SOMMAIRE

1. ACL IPv4 standards

1.Configurez les PC

Les PC sont déjà configurés conformément à la topologie

2.Configurez le routeur R1

Je configure le nom du routeur,désactive la recherche DNS et je chiifre les mots de passe

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#service password-encryption
R1(config)#
```

Je protège l’accès enable avec le mot de passe class et j’ajoute un utilisateur admin avec comme mot de passe cisco

```
R1(config)#enable secret class
R1(config)#username admin secret cisco
R1(config)#
```

Je configure l’accès SSH avec l’utilisateur admin

```
R1(config)#ip domain-name CCNA-Lab.com
R1(config)#username admin privilege 15 secret sshadmin
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#
```

Je configure les interfaces G0/0, G0/1 et S0/0/0 du Routeur R1

G0/0 :

```
R1(config)#int g0/0
R1(config-if)#ip address 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
```

G0/1 :

```
R1(config-if)#int g0/1
R1(config-if)#ip address 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
```

S0/0/0 :

```
R1(config-if)#int s0/0/0
R1(config-if)#ip address 10.0.12.1 255.255.255.252
R1(config-if)#no shut
```

```
R1#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.11.254  YES manual up                    up
GigabitEthernet0/1     192.168.12.254  YES manual up                    up
Serial0/0/0            10.0.12.1       YES manual down                  down
```

3. Configuration du Routeur R2 :

Je configure le nom du Routeur, désactive la recherche DNS et j'active le chiffrement des mots de passe

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#service password-encryption
R2(config)#
```

Je mets comme mot de passe class pour le mode privilégié

```
R2(config)#enable secret class
R2(config)#
```

Je configure l'accès SSH et j'ajoute l'utilisateur admin

```
R2(config)#ip domain-name CCNA-Lab.com
R2(config)#username admin privilege 15 secret sshadmin
R2(config)#line vty 0 4
R2(config-line)#transport input ssh
R2(config-line)#login local
R2(config-line)#exit
R2(config)#
```

Je configure les interfaces sur le Routeur R2

S0/0/0 :

```
R2(config)#int s0/0/0
R2(config-if)#ip address 10.0.23.1 255.255.255.252
R2(config-if)#no shut
```

S0/0/1 :

```
R2(config-if)#int s0/0/1
R2(config-if)#ip address 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
```

Loopback :

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int loopback0
R2(config-if)#ip address 200.0.0.1 255.255.255.255
```

```
R2#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
Serial0/0/0            10.0.23.1       YES manual down                  down
Serial0/0/1            10.0.12.2       YES manual up                    up
Loopback0              200.0.0.1       YES manual up                    up
```

4. Configuration du Routeur R3

Configuration du Routeur R3

Je change le nom du Routeur,désactive la recherche DNS,chiffre les mots de passe et mets comme mot de passe class pour le mode privilégié

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#no ip domain-lookup
R3(config)#service password-encryption
R3(config)#enable secret class
R3(config)#
```

Je configure l’accès SSH et je mets un utilisateur admin

```
R3(config)#ip domain-name CCNA-Lab.com
R3(config)#username admin privilege 15 secret sshadmin
R3(config)#line vty 0 4
R3(config-line)#transport input ssh
R3(config-line)#login local
R3(config-line)#exit
R3(config)#
```

Je configure les interfaces du Routeur R3

G0/0 :

```
R3(config)#int g0/0
R3(config-if)#ip address 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
```

G0/1 :

```
R3(config-if)#int g0/1
R3(config-if)#ip address 192.168.22.254 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

S0/0/1 :

```
R3(config-if)#int s0/0/1
R3(config-if)#ip address 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
```

```
R3#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.21.254  YES manual up                    up
GigabitEthernet0/1     192.168.22.254  YES manual up                    up
Serial0/0/0            unassigned      YES unset  administratively down down
Serial0/0/1            10.0.23.2       YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R3#
```

5.Configuration de RIP V2

R1 :

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.12.0
R1(config-router)#network 192.168.11.0
R1(config-router)#network 10.0.12.0
R1(config-router)#no auto
R1(config-router)#no auto-summary
R1(config-router)#
```

