

RAPPORT EXERCICE ACL

HAROUNI DJIHANE

171731091986

M1 SSI SERE

1/ La configuration des @ ip des pcs et la configuration des interfaces router était en suivant les @ mentionnés dans l'énoncé et par rapport à quel vlan ils appartiennent Création et configuration des VLAN. (puisque ya la connectivité dans les @ sont bien correctes)

2/ Configuration des interfaces des Routeurs R1 -> R3 :

DHCP

Physical Config **CLI** Attributes

IOS Command Line Interface

2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

```
Router>enable
Router#
Router>configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet1/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up
ip address 192.168.12.1 255.255.255.0
Router(config-if)#ip address 192.168.12.1 255.255.255.0
Router(config-if)#ip address 192.168.12.1 255.255.255.252
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#interface FastEthernet1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#interface FastEthernet1/0
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
```

3/ Création des VLANs : 20 && 50 && 70 :

```

Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch(config-if)#
Switch#
%SYS-5-CONFIG_I: Configured from console by console
vtp mode server
^
% Invalid input detected at '^' marker.

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#vtp domain SSI
Changing VTP domain name from NULL to SSI
Switch(config)#VTP Password cisco
Setting device VLAN database password to cisco
Switch(config)#VLAN 20
Switch(config-vlan)#name SSI-G1
Switch(config-vlan)#EXIT
Switch(config)#VLAN 50
Switch(config-vlan)#name SSI-G2
Switch(config-vlan)#EXIT
Switch(config)#VLAN 70
Switch(config-vlan)#name SSI-deleuge
Switch(config-vlan)#exit
Switch(config)#

```

Et là on remarque la propagation des messages et Vlan grâce à VTP:

VLAN Name	Status	Ports
1 default	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
20 SSI-G1	active	Fa0/1, Fa0/3
50 SSI-G2	active	Fa0/2
70 SSI-deleuge	active	Fa0/4, Fa0/6
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trmet-default	active	

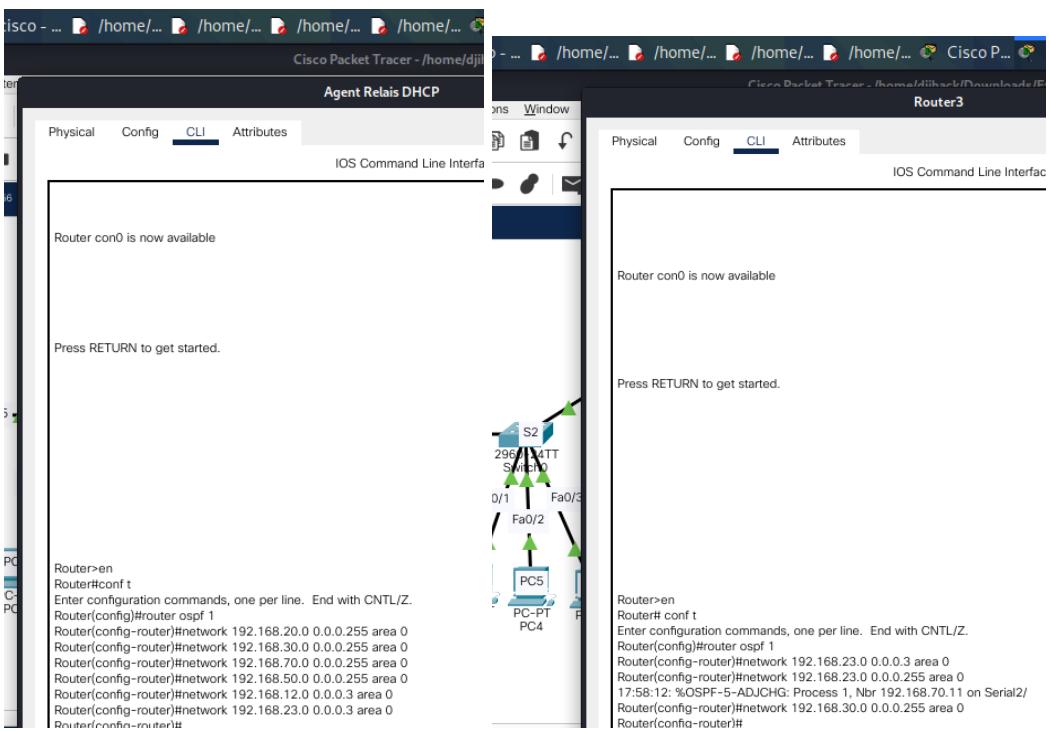
VLAN Name	Status	Ports
1 default	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
20 SSI-G1	active	Fa0/2
50 SSI-G2	active	Fa0/1, Fa0/3
70 SSI-deleuge	active	Fa0/6
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trmet-default	active	

