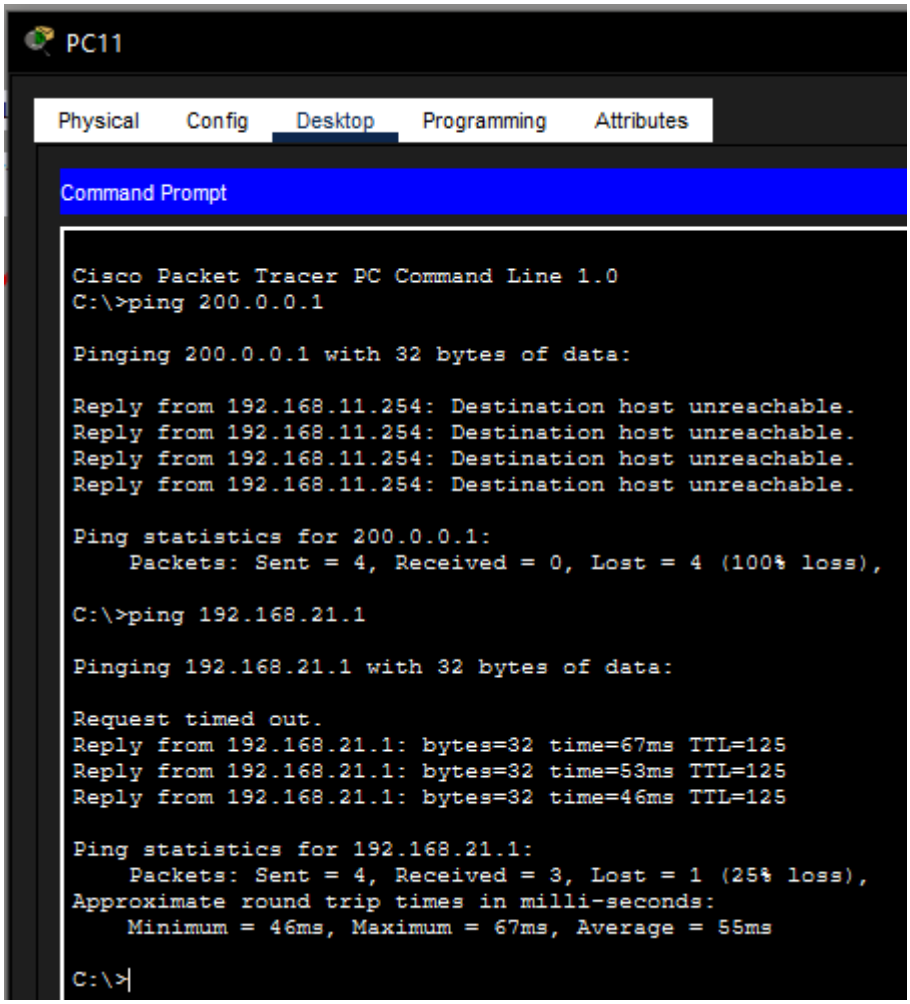
```
sh ip route ospf
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O       10.0.12.0 [110/1294] via 10.0.23.1, 00:02:21, Serial0/0/1
O    192.168.11.0 [110/1295] via 10.0.23.1, 00:02:21, Serial0/0/1
O    192.168.12.0 [110/1295] via 10.0.23.1, 00:02:21, Serial0/0/1

r3#
```

Tous les PC doivent pouvoir se joindre et doivent également pouvoir accéder en SSH aux trois routeurs. De plus, le serveur SRV01 doit pouvoir être accessible en ICMP, HTTP, HTTPS et FTP depuis tous les hôtes. Testez



7. Créer une liste de contrôle d'accès étendue numérique qui n'autorise, pour les réseaux 192.168.11.0/24 et 192.168.12.0/24, que l'accès aux hôtes du réseau 192.168.21.0/24. La direction souhaite pouvoir connaître le nombre de tentatives refusées.

```
r1#en
r1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r1(config)#access
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 192.168.11.0 0.0.0.255 192.168.21.0 0.0.0.255
r1(config)#access-list 112 deny ip any any
r1(config)#interface
r1(config)#interface g0/0
r1(config-if)#ip access-g
r1(config-if)#ip access-group 111 in
r1(config-if)#interface g0/1
r1(config-if)#ip access-group 112 in
r1(config-if)#exit
r1(config)#
```



8. Créer une liste de contrôle d'accès étendue nommée WEB qui n'autorise les hôtes du réseau 192.168.22.0/24 qu'à accéder à Internet en HTTP et HTTPS. Les ping doivent également fonctionner.

```
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-ext-nacl)#exit
r3(config)#int g0/1
r3(config-if)#ip access
r3(config-if)#ip access-group WEB in
r3(config-if)#exit
r3(config)#
```

9. Créer une liste de contrôle d'accès nommée WEB_RETOUR qui autorise uniquement le retour du trafic initié depuis l'intérieur du réseau 192.168.22.0/24. Attention à ne pas bloquer l'accès au réseau 192.168.21.0/24 depuis les réseaux 192.168.11.0/24 et 192.168.12.0/24.

```
r3(config)#ip access-list extended WEB_RETOUR
r3(config-ext-nacl)#permit tcp any 192.168.22.0 0.0.0.255 ex
r3(config-ext-nacl)#permit tcp any 192.168.22.0 0.0.0.255 es
r3(config-ext-nacl)#permit tcp any 192.168.22.0 0.0.0.255 established
r3(config-ext-nacl)#int g0/1
r3(config-if)#ip acc
r3(config-if)#ip access-group WEB_RETOUR out
r3(config-if)#exit
r3(config)#^Z
r3#
%SYS-5-CONFIG_I: Configured from console by console
sh acc
r3#sh access-lists
Extended IP access list WEB
    10 permit icmp 192.168.22.0 0.0.0.255 any echo (4 match(es))
    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#
```

```
Directed broadcast forwarding is disabl
Outgoing access list is WEB_RETOUR
Inbound  access list is WEB
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
```

```
r3#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
r3(config)#ip access
r3(config)#ip access-list EXT
r3(config)#ip access-list EXTended WEB_RETOUR
r3(config-ext-nacl)#20 deny ip any any
r3(config-ext-nacl)#exit
r3(config)#
```

Testons maintenant avec une requête ping depuis PC22 et regardons les compteurs des ACL.
La requête ICMP ne passe pas effectivement .

```
r3#sh access-lists WEB_RETOUR
Extended IP access list WEB_RETOUR
    permit tcp any 192.168.22.0 0.0.0.255 established
    deny ip any any

r3#
```

```
r3#
%SYS-5-CONFIG_I: Configured from console by console
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
    deny ip any any

r3#
```

Les retours de ping passent désormais.

Question 10

```
r3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r3(config)#ip acc
r3(config)#ip access-list extende
r3(config)#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
r3(config-ext-nacl)#
```

Comme 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, il suffit d'ajouter la permission en fin d'ACL. Enfin, il convient d'ajouter un refus explicite en fin de liste pour comptabiliser toutes les tentatives refusée