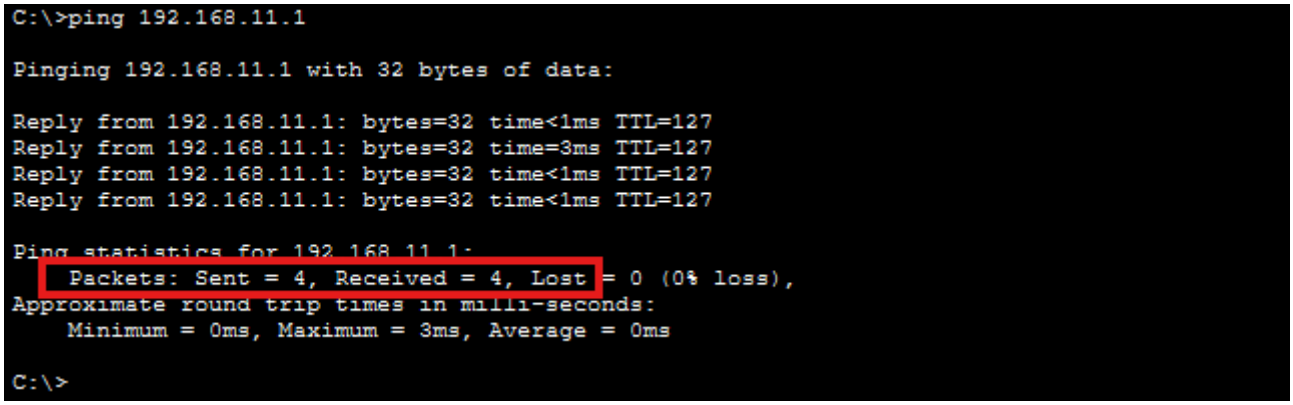
R2 :

```
R2(config-router)#network 10.0.12.0
R2(config-router)#network 10.0.23.0
R2(config-router)#network 200.0.0.0
R2(config-router)#
```

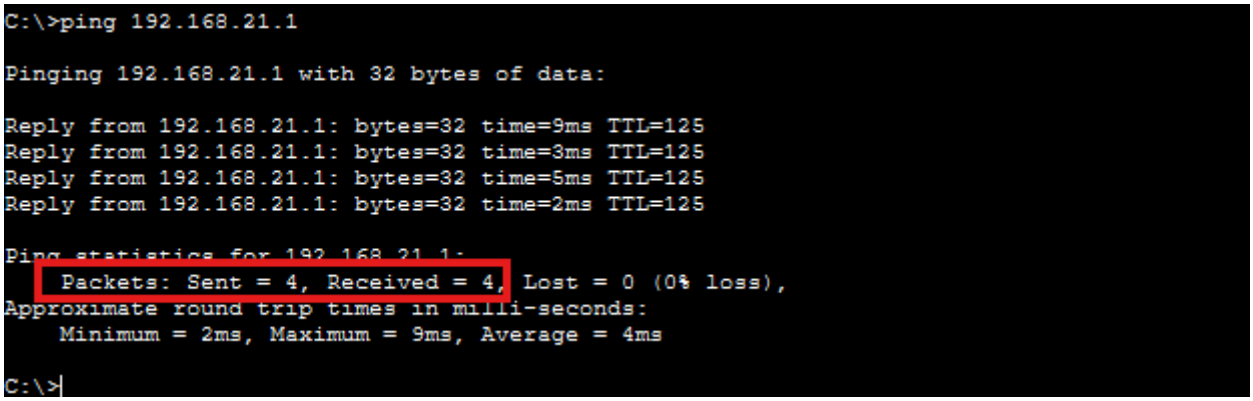
R3 :

