Université Sultan Moulay Slimane Faculté Polydisciplinaire Béni Mellal
Département INFORMATIQUE (MIP)

Filière : Science de données et sécurité des systèmes d'information
A.U : 2023-2024
Module : Réseaux Informatiques

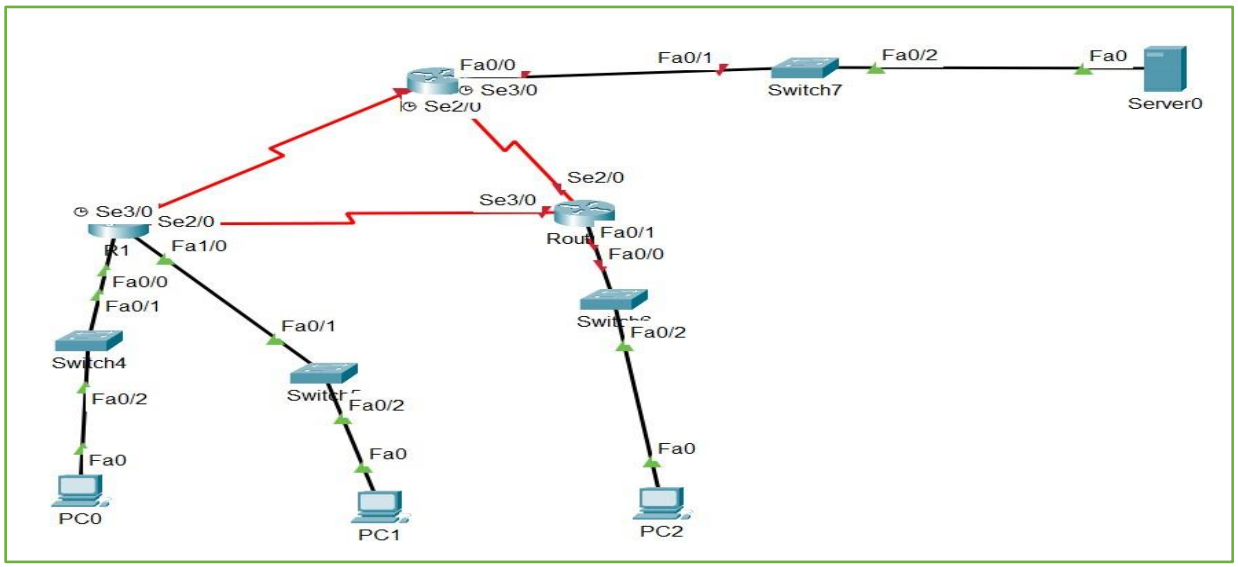
Sujet

Rapport TP05

Présenté Par :
MAFTOUH Omar
KHADIM Mohamed Hamza

Encadré Par :
Pr : FARISS Meriam

Partie 01 : Configuration des listes de contrôle d'accès standard



1) Planification d'une implémentation de la liste de contrôle d'accès :

a. Etape 01 : Configuration de la topologie :

a) Configuration de routeur R1 :

```
R1(config)#int fa1/0
R1(config-if)#ip add 192.168.11.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
exit
R1(config)#int se3/0
R1(config-if)#ip add 10.1.1.1 255.255.255.252
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial3/0, changed state to down
R1(config-if)#int se2/0
R1(config-if)#ip add 10.3.3.1 255.255.255.252
```

b) Configuration RIP v2 sur R1 :

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.10.0
R1(config-router)#network 192.168.11.0
R1(config-router)#network 10.1.1.0
R1(config-router)#network 10.3.3.0
R1(config-router)#passive-interface fa0/0
R1(config-router)#passive-interface fa1/0
```

c) Configuration des interfaces de R2 :

```
R2(config)#int SE2/0
R2(config-if)#IP ADDRESS 10.1.1.2 255.255.255.252
R2(config-if)#NO SHUT

R2(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

R2(config-if)#int SE3/0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

R2(config-if)#IP ADDRESS 10.2.2.1 255.255.255.252
R2(config-if)#NO SHUT

%LINK-5-CHANGED: Interface Serial3/0, changed state to down
R2(config-if)#int FA0/0
R2(config-if)#IP ADDRESS 192.168.20.1 255.255.255.0
R2(config-if)#NO SHUT