4/ Configuration des ports des commutateurs S1 && S2: j'ai oublié de prendre un capture dans vous trouverez ci dessous les commandes de la configuration de S2.

// on doit mettre l'interface f0/5 de S1 ou S2 en mode trunk aussi f0/4 de S2 et enfin f0/3 de S3 pour permettre l'accès du trafic .

```
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport access vlan 50
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport access vlan 20
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport access vlan 50
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/5
```

5/ Configuration du Routage inter-VLANs



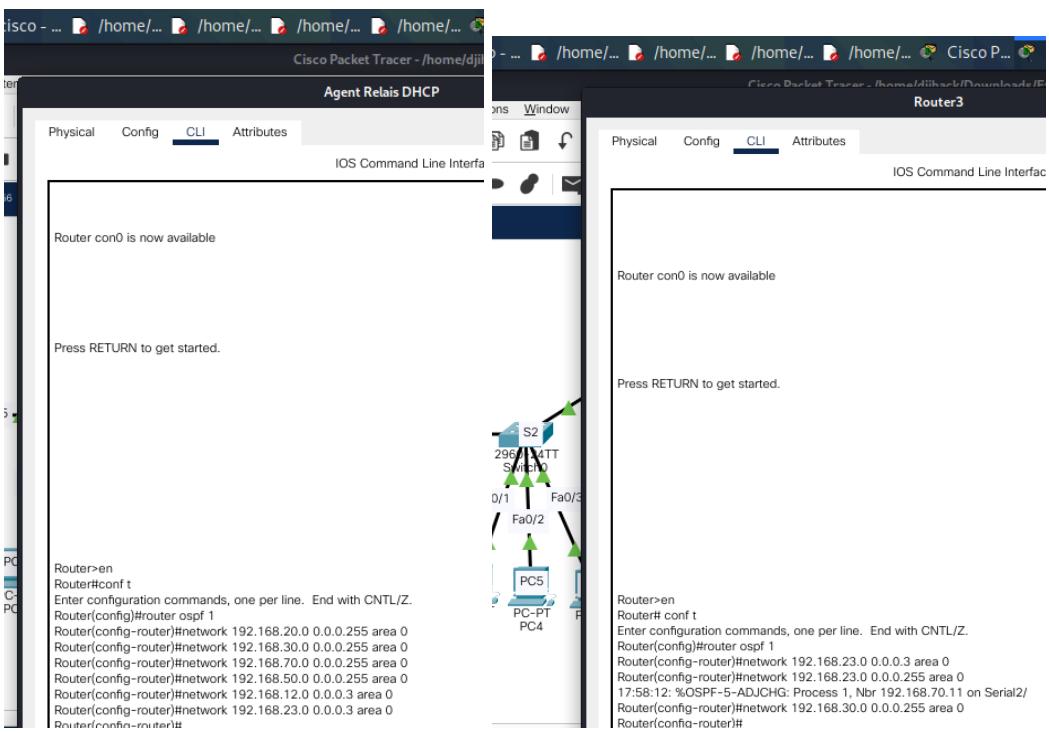
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
18:44:42: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.10 on Serial2/0 from LOADING to FULL, Loading Done

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int f0
Router(config)#int f0/0.1
Router(config-subif)#ip he
Router(config-subif)#ip hel
Router(config-subif)#ip helper
Router(config-subif)#ip helper-address 192.168.12.^
% Invalid input detected at '^' marker.

