LES ACL

Une ACL est une liste d'Access Control Entry (ACE) ou entrée de contrôle d'accès donnant ou supprimant des droits d'accès à une personne ou un groupe.

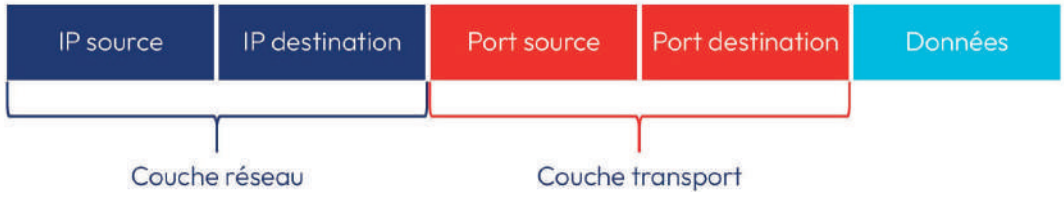
Une ACL désigne traditionnellement deux choses en sécurité informatique :

- un système permettant de faire une gestion plus fine des droits d'accès aux fichiers que ne le permet la méthode employée par les systèmes UNIX.
- Et en réseau, une liste des adresses et ports autorisés ou interdits par un pare-feu.

9.1. Notions de base sur les listes de contrôle d'accès :

9.1.1. Définition :

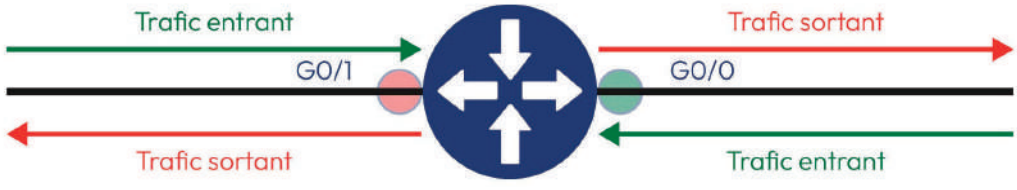
Une ACL est une liste de commandes IOS utilisée pour filtrer les paquets en se basant sur les informations trouvées dans l'en-tête du paquet :



9.1.2. Les opérations ACL :

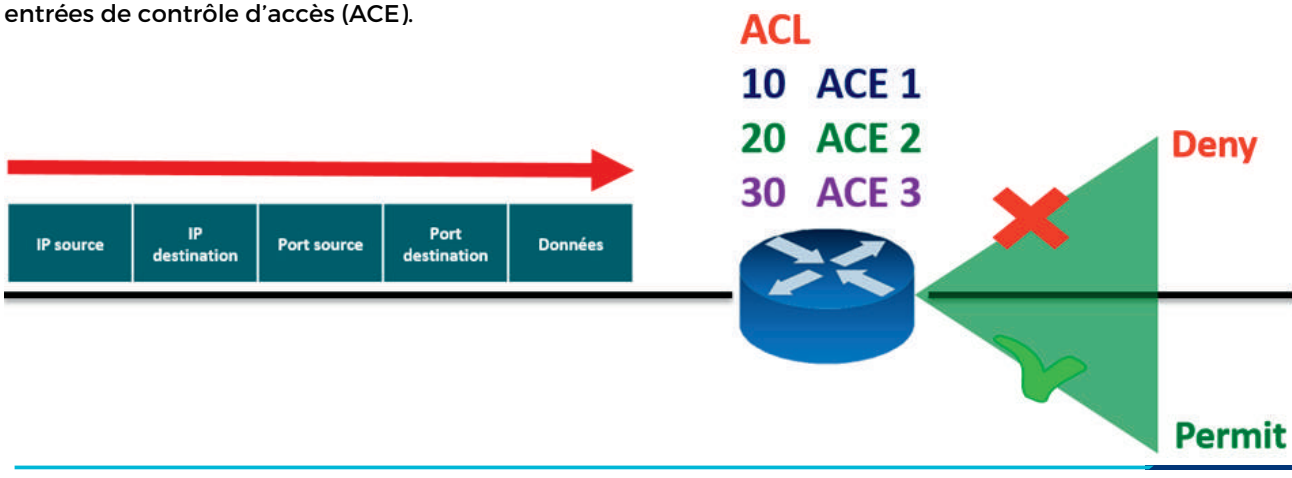
TRAFIC ENTRANT ET TRAFIC SORTANT

Une ACL est appliquée au **trafic entrant**(Inbound) ou au **trafic sortant** (Outbound)