R2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

d) Configuration RIP sur R2

```
R2(config)#ROUTER RIP
R2(config-router)#VERSION 2
R2(config-router)#NETWORK 192.168.20.0
R2(config-router)#NETWORK 10.1.1.0
R2(config-router)#NETWORK 10.2.2.0
R2(config-router)#NO AUTO-SUMMARY
R2(config-router)#PASSIVE-INTERFACE FA0/0
```

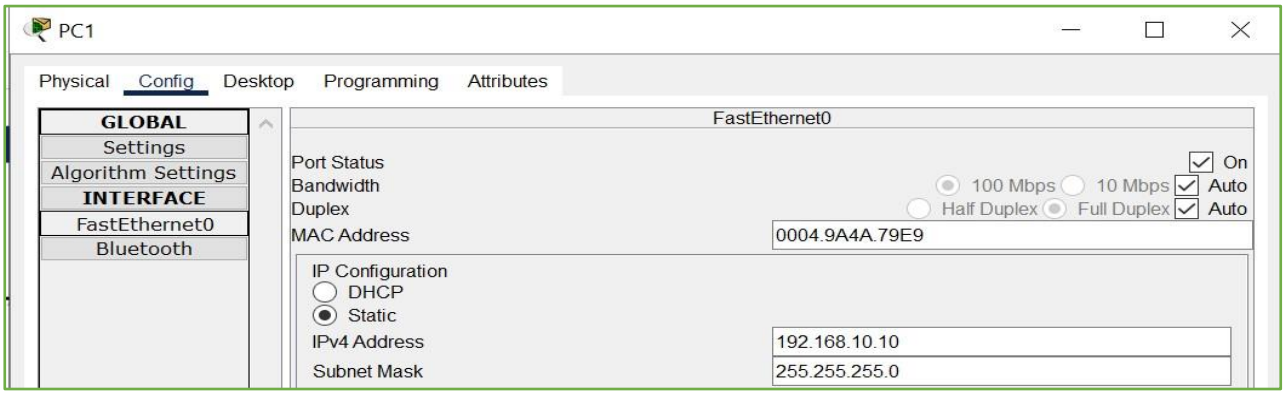
e) Configuration des interfaces de R3 :