Router(config-subif)#end
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int FastEthernet1/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console

Router(config-if)#ip helper-address 192.168.12.2
Router(config-if)#exit
Router(config)#int f0/0.2
Router(config-subif)#ip helper-address 192.168.12.2
Router(config-subif)#int f0/0.3
Router(config-subif)#ip helper-address 192.168.12.2
Router(config-subif)#int s2/0
Router(config-if)#ip helper-address 192.168.12.2
Router(config-if)#
Press RETURN to get started.
```

6/ Configuration du Routage: j'ai choisi d'utiliser le routage ospf :

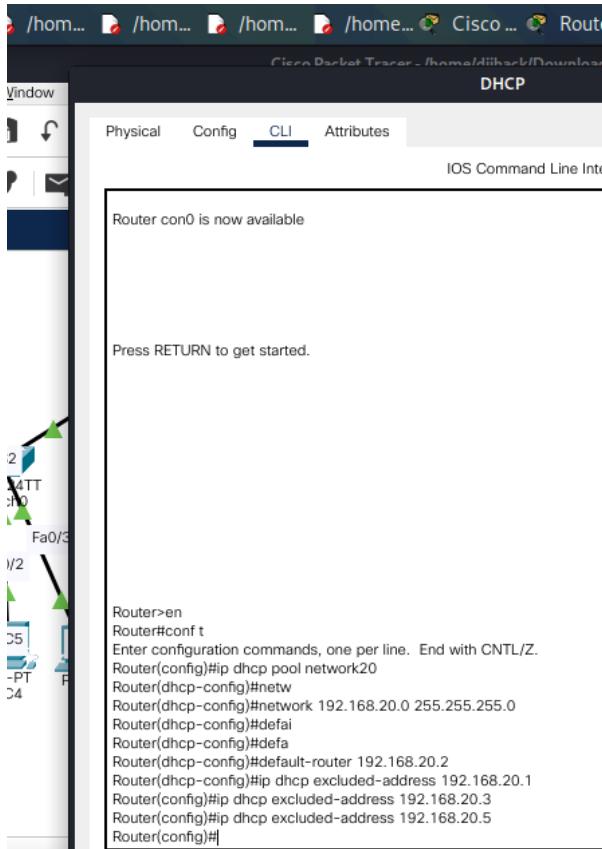


```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.20.0 0.0.0.255 area 0
Router(config-router)#network 192.168.30.0 0.0.0.255 area 0
Router(config-router)#network 192.168.70.0 0.0.0.255 area 0
Router(config-router)#network 192.168.50.0 0.0.0.255 area 0
Router(config-router)#network 192.168.12.0 0.0.0.3 area 0
Router(config-router)#network 192.168.23.0 0.0.0.3 area 0
Router(config-router)#
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.23.0 0.0.0.3 area 0
Router(config-router)#network 192.168.30.0 0.0.0.255 area 0
Router(config-router)#
Press RETURN to get started.
```

7/ Test de la connectivité: on voit que le ping fonctionne bien entre l'agence relais et les PCs des différents vlan.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
,	Successful	Agen...	PC5	IC...	grey	0.000	N	20	(e...)	(delete)
,	Failed	Agen...	PC1	IC...	blue	0.000	N	21	(e...)	(delete)
,	Successful	PC3	Agent Rel...	IC...	red	0.000	N	22	(e...)	(delete)
,	Successful	PC1	Agent Rel...	IC...	blue	0.000	N	23	(e...)	(delete)

8/ Configuration du Protocole DHCP au niveau de R1



The screenshot shows two Cisco routers, Router1 and Router3, connected via their Serial2/0 interfaces. Router1 has several FastEthernet interfaces (Fa0/0, Fa0/1, Fa0/2, Fa0/3) and a GigabitEthernet interface (I/2). Router3 has one FastEthernet interface (I/2). A PC is connected to Router1's Fa0/1 interface. The configuration windows for both routers are open, showing the CLI tab.

Router1 Configuration (CLI tab):

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool network20
Router(dhcp-config)#netw
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#defai
Router(dhcp-config)#defa
Router(dhcp-config)#default-router 192.168.20.2
Router(dhcp-config)#ip dhcp excluded-address 192.168.20.1
Router(config)#ip dhcp excluded-address 192.168.20.3
Router(config)#ip dhcp excluded-address 192.168.20.5
Router(config)#

