- TP 6 -
Listes de contrôle d'accès (ACL)

par Édouard Lumet & [redacted]

Sommaire

Introduction

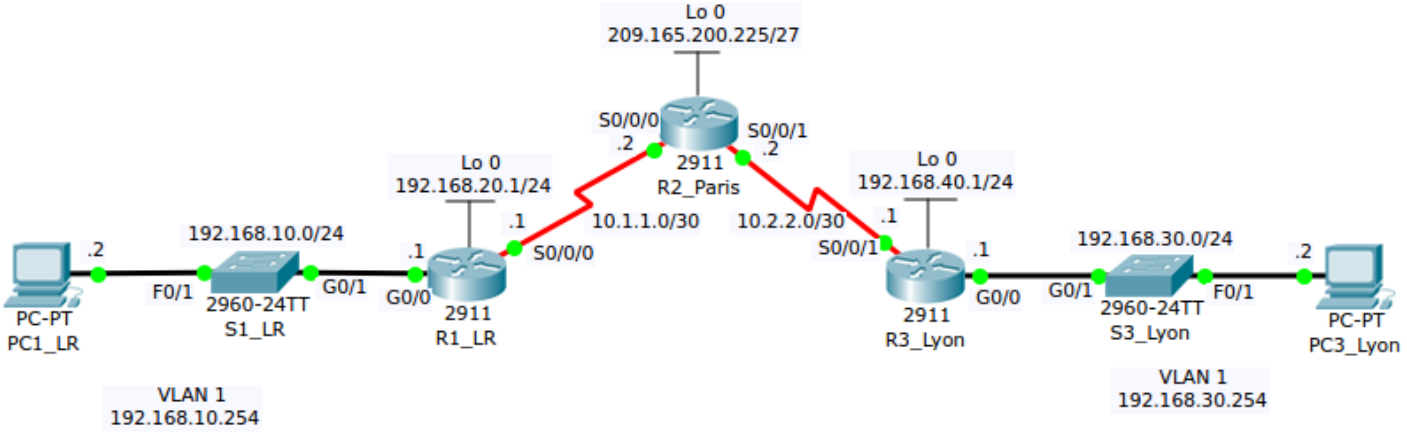
Les listes de contrôle d'accès, ou ACL, sont un premier élément de base de la sécurité des réseaux. Très simples, elles sont cependant une première barrière filtrant les paquets IPv4 et IPv6au niveau des routeurs. Nous allons donc à travers ce TP, apprendre à sur routeur Cisco :

- à configurer des ACL standards et étendues en IPv4,
- à configurer des ACL en IPv6,
- à positionner judicieusement et efficacement les ACL au cœur d'une topologie.

Il existe en effet, en IPv4, deux types d'ACL. Les ACL standards ne sont basées que sur une adresse (ou groupe d'adresses) source, elles doivent être donc positionnées au plus près de la destination pour ne pas bloquer le trafic plus qu'il ne faut. Les ACL étendues quant à elle sont basées sur le protocole (ip, icmp, tcp ou udp), sur l'adresse source, sur l'adresse destination et sur les ports sources et destination. Ces dernières sont placées au plus près de la source pour ne pas encombrer le réseau inutilement.

1. Configuration d'ACL standards

1.1. Topologie pour cet exercice



ELRG_TP6_Exo1_ACL_standard.pkt

Périphérique	Interface	Adresse IPv4 / longueur préfixe sous réseau
R1	gi0/0	192.168.10.1/24
	s0/0/0	10.1.1.1/30
	lo0	192.168.20.1/24
R2	s0/0/0	10.1.1.2/30
	S0/0/1	10.2.2.2/30
	lo0	209.165.200.225/27
R3	gi0/0	192.168.30.1/24
	s0/0/1	10.2.2.1/30
	lo0	192.168.40.1/24
S1_LR	VLAN1	192.168.10.254/24
S2_Lyon	VLAN	192.168.30.254/24
PC1_LR	NIC	192.168.10.2/24
PC3_Lyon	NIC	192.168.30.2/24

1.2. Configuration du protocole de routage OSPF

La configuration d'OSPF dans cette topologie est relativement simple du fait qu'il n'y ait qu'une zone. Toutes les commandes nécessaires à cette configuration figurent dans la fiche d'intervention jointe, commentées bien sûr.

Pour la suite de ce compte-rendu, seule l'interprétation, les conclusions à tirer et la partie théorique seront traitées, les commandes étant commentées dans la fiche d'intervention.

On vérifie ensuite les connectivités entre équipements à l'aide de quelques tests de ping :

```
PC>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.30.2: bytes=32 time=7ms TTL=125
Reply from 192.168.30.2: bytes=32 time=2ms TTL=125
Reply from 192.168.30.2: bytes=32 time=2ms TTL=125
Reply from 192.168.30.2: bytes=32 time=2ms TTL=125
```

Ping PC1 > PC3

```
PC>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.2: bytes=32 time=2ms TTL=125
Reply from 192.168.10.2: bytes=32 time=11ms TTL=125
Reply from 192.168.10.2: bytes=32 time=2ms TTL=125
```

Ping PC3 > PC1

```
R2#ping 10.2.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/15 ms

R2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8 ms
```

Pings R2 > R3 puis R2 > R1

Un test de ping concluant entre PC1 et PC3, au vu de notre topologie, nous indique une configuration à priori correcte. La connectivité entre routeurs est également correcte.