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 192.168.21.0
R3(config-router)#network 192.168.22.0
R3(config-router)#network 10.0.23.0
R3(config-router)#no auto-summary
R3(config-router)#
```

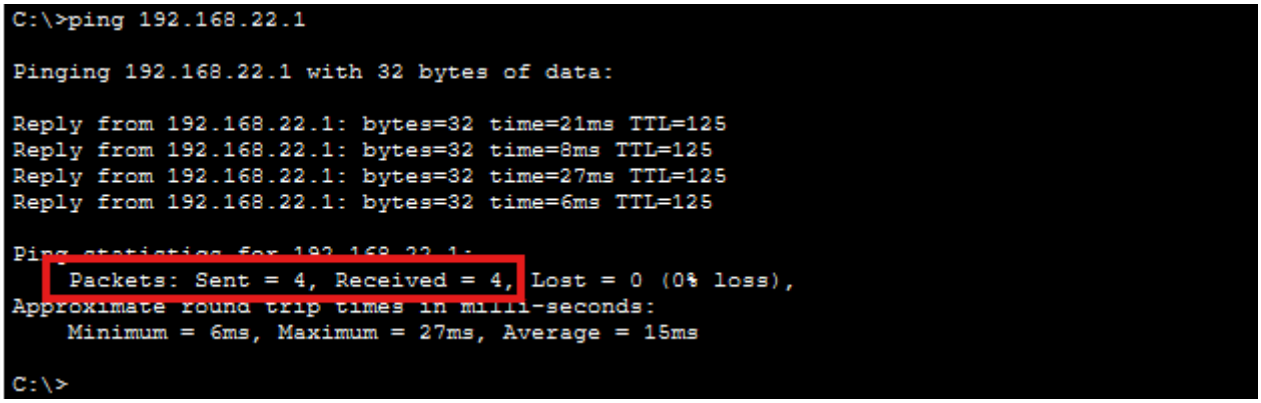
Ping PC-11 depuis PC-12



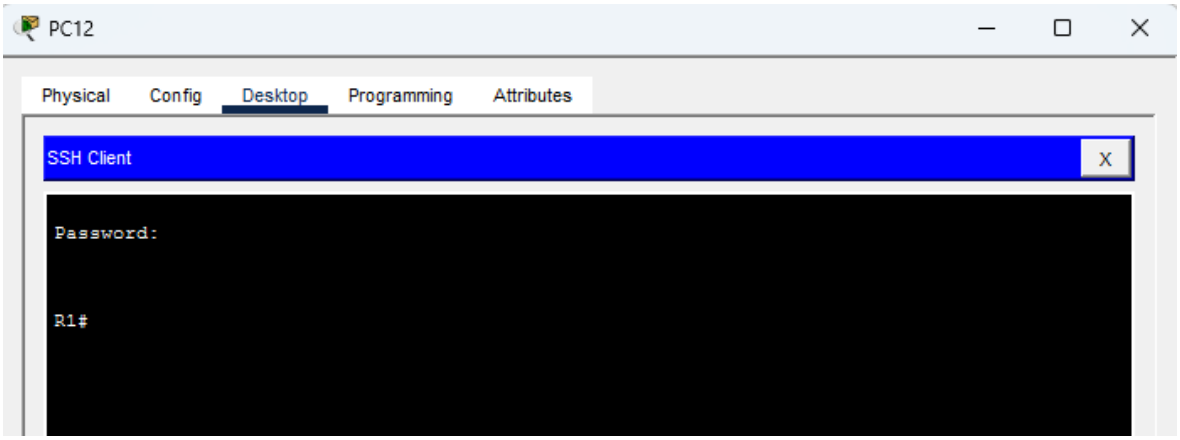
Ping PC-21 depuis PC-12

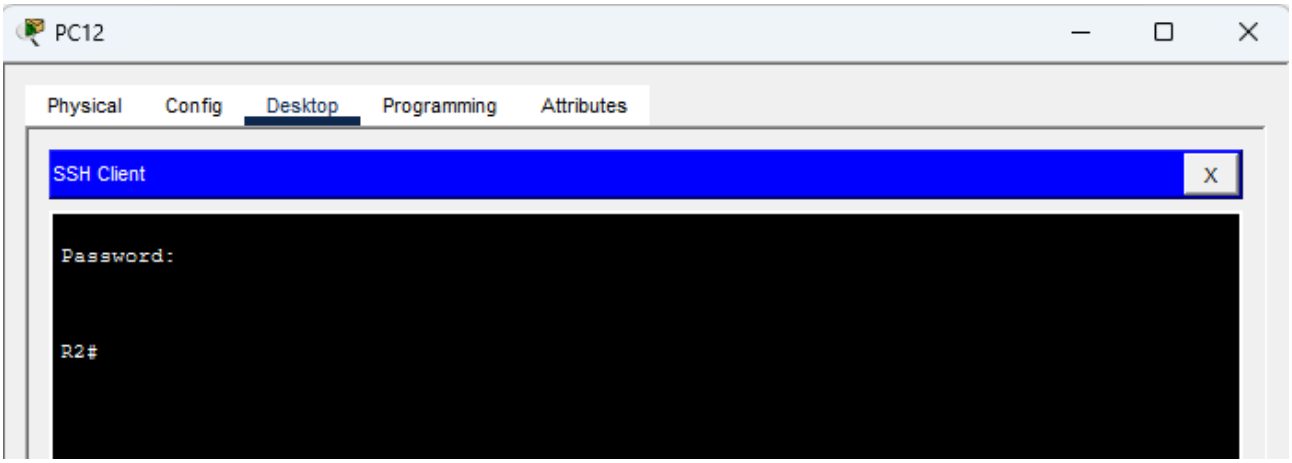


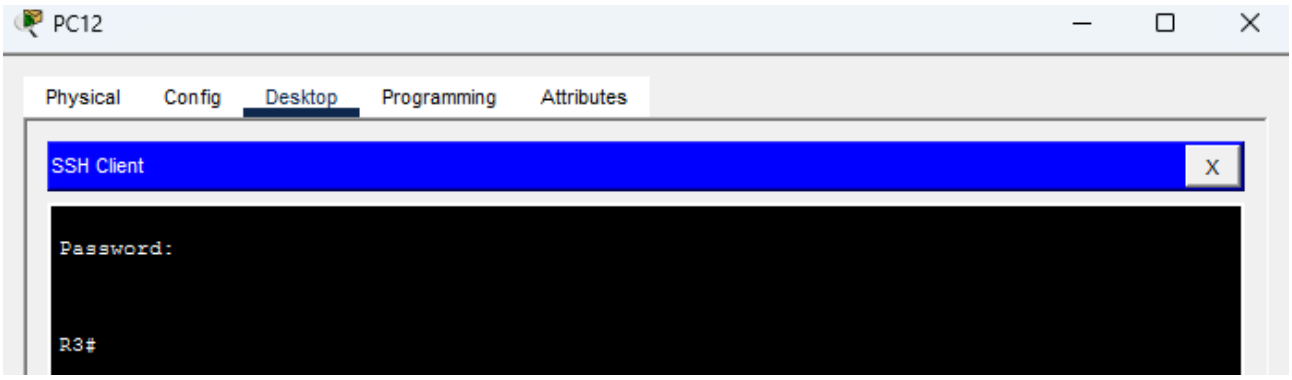
Ping PC-22 depuis PC-12



Je me connecte depuis PC-12 à tout les routeurs en SSH







Je créer une liste d'accès numérotée

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
```