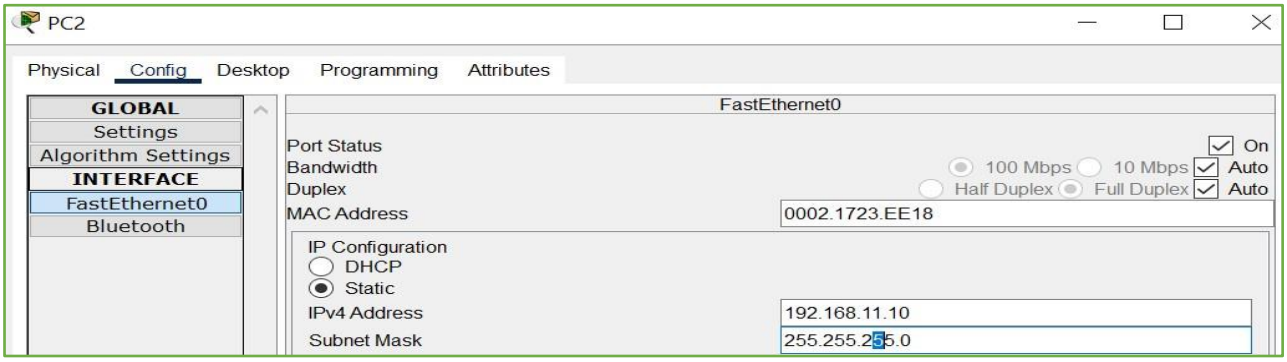
```
R3(config)#INT FA0/1
%Invalid interface type and number
R3(config)#int fa0/1
%Invalid interface type and number
R3(config)#INT SE2/0
R3(config-if)#IP ADDRESS 10.2.2.2 255.255.255.252
R3(config-if)#NO SHUT
R3(config-if)#INT SE3/0
R3(config-if)#IP ADDRESS 10.3.3.2 255.255.255.252
R3(config-if)#NO SHUT
R3(config-if)#INT FA0/0
R3(config-if)#IP ADDRESS 192.168.30.1 255.255.255.0
R3(config-if)#NO SHUT

R3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

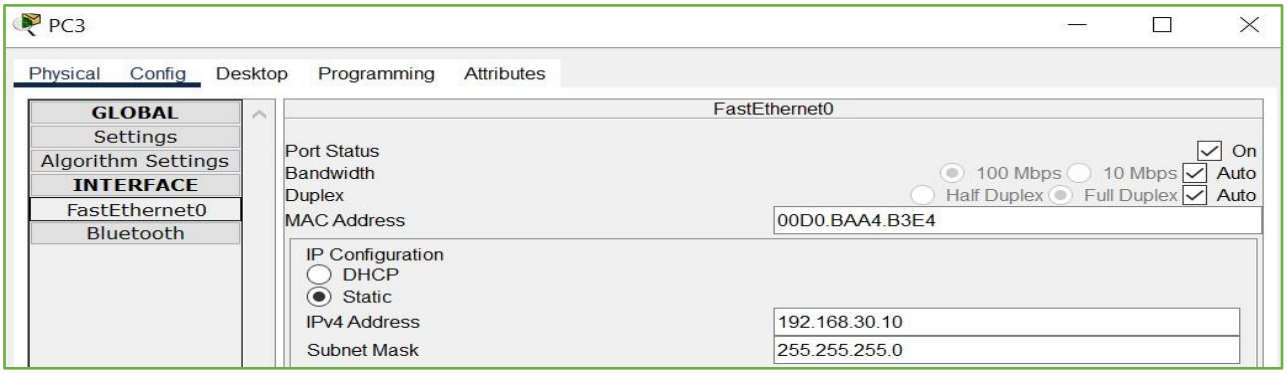
f) Configuration RIP sur R3 :

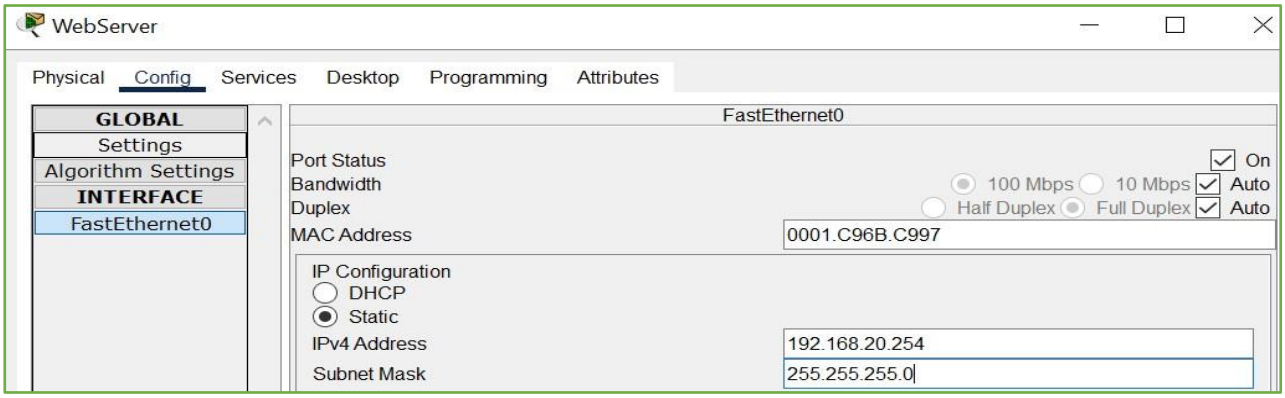
```
R3(config)#ROUTER RIP
R3(config-router)#VERSION 2
R3(config-router)#NETWORK 192.168.30.0
R3(config-router)#NETWORK 10.3.3.0
R3(config-router)#NETWORK 10.2.2.0
R3(config-router)#NO AUTO-SUMMARY
R3(config-router)#PASSIVE-INTERFACE FA0/0
```

g) Configuration PCs & serveur web :









b. Etape 02 : Etudier la configuration réseau actuelle :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2	WebServer	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC3	WebServer	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	WebServer	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC1	PC3	ICMP		0.000	N	3	(edit)	(delete)

2) Configuration, application et vérification d'une liste de contrôle d'accès standard :

a. Etape 01 : Configuration et application d'une liste de contrôle d'accès standard numérotée sur R2 :