1.3. Configuration d'une ACL standard numérotée

Nous devons créer une ACL standard numérotée 1 dont les objectifs sont :

- autorisation du trafic de tous les hôtes des réseaux 192.168.10.0/24 et 192.168.20.0/24 vers 192.168.30.0/24,
- stratégie d'interdiction dans tous les autres cas.

- Cette ACL doit être placée, comme nous l'avons expliqué en introduction, au plus près de la destination. Ici, elle doit donc être placée sur R3 car c'est le routeur qui connecte le réseau 192.168.30.0/24.
- Plus précisément, c'est sur l'interface gi0/0 de R3 en sortie que nous devons la placer, soit depuis l'extérieur vers le réseau 192.168.30.0/24.
- On configure alors l'ACL sur R3 en la plaçant sur l'interface gi0/0 avec les commandes listées dans la fiche d'intervention.
- On vérifie son contenu à l'aide de la commande **#show access-lists 1** :

```
R3(config-if)#do show access-lists 1
Standard IP access list 1
    permit 192.168.10.0 0.0.0.255
    permit 192.168.20.0 0.0.0.255
    deny any
```

Contenu de l'ACL standard 1

- On vérifie ensuite que l'ACL est bien active sur l'interface gi0/0 :

```
R3(config-if)#do show ip interface gi0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.30.1/24
  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 1
  Inbound  access list is not set
  Proxy ARP is enabled
```

*Infos IP de l'interface gi0/0 sur R3 – **show ip interface gi0/0***

On voit que l'ACL1 est bien active en sortie de l'interface gi0/0 de R3 et qu'il n'y a pas d'ACL en entrée.

Rmq : on ne peut alors configurer que deux ACL par interface : l'une en entrée et l'autre en sortie.

```
PC>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.30.2: bytes=32 time=7ms TTL=125
Reply from 192.168.30.2: bytes=32 time=2ms TTL=125
Reply from 192.168.30.2: bytes=32 time=2ms TTL=125
Reply from 192.168.30.2: bytes=32 time=2ms TTL=125
```

Ping PC1 > PC3

- La connectivité entre PC1 et PC3 est possible puis que l'on a autorisé les hôtes du réseau 192.168.10.0/24 vers ceux du réseau 192.168.30.0/24.

- Ayant également autorisé le réseau 192.168.20.0/24, un ping de R1 (Lo0, 192.168.20.1) vers PC3 est possible :

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.30.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.20.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/12/34 ms
```

PC3 ← Target IP address: 192.168.30.2

@ int lo0 de R1 ← Source address or interface: 192.168.20.1

Ping étendu de l'interface Loopback0 de R1 vers PC3

- En revanche, lorsque l'on envoie un ping classique, il est envoyé depuis une autre interface comme s0/0/0 qui ne se trouve pas dans les réseaux autorisés :

```
R1#ping 192.168.30.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

Ping de R1 vers PC3

On voit alors le caractère '**U**' pour Unreachable, le routeur a reçu un PDU d'erreur de destination injoignable.

- L'ACL étant placée en sortie de l'interface gi0/0 de R3, il n'y a que les réseaux connectés à cette interface qui sont visés par la restriction. R1 peut donc toujours communiquer avec le réseau 192.168.40.0/24.

1.4. Configuration d'une ACL standard nommée

Ici, nous allons créer une ACL standard nommée '**EXO1-ACL-NOMMEE**' qui aura pour but :

- d'autoriser tous les hôtes du réseau 192.168.40.0/24 à accéder au réseau 192.168.10.0/24,
- d'autoriser le PC3 uniquement de son réseau à accéder au réseau 192.168.10.0/24.

- Nous devons placer cette ACL sur l'interface gi0/0 en sortie du routeur R1, à l'image de l'ACL que nous venons de créer sur le routeur R3.
- On configure alors cette ACL à l'aide des commandes qui, à priori, ne sont pas parties à la plage mais sont toujours bien dans la fiche d'intervention jointe…
- On vérifie le contenu de l'ACL et l'interface gi0/0 de R1 :

```
R1#show access-lists
Standard IP access list EXO1-ACL-NOMMEE
    10 permit 192.168.40.0 0.0.0.255
    20 permit host 192.168.30.2
    30 deny any
R1#show ip interface gi0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  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 EXO1-ACL-NOMMEE
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
```

Vérification de l'ACL et de son application

On voit que l'ACL est effectivement appliquée en sortie sur l'interface gi0/0 de R1.

- Les requêtes entre PC3 et PC1 aboutissent car nous avons autorisé spécialement l'hôte 192.168.30.2 (PC3) dans cette ACL (vers 192.168.10.0/24 donc).