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

On peut voir que maintenant le réseau 21 n'est plus joignable depuis PC-22

```
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:\>
```

En tapant la commande **sh access-lists** on peut voir le nombre de tentative

```
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))

R3#
```

Je mets les listes d’accès standard au plus près de la destination

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard ACCESS_LANN11
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)#
```

```
R1(config)#int g0/0
R1(config-if)#ip access-group ACCESS_LANN11 out
R1(config-if)#exit
R1(config)#
```

```
R1#sh access-lists
Standard IP access list ACCESS_LANN11
    10 permit 192.168.22.0 0.0.0.255
    20 permit host 192.168.21.1

R1#
```

Depuis PC-21 je ping PC-11

```
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=18ms TTL=125
Reply from 192.168.11.1: bytes=32 time=10ms TTL=125
Reply from 192.168.11.1: bytes=32 time=35ms 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 = 10ms, Maximum = 35ms, Average = 19ms

C:\>
```

Avec la commande sh access-lists je peux voir le nombre de paquets autorisés

```
R1#sh access-lists
Standard IP access list ACCESS_LANN11
    10 permit 192.168.22.0 0.0.0.255
    20 permit host 192.168.21.1 (4 match(es))

R1#
```

Je ping PC-11 depuis PC-22

```
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=15ms TTL=125
Reply from 192.168.11.1: bytes=32 time=38ms TTL=125
Reply from 192.168.11.1: bytes=32 time=30ms 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 = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 38ms, Average = 21ms