```

Router3 Configuration (CLI tab):

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
18:44:42: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.10 on Serial2/0 is now adjacent
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int f0/0.1
Router(config)#ip he
Router(config)#hel
Router(config)#helper
Router(config)#ip helper-address 192.168.12.2
^
% Invalid input detected at '^' marker.

Router(config-subif)#end
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet1/0
Router(config-if)#%
%SYS-5-CONFIG\_!: Configured from console by console
Router(config-if)#ip helper-address 192.168.12.2
Router(config-if)#exit
Router(config)#interface f0/0.2
Router(config-subif)#ip helper-address 192.168.12.2
Router(config-subif)#interface f0/0.3
Router(config-subif)#ip helper-address 192.168.12.2
Router(config-subif)#interface s2/0
Router(config-if)#ip helper-address 192.168.12.2
Router(config-if)#

```

Là on vient de configurer le serveur dhcp au niveau de DHCP et on devait aussi extraire les adresses déjà prise de chaque vlan pour que le serveur ne les attribue pas à l'autre machine au futur.

10/ Création des ACLs qui respectent les règles suivantes

Règle 01 :

L'Accès Telnet est refusé uniquement au réseau LAN-R3 au niveau de R2

On remarque qu'au début quand l'ACL était active on avait host not responding et après l'avoir désactivé on arrive à accéder via telnet au routeur R2 d'après PC8.

RAPPORT... */home/dji... /home/djih... Cisco Pack... Agent Rela... PC7 Sécurité

Cisco Packet Tracer - /home/djihack/Downloads/ExerciceACL.pkt

Agent Relais DHCP

Physical Config CLI Attributes

IOS Command Line Interface

```
% Invalid input detected at '^' marker.

Router(config-ext-nacl)#deny tcp 192.168.30.0 0.0.0.255 192.168.23.1 eq 23
^
% Invalid input detected at '^' marker.

Router(config-ext-nacl)#deny t
Router(config-ext-nacl)#deny tcp 192.168.30.0 0.0.0.255 192.168.23.1 eq 23
^
% Invalid input detected at '^' marker.

Router(config-ext-nacl)#de
Router(config-ext-nacl)#den
Router(config-ext-nacl)#deny tc
Router(config-ext-nacl)#deny tcp
% Incomplete command.
Router(config-ext-nacl)#deny tcp 192.168.30.0
% Incomplete command.
Router(config-ext-nacl)#deny tcp 192.168.30.0
Router(config-ext-nacl)#deny tcp 192.168.30.0 0.0.0.255
Router(config-ext-nacl)#deny tcp 192.168.30.0 0.0.0.255 host 192.168.23.1 eq 23
Router(config-ext-nacl)#permit any any
^
% Invalid input detected at '^' marker.

Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#ip a
Router(config)#
Router(config)#interface s 2/0
Router(config-if)#ip ac
Router(config-if)#ip access-group notelnet in
Router(config-if)#no ip access-group notelnet in
Router(config-if)#

```

Physical Config Desktop Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.23.1
Trying 192.168.23.1 ...
% Connection timed out; remote host not responding
C:\>telnet 192.168.23.1
Trying 192.168.23.1 ...Open
```

User Access Verification

```
Password:
Password:
Router>
```

Règle 02 :

Seul le G2 de la M1SSI est autorisé à administrer R3 à Distance

On remarque qu'en activant IACL on arrive pas a ce connecter a partir du PC 4 et PC manel puisqu' ils appartiennent pas au vlan du G2 par contre en la désactivant l'accès est autorisé