- Ensuite, on teste les pings entre le réseau 192.168.40.0/24 que nous avons autorisé dans l'ACL et le réseau 192.168.10.0/24 (via un ping étendu sur R3). Cette communication est donc possible :

```
PC>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.2: bytes=32 time=2ms TTL=125
Reply from 192.168.10.2: bytes=32 time=11ms TTL=125
Reply from 192.168.10.2: bytes=32 time=2ms TTL=125
```

Ping PC3 > PC1 : OK

```
R3#ping
Protocol [ip]:
Target IP address: 192.168.10.2
Source address or interface: 192.168.40.1
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.40.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/9 ms
```

L'affichage a été tronqué, cela reste un ping étendu

- Cependant, les pings depuis R2 et R3 n'aboutissent pas car leurs adresses sources sont respectivement 10.1.1.2 et 10.2.2.1 pour les pings vers PC1, les réseaux 10.1.1.0/24 et 10.2.2.0/24 ne sont pas autorisés par l'ACL nommée donc interdits par défaut :

```
R2#ping 192.168.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

Ping R2 > PC1 : NOK (unreachable)

```
R3#ping 192.168.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```

Ping R3 > PC1 : NOK (unreachable)

- Pour les mêmes raisons que R1 peut communiquer avec le réseau 192.168.40.0/24 malgré la présence de l'ACL standard 1, R2 et R3 peuvent toujours communiquer avec le réseau 192.168.20.0/24 (lo0) puisque l'ACL est située juste après cette liaison.

2. Contrôle de l'accès VTY à l'aide d'une ACL

2.1. Configuration de l'accès VTY à R1

On conserve la même topologie que lors de la partie 1.

- On configure sur R1 un mot de passe chiffré pour le mode d'exécution privilégié : « larochelle ». Puis on configure le mot de passe « rtrt » pour les lignes VTY dont on active la connexion.
- L'accès Telnet est possible depuis PC1 et PC3 vers R1 mais uniquement vers l'interface gi0/0 (192.168.10.1). En effet, les deux ACL que nous avons précédemment configurées n'autorisent pas la réponse de l'interface s0/0/0 de R1 vers PC1 et PC3.

```
PC>telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection timed out; remote host not responding
PC>telnet 192.168.10.1
Trying 192.168.10.1 ...Open


User Access Verification

Password:
R1>en
Password:
R1#
```

Telnet de PC1 et PC3 vers R1 ***(s0/0/0 : NOK ; puis gi0/0 : OK)***

2.2. Création de l'ACL appliquée aux accès VTY

- On crée une ACL standard nommée '**ADMIN_MNGT**' sur R1 afin de n'autoriser que le PC1 (192.168.10.2) à accéder à R1 via Telnet.
- On applique donc cette ACL sur les lignes VTY 0 à 15 en entrée.

NB : pour rappel, les commandes sont listées et commentées dans la fiche d'intervention

- On affiche, par soucis de vérification, le contenu de l'ACL que nous venons de créer :

```
R1#show access-lists
Standard IP access list EXO1-ACL-NOMMEE
    10 permit 192.168.40.0 0.0.0.255 (5 match(es))
    20 permit host 192.168.30.2 (4 match(es))
    30 deny any (10 match(es))
Standard IP access list ADMIN_MNGT
    10 permit host 192.168.10.2
    20 deny any
```

2.3. Test de l'ACL sur les accès VTY

- On teste l'accès à R1 via Telnet comme dans la partie 2.1 :

```
PC>telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection timed out; remote host not responding
PC>telnet 192.168.10.1
Trying 192.168.10.1 ...
% Connection refused by remote host
```

Telnet PC3 > R1 (s0/0/0 puis gi0/0)

On observe toujours un « timeout » vers s0/0/0 puisque PC3 peut envoyer sa requête vers 10.1.1.1 mais il ne peut pas recevoir la réponse. En revanche, c'est bien un refus que l'on a lorsque l'on tente l'accès vers 192.168.10.1 puisque seul PC1 est autorisé.

- Afin de vérifier que seul PC1 et donc son adresse est autorisé à se connecter via Telnet à R1, on modifie son adresse en 192.168.10.3 et on tente de nouveau une connexion :

```
PC>telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection timed out; remote host not responding
PC>telnet 192.168.10.1
Trying 192.168.10.1 ...
% Connection refused by remote host
```