C:\>
```

Je ping PC-11 depuis PC-12

```
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),

C:\>
```

Je retape la commande **sh access-lists** sur le routeur R1

```
R1#sh access-lists
Standard IP access list ACCESS_LANN11
    10 permit 192.168.22.0 0.0.0.255 (4 match(es))
    20 permit host 192.168.21.1 (4 match(es))

R1#
```

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard ACCESS_LANN11
R1(config-std-nacl)#no 20 permit host 192.168.21.0 0.0.0.255
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)#
```

Je ping PC-11 depuis PC-12

```
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),

C:\>
```

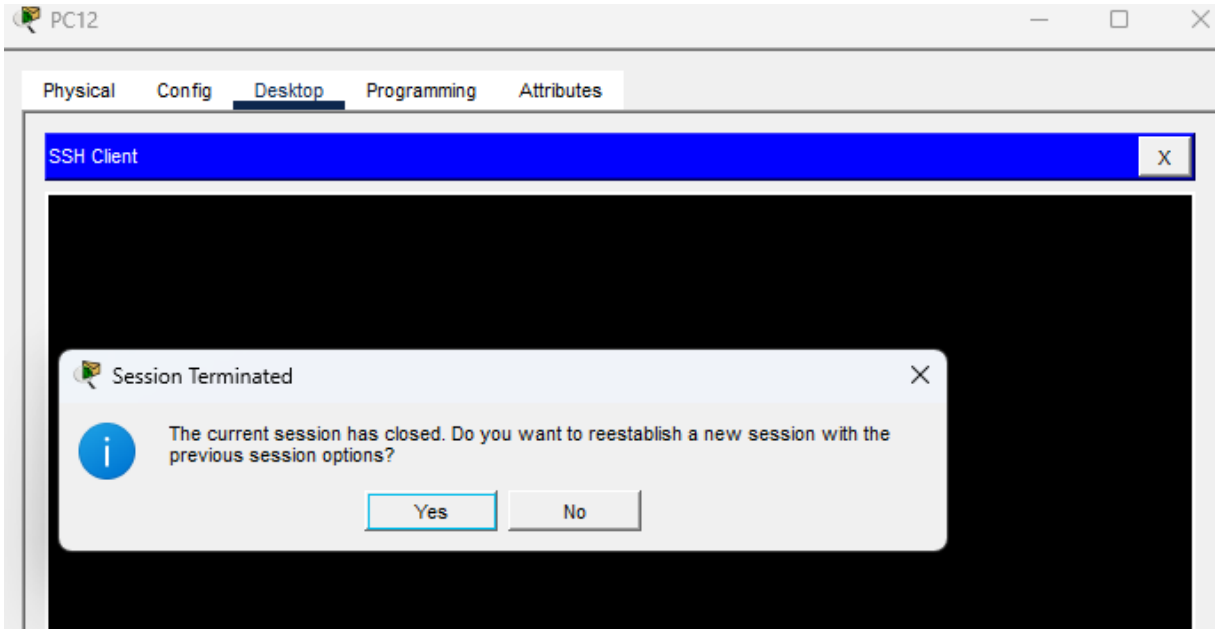
```
R1#sh access-lists
Standard IP access list ACCESS_LANN11
    10 permit 192.168.22.0 0.0.0.255 (4 match(es))
    20 permit 192.168.21.0 0.0.0.255
    30 deny any (4 match(es))

R1#
```

Je créer une liste d'accès standard nommée ACCESS_SSH_ADMIN pour sécuriser les accès SSH