Router3

```

Physical Config CLI Attributes
IOS Command Line Interface

O 192.168.12.0 [110/65] via 192.168.23.1, 00:06:45, Serial2/0
O 192.168.20.0/24 [110/65] via 192.168.23.1, 00:06:45, Serial2/0
  192.168.23.0/30 is subnetted, 1 subnets
C   192.168.23.0 is directly connected, Serial2/0
C   192.168.30.0/24 is directly connected, FastEthernet0/0
O 192.168.50.0/24 [110/65] via 192.168.23.1, 00:06:45, Serial2/0
O 192.168.70.0/24 [110/65] via 192.168.23.1, 00:06:45, Serial2/0

Router(config-if)#ip access-list extended G2R3
Router(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 host 192.168.23.2
Router(config-ext-nacl)#deny ip any host 192.168.23.2
Router(config-ext-nacl)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip access-group G2R3 in
Router(config-if)#
19:04:49: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from FL
expired

19:04:49: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from FL
down or detached
no ip access-group G2R3 in
Router(config-if)#
19:05:39: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from LC
ip access-group G2R3 in
Router(config-if)#ip access-group G2R3 in
19:07:09: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from FL
expired

19:07:09: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from FL
down or detached
no ip access-group G2R3 in
Router(config-if)#
19:08:09: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from LC

Ctrl+F6 to exit CLI focus

```

Router3

```

Physical Config CLI Attributes
IOS Command Line Interface

O 192.168.12.0 [110/65] via 192.168.23.1, 00:06:45, Serial2/0
O 192.168.20.0/24 [110/65] via 192.168.23.1, 00:06:45, Serial2/0
  192.168.23.0/30 is subnetted, 1 subnets
C   192.168.23.0 is directly connected, Serial2/0
C   192.168.30.0/24 is directly connected, FastEthernet0/0
O 192.168.50.0/24 [110/65] via 192.168.23.1, 00:06:45, Serial2/0
O 192.168.70.0/24 [110/65] via 192.168.23.1, 00:06:45, Serial2/0

Router(config-if)#ip access-list extended G2R3
Router(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 host 192.168.23.2
Router(config-ext-nacl)#deny ip any host 192.168.23.2
Router(config-ext-nacl)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip access-group G2R3 in
Router(config-if)#
19:04:49: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from FL
expired

19:04:49: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from FL
down or detached
no ip access-group G2R3 in
Router(config-if)#
19:05:39: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from LC
ip access-group G2R3 in
Router(config-if)#ip access-group G2R3 in
19:07:09: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from FL
expired

19:07:09: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from FL
down or detached
no ip access-group G2R3 in
Router(config-if)#
19:08:09: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from LC

Ctrl+F6 to exit CLI focus

```

Router3

```

Physical Config CLI Attributes
IOS Command Line Interface

O 192.168.12.0 [110/65] via 192.168.23.1, 00:06:45, Serial2/0
O 192.168.20.0/24 [110/65] via 192.168.23.1, 00:06:45, Serial2/0
  192.168.23.0/30 is subnetted, 1 subnets
C   192.168.23.0 is directly connected, Serial2/0
C   192.168.30.0/24 is directly connected, FastEthernet0/0
O 192.168.50.0/24 [110/65] via 192.168.23.1, 00:06:45, Serial2/0
O 192.168.70.0/24 [110/65] via 192.168.23.1, 00:06:45, Serial2/0

Router(config-if)#ip access-list extended G2R3
Router(config-ext-nacl)# permit ip 192.168.50.0 0.0.0.255 host 192.168.23.2
Router(config-ext-nacl)#deny ip any host 192.168.23.2
Router(config-ext-nacl)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip access-group G2R3 in
Router(config-if)#
19:04:49: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from FL
expired

19:04:49: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from FL
down or detached
no ip access-group G2R3 in
Router(config-if)#
19:05:39: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from LC
ip access-group G2R3 in
Router(config-if)#ip access-group G2R3 in
19:07:09: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from FL
expired

19:07:09: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from FL
down or detached
no ip access-group G2R3 in
Router(config-if)#
19:08:09: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on Serial2/0 from LC

Ctrl+F6 to exit CLI focus