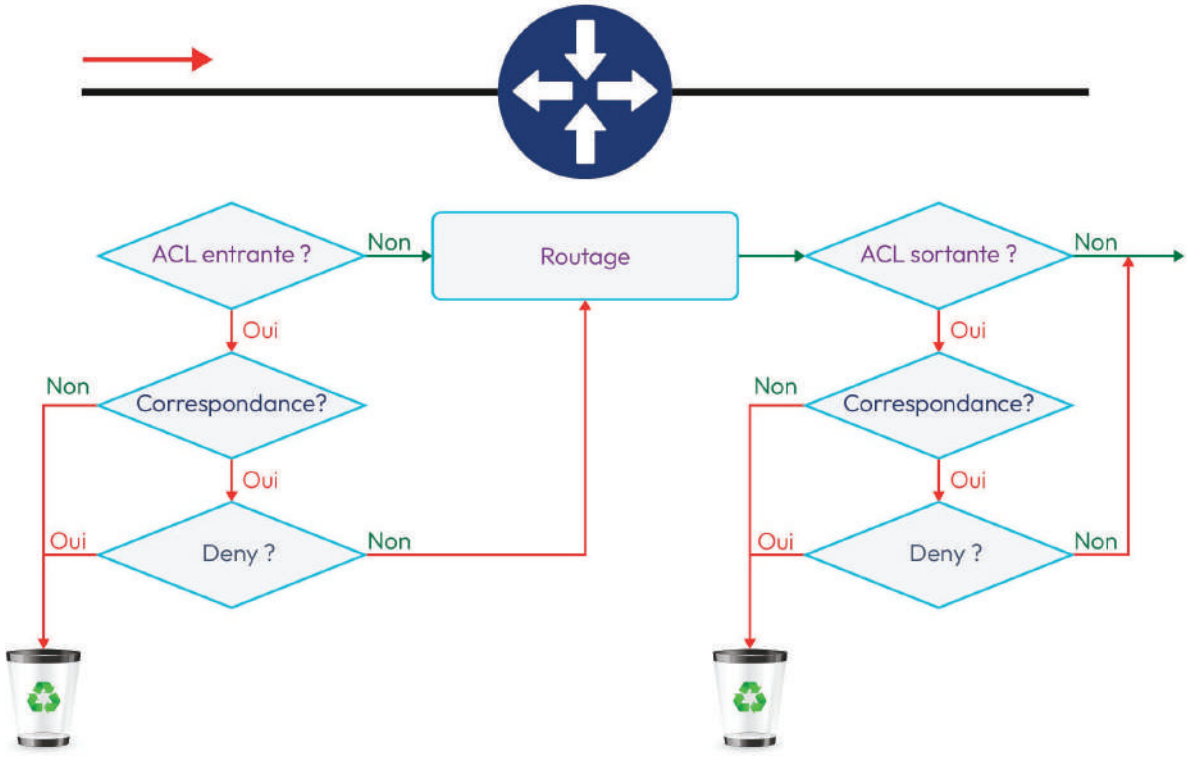


LES ENTRÉES DE CONTRÔLE D'ACCÈS ACE

Une ACL utilise une liste séquentielle d'instructions d'autorisation « **permit** » ou de refus « **deny** », appelées entrées de contrôle d'accès (ACE).



9.1.3. Fonctionnement d'une ACL :



9.2. Le masque inversé :

Les masques génériques, ou wildcard mask, parfois appelés aussi masques inversés, ressemblent à des masques de sous-réseaux, mais au lieu de contenir des bits de sous-réseaux, ils vont contenir des bits d'hôtes.

Ces masques sont utilisés dans différentes solutions réseau, autour des Access Control Lists (ACL) par exemple, mais aussi dans le cadre de protocoles de routage.

Le masque générique est un nombre de 32 bits qui permet de déterminer quels sont les bits d'une adresse IP à vérifier pour trouver la correspondance.

- Le bit 0 du masque générique signifie qu'au niveau de l'adresse IP, le bit doit correspondre.
- Le bit 1 du masque générique signifie qu'au niveau de l'adresse IP, le bit est ignoré.