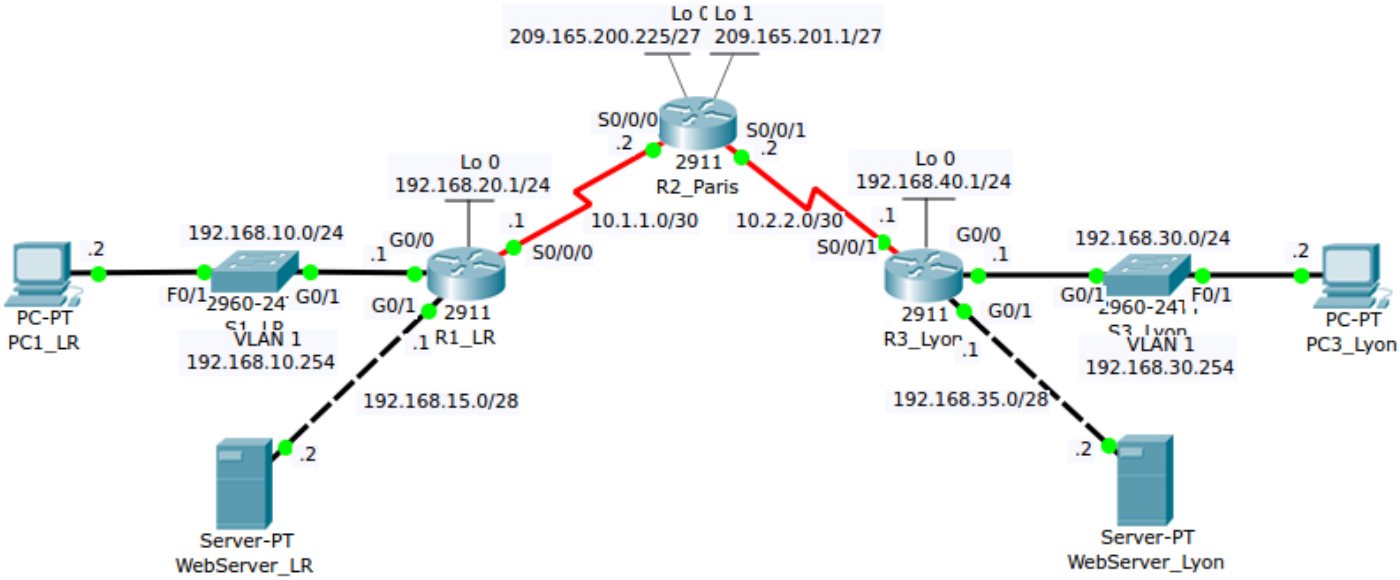
Telnet PC1 (tempo 192.168.10.3) > R1 (192.168.10.1)

la connexion est bien refusée par R1…

Pour conclure sur les ACL standards, on peut noter qu'elles ont principalement l'inconvénient de bloquer tout le trafic à partir de l'endroit où elles sont positionnées (pour une adresse ou un groupe d'adresses source donné bien sûr). Il faut donc qu'elles soient positionnées au plus près de la destination, les messages étant filtrés par une ACL standard auront donc parcouru une grande partie du réseau pour finalement être supprimés. On perd donc en débit (ou bande passante numérique) utile sur notre réseau.

3. Configuration d'ACL étendues

3.1. Topologie pour cet exercice



ELRG_TP6_Exo3_ACL_etendue.pkt

Périphérique	Interface	Adresse IPv4 / longueur préfixe sous réseau
R1	gi0/0	192.168.10.1/24
	gi0/1	192.168.15.1/24
	s0/0/0	10.1.1.1/30
	lo0	192.168.20.1/24
R2	s0/0/0	10.1.1.2/30
	S0/0/1	10.2.2.2/30
	lo0	209.165.200.225/27
	lo1	209.165.201.1/27
R3	gi0/0	192.168.30.1/24
	gi0/1	192.168.35.1/24
	s0/0/1	10.2.2.1/30
	lo0	192.168.40.1/24
S1_LR	VLAN1	192.168.10.254/24
S2_Lyon	VLAN1	192.168.30.254/24
PC1_LR	NIC	192.168.10.2/24
WebServer_LR	NIC	192.168.15.2/24
PC3_Lyon	NIC	192.168.30.2/24
WebServer_Lyon	NIC	192.168.35.2/24

3.2. Configurations complémentaires préalables

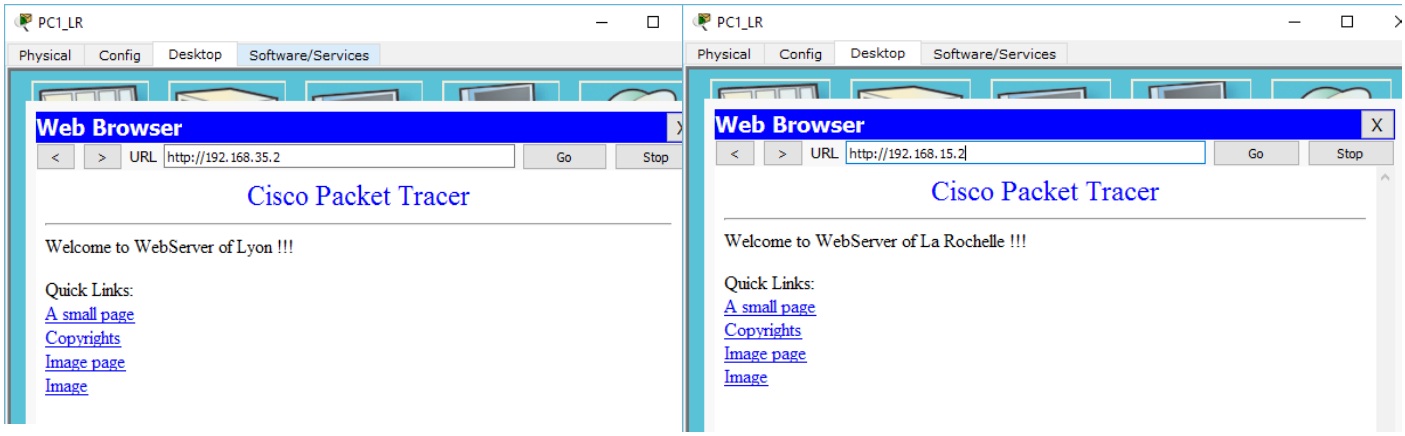
Toutes les configurations préalables sont également listées et commentées dans la fiche d'intervention.