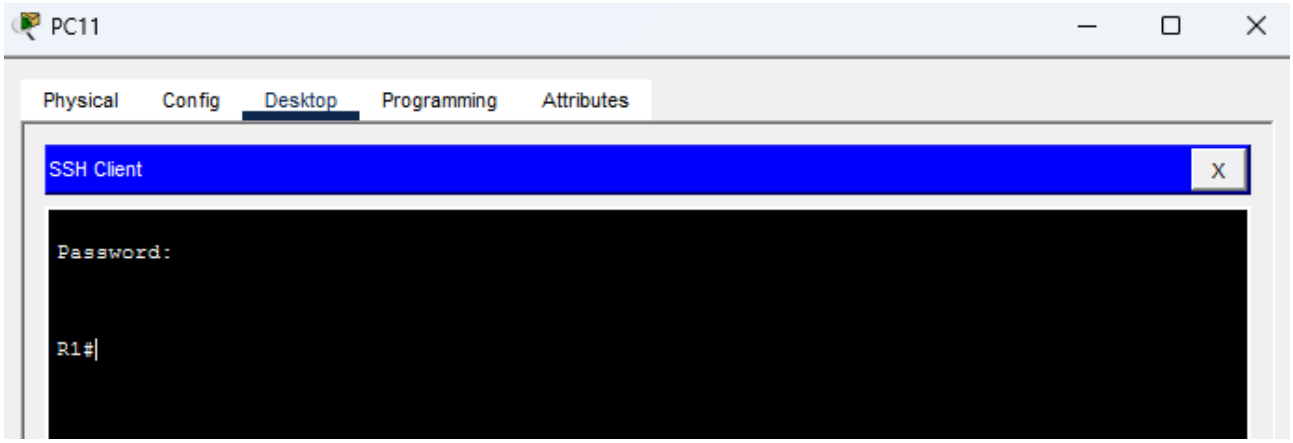
```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip access-list standard ACCESS_SSH_ADMIN
R1(config-std-nacl)#permit 192.168.11.0 0.0.0.255
R1(config-std-nacl)#
```

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
```

Depuis PC-12 il n’est pas possible de se connecter en SSH au routeur R1



Depuis PC-11 ça fonctionne car ils sont sur le même réseau



2. ACL IPv4 étendues

Sur R1 je configure OSPF

```
R1(config-router)#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 100000
R1(config-if)#int g0/1
R1(config-if)#bandwidth 100000
R1(config-if)#int s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#
```

Sur R2 je configure OSPF

```
R2(config)#router ospf 1
R2(config-router)#auto-cost reference-bandwidth 1000
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)#
02:26:20: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.12.254 on Serial0/0/1 from LOADING to
FULL, Loading Done
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)#
```

Sur R3 je configure OSPF

```
R3(config-router)#router ospf 1
R3(config-router)#auto-cost reference-bandwidth 1000
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
02:28:49: %OSPF-5-ADJCHG: Process 1, Nbr 200.0.0.1 on Serial0/0/1 from LOADING to FULL,
Loading Done

R3(config-router)#passive-interface g0/1
R3(config-router)#int g0/0
R3(config-if)#bandwidth 100000
R3(config-if)#int g0/1
R3(config-if)#bandwidth 100000
R3(config-if)#int s0/0/1
R3(config-if)#bandwidth 128
R3(config-if)#
```

Je vérifie que depuis R3 les routes de R1 et R2 sont apprises

```
R3#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, 00:01:46, Serial0/0/1
O    192.168.11.0 [110/1304] via 10.0.23.1, 00:01:46, Serial0/0/1
O    192.168.12.0 [110/1304] via 10.0.23.1, 00:01:46, Serial0/0/1

R3#
```

Je créer deux ACL et les appliques aux interfaces

```
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)#int g0/0
R1(config-if)#ip access-group 111 in
R1(config-if)#int g0/1
R1(config-if)#ip access-group 112 in
R1(config-if)#
```

Ping depuis PC-11

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.0.0.1

Pinging 200.0.0.1 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.

Ping statistics for 200.0.0.1:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

Control-C
^C
C:\>
```

```
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=36ms TTL=125
Reply from 192.168.21.1: bytes=32 time=36ms TTL=125
Reply from 192.168.21.1: bytes=32 time=37ms 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 = 36ms, Maximum = 37ms, Average = 36ms
```

Sur R3 je créer une ACL étendue

```
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)#
```

J’applique sur l’interface G0/1 en entrée

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

Je créer une ACL étendue et je l'applique sur l'interface G0/1 en sortie pour autoriser les ping retour

```
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)#
```

Je vérifie les ACL

```
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#
```

```
R3#sh ip int 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
```

Je modifie l'ACL

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

Depuis PC-22 je fais ping

```
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),
```

Je modifie l'ACL pour autoriser les requêtes ICMP

```
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
R3(config-ext-nacl)#
```

Je modifie l'ACL WEB

```
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)#
```