9.2.1. Correspondance à une seule adresse IP

Données :

- Adresse IP : 192.168.1.1
- Masque inversé : 0.0.0.0

	Décimal	Binaire
Adresse IPv4	192.168.1.1	11000000.10101000.00000001.00000001
Masque générique	0.0.0.0	00000000.00000000.00000000.00000000
Adresses IP correspondantes	**192.168.1.1**	11000000.10101000.00000001.00000001

Tous les bits du masque inversé sont égaux à 0

- ➔ tous les bits de l'adresse IPv4 doivent correspondre
- ➔ une seule adresse IP correspondante : **192.168.1.1**

9.2.2. Correspondance à un réseau :

Données :

- Adresse IP : 192.168.1.1
- Masque inversé : 0.0.0.255

	Décimal	Binaire
Adresse IPv4	192.168.1.1	11000000.10101000.00000001.00000001
Masque générique	0.0.0.255	00000000.00000000.00000000.11111111
Adresses IP correspondantes	**192.168.1.0/24**	11000000.10101000.00000001.00000000

Les 3 derniers octets du masque inversé sont égaux à 0

- ➔ Les 3 derniers octets de l'adresse IPv4 doivent correspondre
- ➔ Les adresses correspondantes sont les adresses qui commencent par « **192.168.1**»
- ➔ Les adresses correspondantes sont toutes les adresses du réseau « **192.168.1.0/24**»

9.2.3. Correspondance à toutes les adresses IPv4 :

Données :

- Adresse IP : 192.168.0.0
- Masque générique (inversé) : 255.255.255.255

	Décimal	Binaire
Adresse IP	192.168.0.0	11000000.10101000.00000000.00000000
Masque générique	255.255.255.255	11111111.11111111.11111111.11111111
Adresses IP correspondantes	**Toutes les adresses IPv4**	

Tous les bits du masque générique sont égaux à 1 :

- ➔ tous les bits de l'adresse IPv4 sont donc ignorés
- ➔ les adresses IP correspondantes, sont toutes les adresses IPv4...

9.2.4. Correspondance à quelques adresses IP particulières

Données :

- Adresse IP : 192.168.0.0
- Masque générique : 0.0.0.254

	Décimal	Binaire
Adresse IPv4	192.168.0.0	11000000.10101000.00000000.00000000
Masque générique	0.0.0.254	00000000.00000000.00000000.11111110
Adresses IP correspondantes	**192.168.0.0** **192.168.0.2** **192.168.0.4** **192.168.0.6** **192.168.0.254**	11000000.10101000.00000000.00000000 11000000.10101000.00000000.00000010 11000000.10101000.00000000.00000100 11000000.10101000.00000000.00000110 11000000.10101000.00000000.11111110

Pour trouver les adresses IP correspondantes :

- On garde les valeurs des bits dont le masque générique est égal à 0 (**en vert**)
- On ignore les valeurs des bits dont le masque générique est égal à 1 (**en rouge**)

➔ les adresses IP correspondantes sont les adresses IP qui commencent par « **192.168.0** » et dont le premier octet est pair.

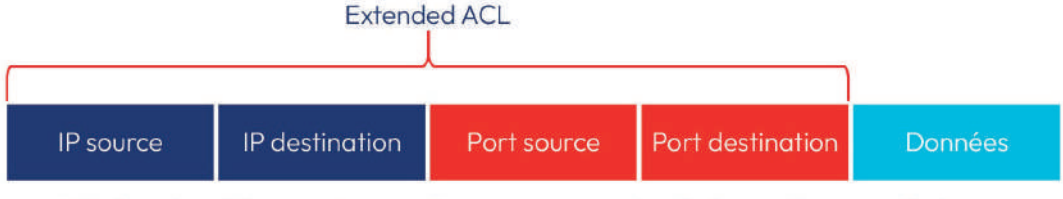
9.3. Types de listes de contrôle d'accès :

9.3.1. ACL standard :

Une ACL standard peut être numérotée ou nommée :

- **Numérotée** : De 1 à 99 ou de 1300 à 1999
- **Nommée** : ACL portant un nom significatif

9.3.2. ACL étendue :



ACL étendue : Elle autorise ou refuse un paquet selon l'adresse IP source, l'adresse IP destination, le type de protocole, le numéro de port source, le numéro de port destination et autres.

Une ACL étendue peut être numérotée ou nommée :

- **Numérotée** : De 100 à 199 ou de 2000 à 2699

Exemple : ACL étendue numéro 100

```
R1(config)#access-list 100 permit tcp  192.168.10.0 0.0.0.255 any eq ftp
R1(config)#access-list 100 permit tcp  192.168.10.0 0.0.0.255 any eq ftp-data
```