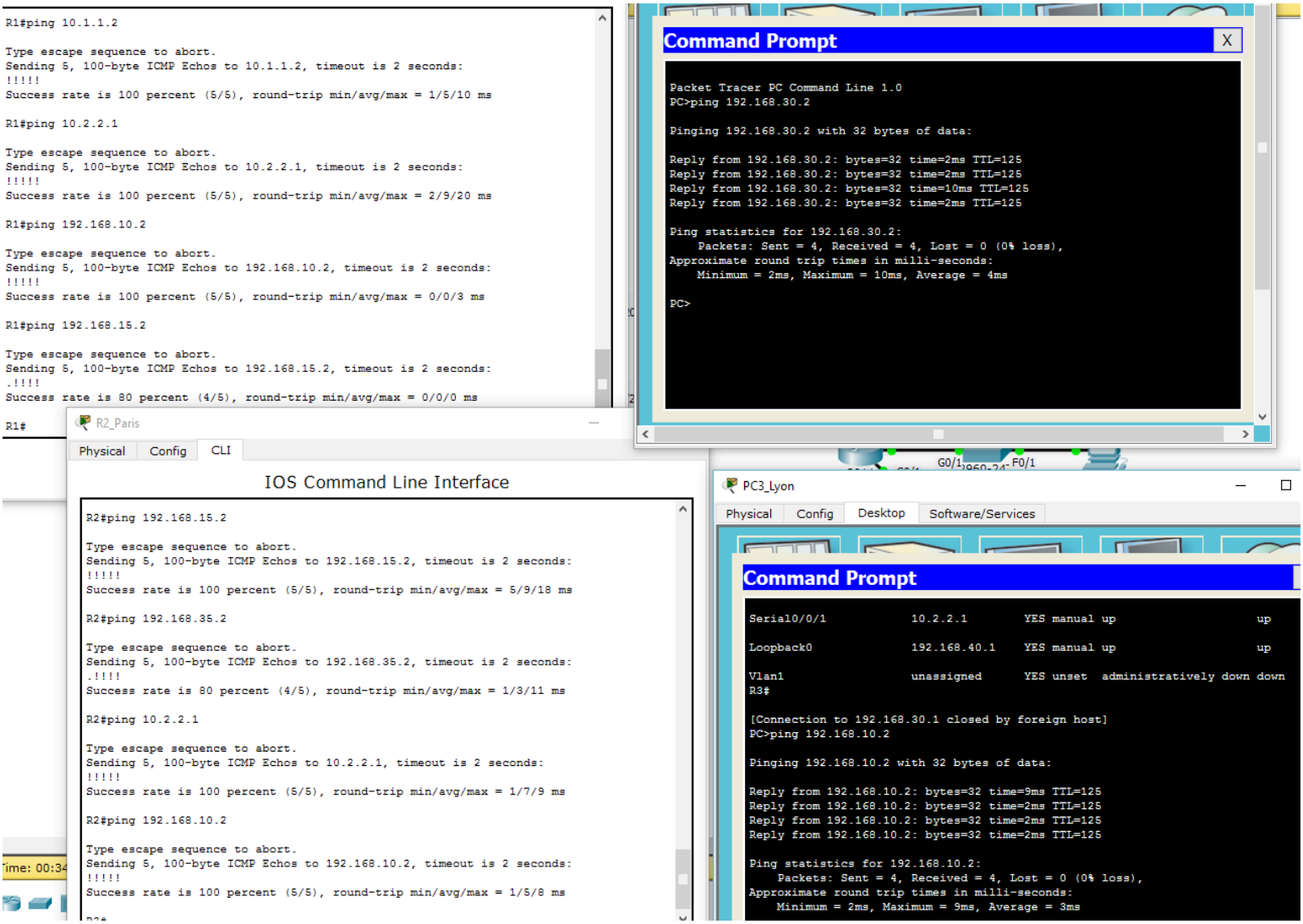
- Sur R1 et R2, on configure le mot de passe chiffré « larochelle » pour le mode d'exécution privilégié puis on attribue le mot de passe « rtrt » aux accès VTY que l'on active.
- Sur R3, on configure aussi le mot de passe chiffré « larochelle » pour le mode d'exécution privilégié puis on active SSH pour les accès VTY en créant un profil utilisateur local.
- On vérifie la configuration en tentant une connexion SSH depuis PC3 vers R3 :

```
PC>ssh -l admin 192.168.30.1
Open
Password:



R3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     192.168.30.1    YES manual up                    up

GigabitEthernet0/1     192.168.35.1    YES manual up                    up

GigabitEthernet0/2     unassigned      YES unset  administratively down down

Serial0/0/0            unassigned      YES unset  administratively down down

Serial0/0/1            10.2.2.1        YES manual up                    up

Loopback0              192.168.40.1    YES manual up                    up

Vlan1                  unassigned      YES unset  administratively down down
R3#
```

ssh -l admin 192.168.30.1 | connexion SSH depuis PC3 vers R3 : OK

- Ensuite, on configure sur les trois routeurs le protocole OSPF qui là aussi reste assez simple car, malgré le nombre de réseaux plus important que dans la topologie de la partie 1, il n'y a toujours qu'une zone (0).
- On vérifie alors les connectivités entre équipements et la connectivité web :





On peut voir que l'on peut afficher avec succès le contenu web des deux serveurs Web de la topologie depuis un PC et que toutes les machines peuvent pinguer entre elles, ce qui signifie que la configuration réseau est correcte.