```
R2(config)#ACCESS-LIST 1 DENY 192.168.11.0 0.0.0.255
R2(config)#ACCESS-LIST 1 PERMIT ANY
R2(config)#INT FA0/0
R2(config-if)#IP ACCESS-GROUP 1 OUT
```

b. Etape2 : Configuration et application une liste de contrôle d'accès standard numérotée sur R3 :

```
R3(config)#ACCESS-LIST 1 DENY 192.168.10.0 0.0.0.255
R3(config)#ACCESS-LIST 1 PERMIT ANY
R3(config)#INT FA0/0
R3(config-if)#IP ACCESS-GROUP 1 OUT
```

c. Etape 03 : Vérification de la configuration et le fonctionnement des listes de contrôle d'accès :

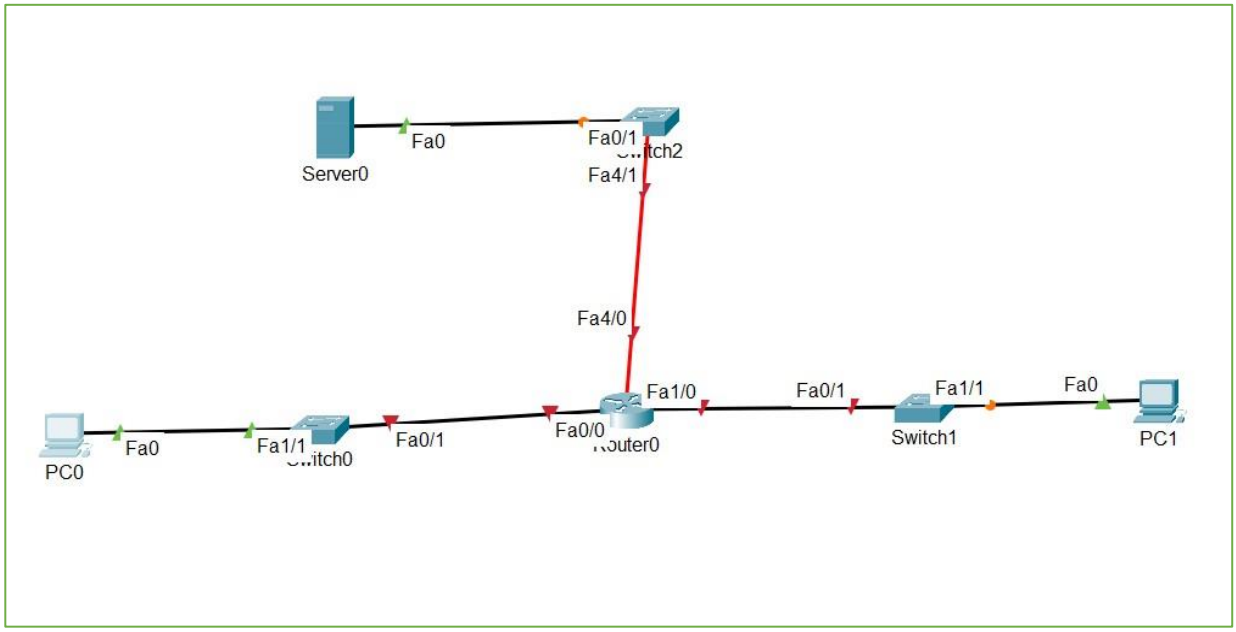
```
R3#SHOW ACCESS-LIST
Standard IP access list 1
    10 deny 192.168.10.0 0.0.0.255
    20 permit any
```