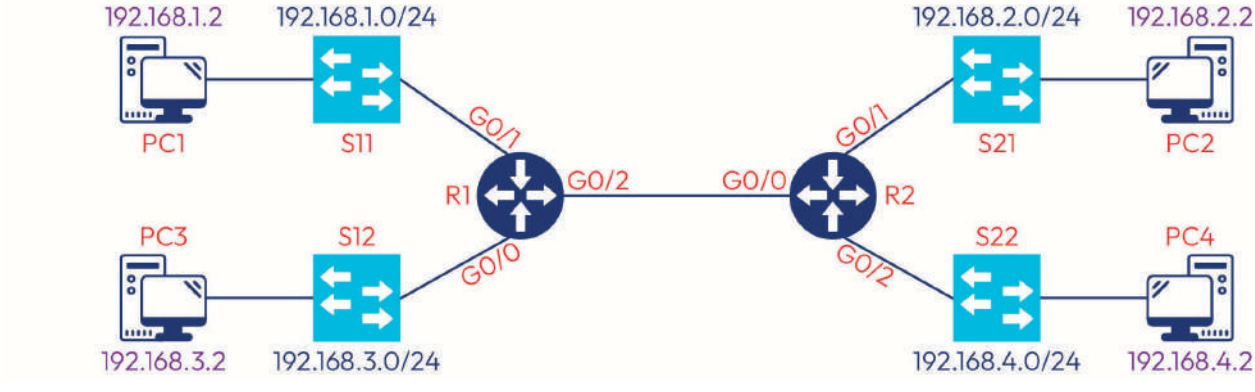
- **Nommée :** ACL portant un nom significatif

Exemple : ACL étendue nommée « FTP-FILTER »

```
R1(config)#ip access-list extended FTP-FILTER
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq ftp
R1(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data
```

9.4. Configuration des ACL :

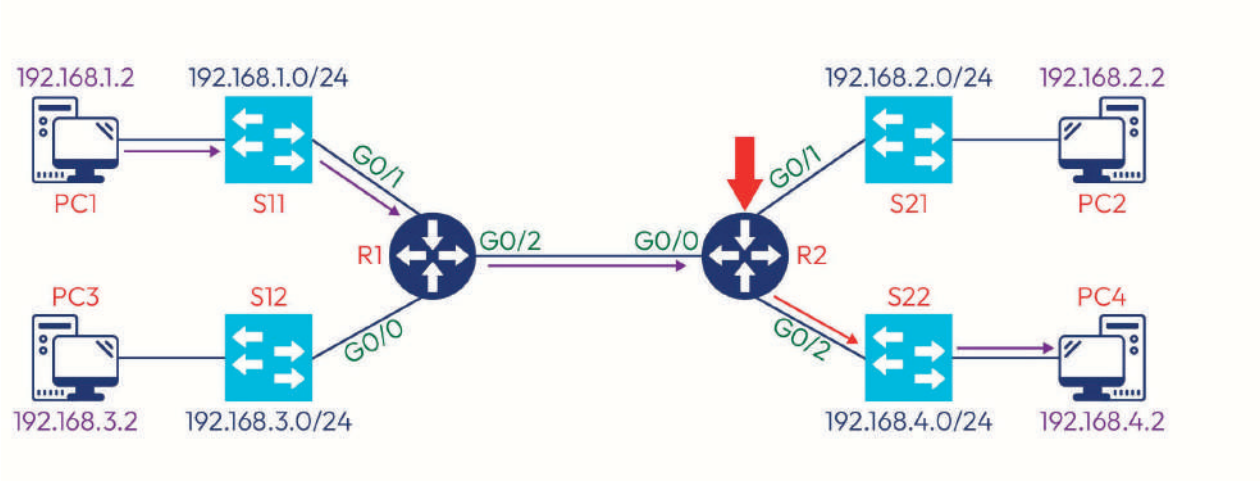
Considérons le schéma suivant :



9.4.1. ACL standard

ACCÈS D'UN SOUS-RÉSEAU À UN AUTRE SOUS-RÉSEAU

Exemple 1 : Refuser l'accès du sous-réseau 192.168.1.0 au sous-réseau 192.168.4.0



Source	192.168.1.0/24	**Routeur**	Le plus proche de la destination (R2)
Destination	192.168.4.0/24	**Interface**	La plus proche de la destination (G0/2 Out)

Configuration :

Utilisation d'une ACL nommée :

```
R2(config)#ip access-list standard SR1-Vers-SR4
R2(config-std-nacl)#deny 192.168.1.0 0.0.0.255
R2(config-std-nacl)#permit any
R2(config-std-nacl)#exit
R2(config)#interface G0/2
R2(config-if)#ip access-group SR1-Vers-SR4 out
```