```

Règle 03 :

Seul le G1 de la M1SSI est autorisé à envoyer des paquets ICMP au réseau LAN-R3

On remarque qu'en activant IACL on arrive pas a pinger à partir du PC 1 puisqu' il appartient pas au vlan du G1 par contre en la désactivant l'accès est autorisé

Règle 04 :

La Déléguée Manel est la seule à pouvoir administrer le serveur DHCP

On voit très bien que lorsque l'ACL est activée tous les PC arrive à pinger le serveur DHCP par contre en l'activant que le PC manel qui arrive à le faire.

Règle 05 :

La section M1SSI ne peut joindre le serveur DHCP que pour récupérer sa configuration réseau (@IP + Masque + Passerelle par Défaut + Serveur DNS)

```

DHCP
Physical Config CLI Attributes
IOS Command Line Interface

Router(config-if)#int f1/0
20:39:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.70.11 on FastEthernet1/0 from LOADIN
Router(config-if)#ip ac
Router(config-if)#ip access-l
Router(config-if)#ip access-li
Router(config-if)#exit
Router(config)#ip access-list extended onlyconfdhcp
^
% Invalid input detected at '^' marker.

Router(config)#int f1/0
Router(config-if)#ip access-list extended onlyconfdhcp
^
% Invalid input detected at '^' marker.

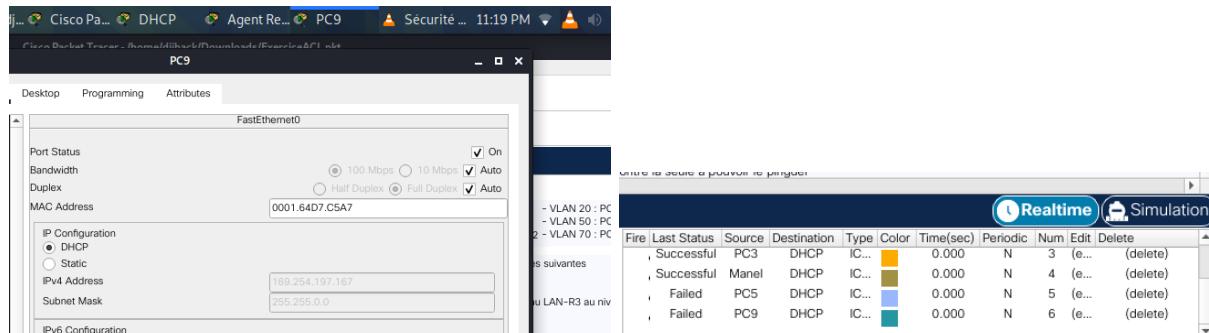
Router(config-if)#int
^
% Invalid input detected at '^' marker.

Router(config-if)#ip access-list extended onlyconfdhcp
^
% Invalid input detected at '^' marker.

Router(config-if)#ip access-list extended onlyconfdhcp
Router(config-ext-nacl)#permit udp 192.168.20.0 0.0.0.255 host 192.168.12.1 eq bootpc boc
^
% Invalid input detected at '^' marker.

Router(config-ext-nacl)#permit udp 192.168.20.0 0.0.0.255 host 192.168.12.1 eq bootpc
Router(config-ext-nacl)#permit udp 192.168.20.0 0.0.0.255 host 192.168.12.1 eq bootps
Router(config-ext-nacl)#permit udp 192.168.50.0 0.0.0.255 host 192.168.12.1 eq bootps
Router(config-ext-nacl)#permit udp 192.168.50.0 0.0.0.255 host 192.168.12.1 eq bootpc
Router(config-ext-nacl)#permit udp 192.168.70.0 0.0.0.255 host 192.168.12.1 eq bootpc
Router(config-ext-nacl)#permit udp 192.168.70.0 0.0.0.255 host 192.168.12.1 eq bootps
Router(config-ext-nacl)#