3.3. Configuration d'une ACL étendue numérotée

Nous allons maintenant créer notre première ACL étendue numérotée 100. Ses objectifs sont les suivants :

- autoriser le trafic web pour le réseau 192.168.10.0/24,
- autoriser le PC1 (192.168.10.2) à se connecter en SSH à l'interface s0/0/1 de R3,
- interdire tout autre type de trafic pour le réseau 192.168.10.0/24.

- Nous devons placer cette ACL sur l'interface gi0/0 en entrée du routeur R1, soit au plus près de la source.
- On configure l'ACL sur le routeur R1, les commandes étant dans la fiche d'intervention.

- On vérifie ensuite le contenu de l'ACL comme dans les parties précédentes :

```
R1#show ip access-lists 100
Extended IP access list 100
    permit tcp 192.168.10.0 0.0.0.255 any eq www (5 match(es))
    permit tcp 192.168.10.0 0.0.0.255 any eq 443
    permit tcp host 192.168.10.2 host 10.2.2.1 eq 22 (29 match(es))
    deny ip any any (15 match(es))
```

Vérification de l'ACL étendue 100

```
R1#show ip int gi0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  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 not set
  Inbound  access list is 100
  Proxy ARP is enabled
```

Infos IP de l'interface gi0/0

On peut voir que l'ACL est correcte et qu'elle est bien appliquée sur R1 en entrée de l'interface gi0/0.

- On effectue quelques tests pour vérifier que l'ACL effectue ce que l'on voulait :

Accès depuis PC1 au serveur web La Rochelle

Accès depuis PC1 au serveur web Lyon

```
PC>ping 192.168.15.2

Pinging 192.168.15.2 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.15.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.35.2

Pinging 192.168.35.2 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.35.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Pings depuis le PC1 vers les deux serveurs web

Le PC1 peut se connecter aux deux serveurs web via le navigateur mais il ne peut pas les pinguer. En effet, l'ACL autorise seulement le trafic TCP/80 et TCP/443 (web et web sécurisé) depuis le réseau 192.168.10.0/24. Le protocole ICMP (ping) ne peut donc pas passer le routeur R1.

- Pour la même raison, PC1 ne peut pas se connecter en Telnet à R1, PC3 lui le peut :
  voir page suivante

```
PC>telnet 192.168.10.1
Trying 192.168.10.1 ...Open


User Access Verification

Password:
R1>
```

Connexion Telnet PC3 > R1 (gi0/0)

```
PC>telnet 192.168.10.1
Trying 192.168.10.1 ...
% Connection timed out; remote host not responding
```

Connexion Telnet PC1 > R1 (gi0/0)

La connexion est bien refusée pour PC1, et non pour PC3.

- Comme nous l'avons vu précédemment, notre ACL compte 4 ACE.
- On la modifie pour y ajouter deux lignes, impérativement avant la dernière (*voir fiche d'intervention*). Elle doit maintenant permettre à PC1 de se connecter en Telnet aux interfaces gi0/0 et lo0 uniquement de R1.
- Le contenu de l'ACL est désormais le suivant :

```
R1(config-ext-nacl)#do show access-lists
Extended IP access list 100
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www (15 match(es))
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
    30 permit tcp host 192.168.10.2 host 10.2.2.1 eq 22 (29 match(es))
    35 permit tcp host 192.168.10.2 host 192.168.10.1 eq telnet
    36 permit tcp host 192.168.10.2 host 192.168.20.1 eq telnet
    40 deny ip any any (35 match(es))
```

Contenu de l'ACL étendue 100

On que les deux lignes ont bien été insérées avec les numéros indiquées juste avant la dernière. Après un redémarrage du routeur, on peut voir que IOS renumérote les ACE pour reprendre une numérotation de 10 en 10 et permettre l'insertion de nouvelles lignes :

```
R1#show access-lists
Extended IP access list 100
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
    30 permit tcp host 192.168.10.2 host 10.2.2.1 eq 22
    40 permit tcp host 192.168.10.2 host 192.168.10.1 eq telnet
    50 permit tcp host 192.168.10.2 host 192.168.20.1 eq telnet
    60 deny ip any any
```

ACL étendue 100 après redémarrage

- La connexion Telnet entre PC1 et R1 est désormais effectivement possible :

```
PC>telnet 192.168.10.1
Trying 192.168.10.1 ...Open


User Access Verification

Password:
R1>exit

[Connection to 192.168.10.1 closed by foreign host]
PC>telnet 192.168.20.1
Trying 192.168.20.1 ...Open