```
Standard IP access list 1
    10 deny 192.168.11.0 0.0.0.255
    20 permit any
```

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	PC2	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	WebServer	ICMP		0.000	N	1	(edit)	(delete)
	Failed	PC2	WebServer	ICMP		0.000	N	2	(edit)	(delete)

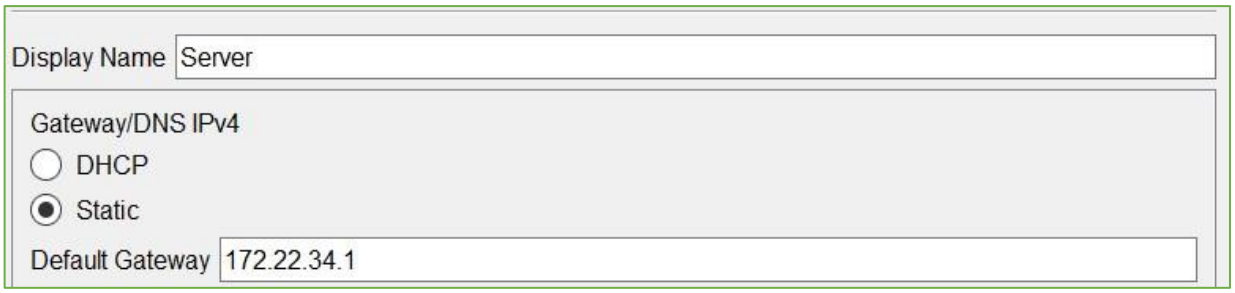
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC1	PC3	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC2	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC3	WebServer	ICMP		0.000	N	2	(edit)	(delete)

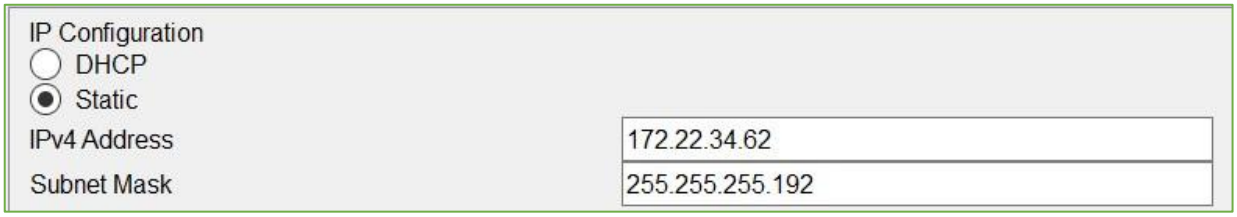
Partie 02 : Configuration des listes de contrôle d'accès étendues

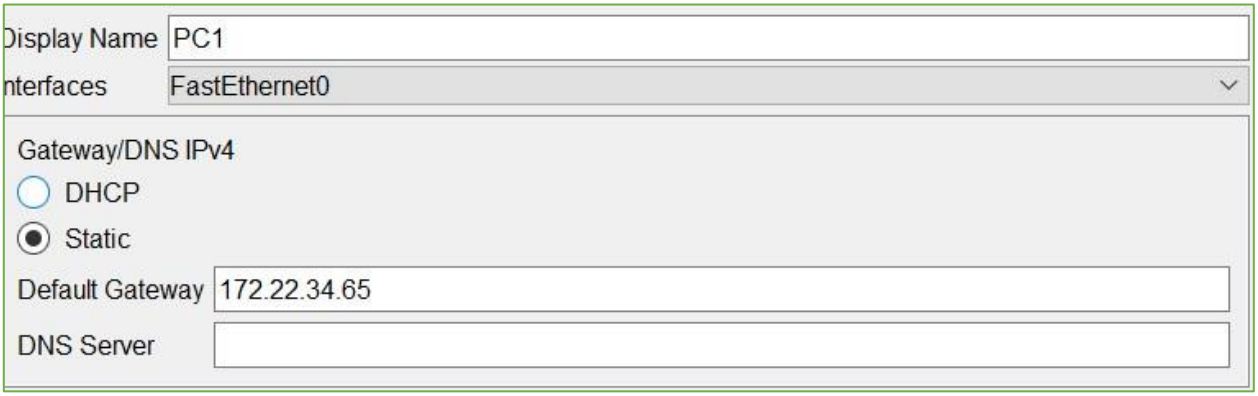


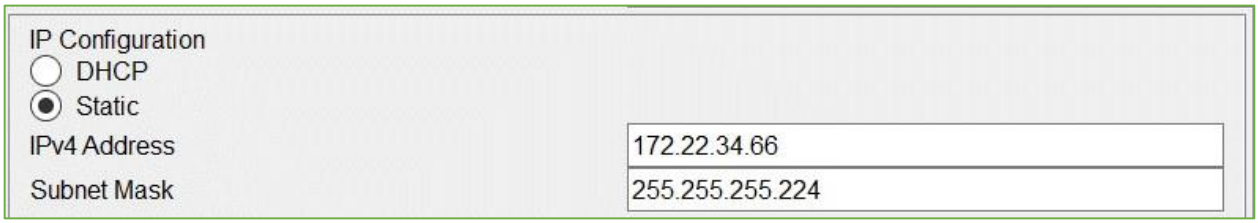
1) Configuration, application et vérification d'une liste de contrôle d'accès numérotée étendue :

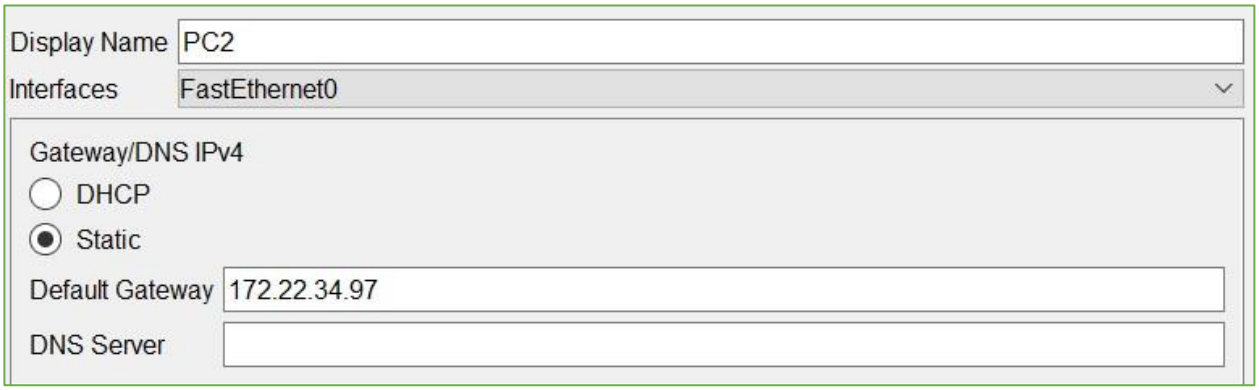
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int fa0/0
R1(config-if)#ip add 172.22.34.65 255.255.255.224
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
exit
R1(config)#int fa1/0
R1(config-if)#ip add 172.22.34.97 255.255.255.240
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
exit
R1(config)#int fa4/0
R1(config-if)#ip add 172.22.34.1 255.255.255.192
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet4/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet4/0, changed state to up
exit
```