```



On voit que l'attribution du dhcp fonctionne et le ping ne fonctionne pas pour les PCs du G1 et G2 après avoir activé l'ACL bien sur

Règle 06 :

Le LAN-R3 est autorisé à envoyer uniquement un trafic en mode fiable && connecté au G1-SSI, ainsi qu'un trafic en mode non fiable et non connecté au G2-SSI

```
Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended LANR3M1SSI
Router(config-ext-nacl)# permit tcp 192.168.20.0 0.0.0.255 192.168.23.2
% Incomplete command.
Router(config-ext-nacl)# permit tcp 192.168.20.0 0.0.0.255 192.168.23.2
% Incomplete command.
Router(config-ext-nacl)#permit tcp 192.168.20.0 0.0.0.255 192.168.23.2
% Incomplete command.
Router(config-ext-nacl)#permit tcp 192.168.20.0 0.0.0.255 host 192.168.23.2
Router(config-ext-nacl)#permit udp 192.168.50.0 0.0.0.255 host 192.168.23.2
Router(config-ext-nacl)#no permit udp 192.168.50.0 0.0.0.255 host 192.168.23.2
Router(config-ext-nacl)#no permit udp 192.168.20.0 0.0.0.255 host 192.168.23.2
Router(config-ext-nacl)# permit tcp host 192.168.23.2 0.0.0.3 192.168.20.0
Router(config-ext-nacl)# permit udp host 192.168.23.2 0.0.0.3 192.168.50.0
Router(config-ext-nacl)#exit
Router(config)#int s2/0
Router(config-if)#ip acc
Router(config-if)#ip access-list extended LANR3M1SSI
Router(config-ext-nacl)#deny ip any any
Router(config-ext-nacl)#exit
Router(config)#int s2/0
Router(config-if)#access-group LANR3M1SSI out
^
% Invalid input detected at '^' marker.

Router(config-if)#ip acess-group LANR3M1SSI out
^
% Invalid input detected at '^' marker.

Router(config-if)#ip acc
Router(config-if)#ip access-group LANR3M1SSI out
Router(config-if)#

```

Realtime											Simulation
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete	
	Failed	Manel	PC7	IC...	Green	0.000	N	0	(e...)	(delete)	
	Failed	PC2	PC7	IC...	Red	0.000	N	1	(e...)	(delete)	
	Failed	PC1	PC7	IC...	Blue	0.000	N	2	(e...)	(delete)	
	Successful	PC2	PC7	IC...	Purple	0.000	N	3	(e...)	(delete)	
	Successful	PC1	PC7	IC...	Cyan	0.000	N	4	(e...)	(delete)	

Règle 07 :

La section M1SSI est uniquement autorisé à consulter le site web hébergé au niveau du serveur SSI, Manel est par contre la seule à pouvoir le pinguer

```
Router>en
Password:
Password:
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended serveurSSI
Router(config-ext-nacl)# permit tcp 192.168.20.0 0.0.0.255 192.168.70.2 eq 80
^
% Invalid input detected at '^' marker.

Router(config-ext-nacl)#permit tcp 192.168.20.0 0.0.0.255 192.168.70.2 eq 80
^
% Invalid input detected at '^' marker.

Router(config-ext-nacl)#permit tcp 192.168.20.0 0.0.0.255 192.168.70.2 eq 80
^
% Invalid input detected at '^' marker.

Router(config-ext-nacl)#permit tcp host 192.168.20.0 0.0.0.255 192.168.70.2 eq 80
Router(config-ext-nacl)#permit tcp host 192.168.50.0 0.0.0.255 192.168.70.2 eq 80
Router(config-ext-nacl)#permit icmp host 192.168.70.7 0.0.0.255 192.168.70.2
Router(config-ext-nacl)#deny ip any any
```