User Access Verification

Password:
R1>exit
```

Connexion Telnet PC1 > R1 (gi0/0 puis lo0)

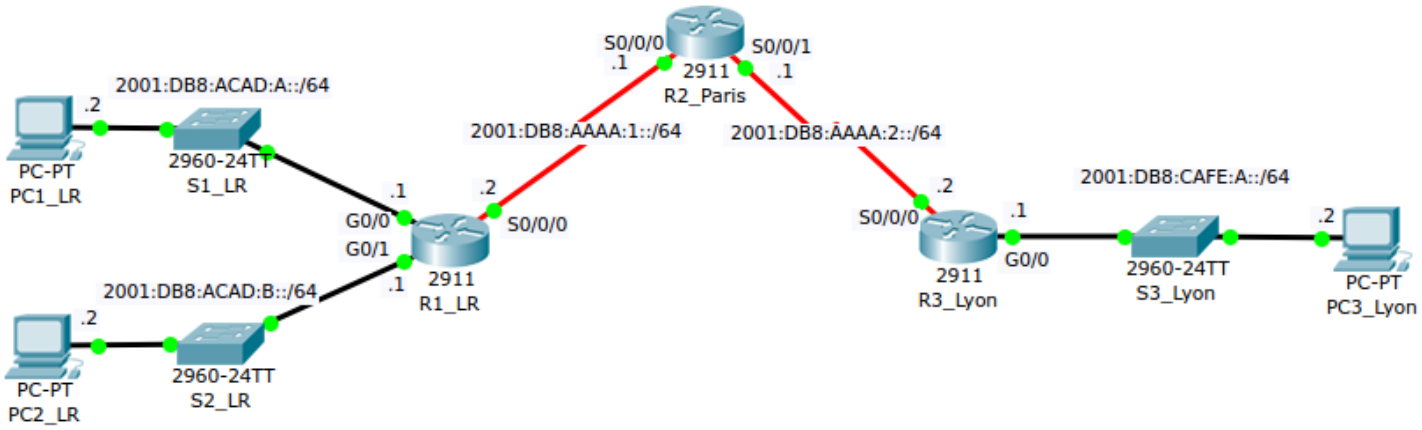
```
PC>telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection timed out; remote host not responding
```

Connexion Telnet PC1 > R1 (s0/0/0)

…sauf via l'interface s0/0/0 (comme voulu) !

4. Configuration d'ACL IPv6

4.1. Topologie IPv6 pour l'exercice



ELRG_TP6_Exo4_ACL_IPv6.pkt

Périphérique	Interface	Adresse IPv6 / préfixe	Adresse IPv6 link-local
R1	gi0/0	2001:DB8:ACAD:A::1/64	FE80::1
	gi0/1	2001:DB8:ACAD:B::1/64	FE80::1
	s0/0/0	2001:DB8:AAAA:1::2/64	FE80::1
R2	s0/0/0	2001:DB8:AAAA:1::1/64	FE80::2
	S0/0/1	2001:DB8:AAAA:2::1/64	FE80::2
R3	gi0/0	2001:DB8:CAFE:A::1/64	FE80::3
	s0/0/0	2001:DB8:AAAA:2::2/64	FE80::3
PC1_LR	NIC	2001:DB8:ACAD:A::2/64	FE80::202:4AFF:FE2D:EE01
PC2_LR	NIC	2001:DB8:ACAD:B::2/64	FE80::201:C7FF:FE5D:16AD
PC3_Lyon	NIC	2001:DB8:CAFE:A::2/64	FE80::2D0:D3FF:FEAB:B295

4.2. Configurations complémentaires préalables

Comme pour les parties précédentes, toutes les commandes nécessaires à ces configurations préalables sont dans la fiche d'intervention jointe.

- On commence par configurer une route statique par défaut directement connectée sur R1 et sur R3 (via leur interface série s0/0/0), puis on configure deux routes statiques sur R2 vers les LANs de R1 et le LAN de R3. Le première devra donc être une route récapitulative.
- Sur les trois routeurs, on configure ensuite un mot de passe pour le mode d'exécution privilégié et on active et on configure SSH pour les accès VTY. On finira bien sûr par activer le routage des paquets IPv6.

- On teste les connexions SSH depuis un PC :

```
PC>ssh -l admin 2001:db8:aaaa:1::2
Open
Password:



R1_LR#
```

Connexion SSH PC2 > R1 (s0/0/0)

Ceci est un exemple de connexion SSH. Toutes les connectivités sont correctes dans notre topologie.

4.3. Contrôle d'accès VTY à l'aide d'une ACL IPv6

- On crée une ACL IPv6 nommée 'RESTRICT-VTY' afin de contrôler l'accès via les lignes virtuelles VTY. Les objectifs sont d'autoriser uniquement les hôtes du réseau 2001:DB8:ACAD:A::/64 à se connecter en SSH à R1 sauf l'hôte 2001:DB8:ACAD:A::666. Tout le reste est interdit sur ces lignes. A noter qu'il faut d'abord interdire l'hôte avant d'autoriser le réseau entier.
- On affiche alors le contenu de l'ACL :

```
R1_LR(config-ipv6-acl)#do show ipv6 access-list RESTRICT-VTY
IPv6 access list RESTRICT-VTY
    deny tcp host 2001:DB8:ACAD:A::666 any eq 22
    permit tcp 2001:DB8:ACAD:A::/64 any eq 22
    deny ipv6 any any
```

ACL IPv6 'RESTRICT-VTY'

- On finit par tester cette ACL :