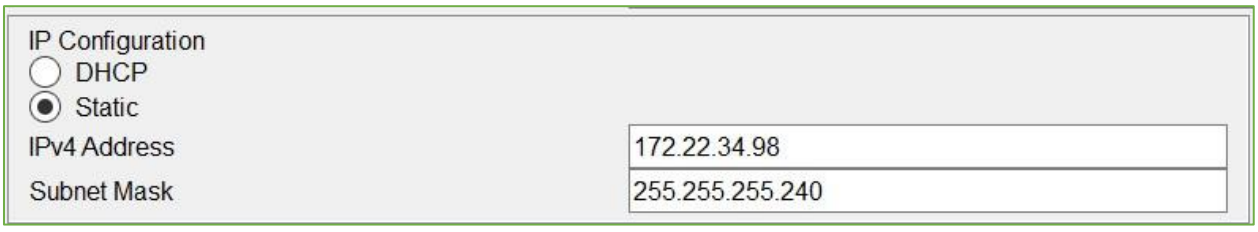












Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	Server	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Server	PC2	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	PC2	ICMP		0.000	N	2	(edit)	(delete)

a. Etape 01 : Configuration d'une liste de contrôle d'accès pour autoriser l'accès PTP et ICMP :

```
R1(config)#access-list ?
  <1-99>      IP standard access list
  <100-199>   IP extended access list
```