```
PC>ssh -l admin 2001:db8:acad:a::1
Open
Password:



R1_LR#
```

Connexion SSH PC1 > R1

```
PC>ssh -l admin 2001:db8:aaaa:1::2

% Connection refused by remote host
PC>
```

Connexion SSH PC3 > R1

PC1 peut effectivement toujours se connecter via SSH à R1 mais pas R3.

- On modifie l'adresse de PC1 pour 2001:DB8:ACAD:A::666 afin de vérifier que l'hôte est bien interdit sur les lignes VTY de R1 même via SSH :

```
PC>ssh -l admin 2001:db8:acad:a::1
Open
Password:



R1_LR#
% Connection timed out; remote host not responding
PC>ssh -l admin 2001:db8:acad:a::1

% Connection refused by remote host
```

Connexion SSH PC1 > R1 avec changement d'adresse

On peut voir que, dès l'instant où l'on change d'adresse, la connexion SSH est réinitialisée et on ne peut plus se reconnecter à R1.

4.4. Contrôle de trafic par ACL IPv6

- On teste la connectivité entre PC3 et les deux réseaux WAN interconnectant R1 et R3 à R2 :

```
PC>ping 2001:db8:aaaa:2::1

Pinging 2001:db8:aaaa:2::1 with 32 bytes of data:

Reply from 2001:DB8:AAAA:2::1: bytes=32 time=5ms TTL=254
Reply from 2001:DB8:AAAA:2::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:AAAA:2::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:AAAA:2::1: bytes=32 time=1ms TTL=254

Ping statistics for 2001:DB8:AAAA:2::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

PC>ping 2001:db8:aaaa:1::1

Pinging 2001:db8:aaaa:1::1 with 32 bytes of data:

Reply from 2001:DB8:AAAA:1::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:AAAA:1::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:AAAA:1::1: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:AAAA:1::1: bytes=32 time=1ms TTL=254
```

Pings PC3 > réseaux WAN

La connectivité est correcte, les tests de ping sont concluants.

- On configure sur R3 une ACL IPv6 nommée 'RESTRICT-TRAFFIC' qui a pour but d'interdire tout trafic depuis le réseau 2001:DB8:CAFE:A::/64 vers les deux réseaux WAN 2001:DB8:AAAA:1::/64 et 2001:DB8:AAAA:2::/64 puisqu'il n'y a pas d'équipements terminaux connectés sur ces réseaux. *Rappel : voir fiche d'intervention*
- On vérifie l'ACL puis on refait les tests de ping :

```
R3_Lyon(config-ipv6-acl)#do show ipv6 access-list RESTRICT-TRAFFIC
IPv6 access list RESTRICT-TRAFFIC
    deny ipv6 2001:DB8:CAFE:A::/64 2001:DB8:AAAA:1::/64
    deny ipv6 2001:DB8:CAFE:A::/64 2001:DB8:AAAA:2::/64
    permit ipv6 any any
```

ACL IPv6 'RESTRICT-TRAFFIC' sur R3

```
PC>ping 2001:db8:aaaa:1::1

Pinging 2001:db8:aaaa:1::1 with 32 bytes of data:

Reply from 2001:DB8:CAFE:A::1: Destination host unreachable.
Reply from 2001:DB8:CAFE:A::1: Destination host unreachable.
Reply from 2001:DB8:CAFE:A::1: Destination host unreachable.
Reply from 2001:DB8:CAFE:A::1: Destination host unreachable.

Ping statistics for 2001:DB8:AAAA:1::1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 2001:db8:aaaa:2::1

Pinging 2001:db8:aaaa:2::1 with 32 bytes of data:

Reply from 2001:DB8:CAFE:A::1: Destination host unreachable.
Reply from 2001:DB8:CAFE:A::1: Destination host unreachable.
Reply from 2001:DB8:CAFE:A::1: Destination host unreachable.
Reply from 2001:DB8:CAFE:A::1: Destination host unreachable.
```

Comme le démontrent ces tests de ping, les réseaux WAN ne sont plus accessibles depuis le PC3 qui n'est autre qu'un témoin pour le réseau 2001:DB8:CAFE:A::/64 dans nos tests. L'erreur ICMP « Destination host unreachable » indique que le paquet a été refusé par le routeur et que l'ACL est efficace.

Conclusion

Nous avons donc pu constater dans ce TP les différences entre ACL standards et étendues pour IPv4, et quels sont les enjeux des ACL dans un réseau.

Ce premier élément de la sécurité est efficace car, dans le cas des ACL étendues en IPv4 ou des ACL IPv6, on peut cibler des communications précises à autoriser ou à interdire. Cependant, la configuration est assez lourde et de façon proportionnelle à la taille du réseau. Il faut de plus faire attention à l'ordre des ACE mais aussi au positionnement des ACL, les probabilités d'erreur sont donc assez élevées. Le meilleur moyen de parer cet inconvénient est d'être attentif et de réfléchir par brouillon avant d'effectuer les configurations.

Pour finir, il peut être aisé de détourner ces sécurités en changeant tout simplement son adresse IP… il faut néanmoins avoir suffisamment de chance pour trouver quels réseaux sont discriminés ou non, via quels protocoles, etc.