A

```
R1(config)#access-list 100 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
```

B

```
R1(config)#access-list 100 permit ?
  ahp     Authentication Header Protocol
  eigrp   Cisco's EIGRP routing protocol
  esp     Encapsulation Security Payload
  gre     Cisco's GRE tunneling
  icmp    Internet Control Message Protocol
  ip      Any Internet Protocol
  ospf    OSPF routing protocol
  tcp     Transmission Control Protocol
  udp     User Datagram Protocol
```

C

```
R1(config)#access-list 100 permit tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
```

D

```
R1(config)#access-list 100 permit tcp 172.22.34.64 ?
  A.B.C.D  Source wildcard bits
```

E

f. Le masque générique est **0.0.0.31**

```
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?
  A.B.C.D  Destination address
  any      Any destination host
  eq       Match only packets on a given port number
  gt       Match only packets with a greater port number
  host     A single destination host
  lt       Match only packets with a lower port number
  neq      Match only packets not on a given port number
  range    Match only packets in the range of port numbers
```

G

```
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?
  dscp          Match packets with given dscp value
  eq            Match only packets on a given port number
  established   established
  gt            Match only packets with a greater port number
  lt            Match only packets with a lower port number
  neq           Match only packets not on a given port number
  precedence    Match packets with given precedence value
  range         Match only packets in the range of port numbers
  <cr>
```

H

```
R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?
  <0-65535>  Port number
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80)
```

I

```
R1(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
```

J

```
R1(config)#access-list 100 deny icmp any any
```

K

b. Etape 02 : Appliquer la liste de contrôle d'accès sur l'interface appropriée pour filtrer le trafic :

```
R1(config)#int fa0/0
R1(config-if)#ip access-group 100 in
```

c. Etape 03 : Vérifier l'implémentation de la liste de contrôle d'accès :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	Server	ICMP		0.000	N	0	(edit)	(delete)

A

```
C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62

%Error opening ftp://172.22.34.62/ (Timed out)
.
```

B

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC1	PC2	ICMP		0.000	N	0	(edit)	(delete)

C

2) Configuration, application et vérification d'une liste de contrôle d'accès nommée étendue :

a. Etape 01 : Configurer une liste de contrôle d'accès pour autoriser l'accès HTTP et ICMP :

```
R1(config)#Ip access-list ?
  extended  Extended Access List
  standard  Standard Access List
```

A

```
R1(config)#Ip access-list extended HTTP_ONLY
R1(config-ext-nacl)#
```

B

```
R1(config-ext-nacl)#permit tcp 172.22.34.96 ?
  A.B.C.D  Source wildcard bits
```

C

```
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 ?
  A.B.C.D  Destination address
  any      Any destination host
  eq       Match only packets on a given port number
  gt       Match only packets with a greater port number
  host     A single destination host
  lt       Match only packets with a lower port number
  neq      Match only packets not on a given port number
  range    Match only packets in the range of port numbers
```

D

```
R1(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
```

E

```
R1(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

F

```
R1(config-ext-nacl)#deny ip any any
R1(config-ext-nacl)#exit
```

G

b. Etape 02 : Appliquer une liste de contrôle d'accès sur l'interface appropriée pour filtrer le trafic :

```
R1(config)#int fa1/0
R1(config-if)#ip access-group HTTP_ONLY in
```

c. Etape 03 : Vérifier l'implémentation de la liste de contrôle d'accès :

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2	Server	ICMP		0.000	N	0	(edit)	(delete)

A

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62

%Error opening ftp://172.22.34.62/ (Timed out)
.
```

B

C