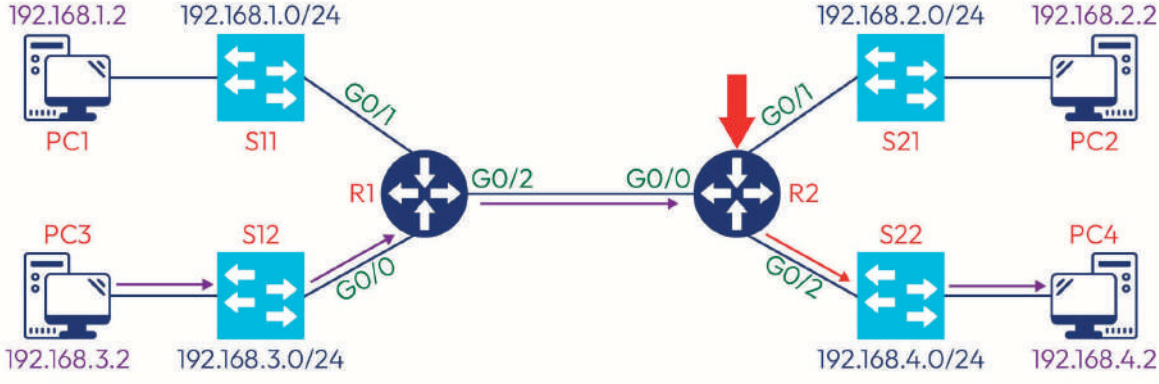
Utilisation d'une ACL numérotée :

```
R2(config)#access-list 1 deny 192.168.1.0 0.0.0.255
R2(config)# access-list 1 permit any
R2(config)#interface G0/2
R2(config-if)#ip access-group 1 out
```

> Si la commande « permit any » n'est pas utilisée, tout le trafic sera refusé.

ACCÈS D'UN HÔTE À UN SOUS-RÉSEAU

Exemple 2 : Refuser l'accès de l'hôte 192.168.3.2 au sous-réseau 192.168.4.0



Source	192.168.3.2	**Routeur**	Le plus proche de la destination (R2)
Destination	192.168.4.0/24	**Interface**	La plus proche de la destination (G0/2 Out)

Configuration :

Utilisation d'une ACL nommée :

```
R2(config)#ip access-list standard PC3-Vers-SR4
R2(config-std-nacl)#deny 192.168.3.2 0.0.0.0
R2(config-std-nacl)#permit any
R2(config-std-nacl)#exit
R2(config)#interface G0/2
R2(config-if)#ip access-group PC3-Vers-SR4 out
```

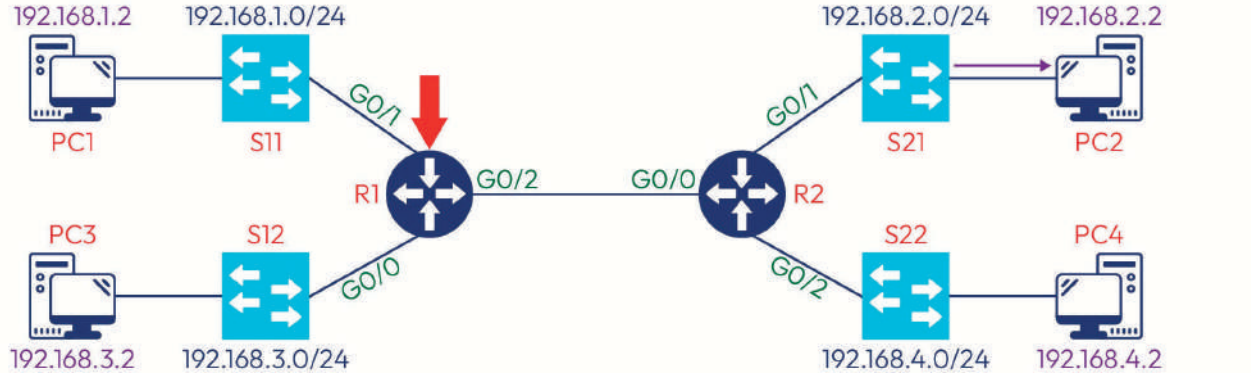
> On peut utiliser le mot-clé « host » au lieu du masque générique (inversé) « 0.0.0.0 »

```
R2(config)#ip access-list standard PC3-Vers-SR4
R2(config-std-nacl)#deny host 192.168.3.2
R2(config-std-nacl)#permit any
R2(config-std-nacl)#exit
R2(config)#interface G0/2
R2(config-if)#ip access-group PC3-Vers-SR4 out
```

Utilisation d'une ACL numérotée :

```
R2(config)#access-list 1 deny host 192.168.3.2
R2(config)# access-list 1 permit any
R2(config)#interface G0/2
R2(config-if)#ip access-group 1 out
```

ACCÈS À DISTANCE VIA TELNET



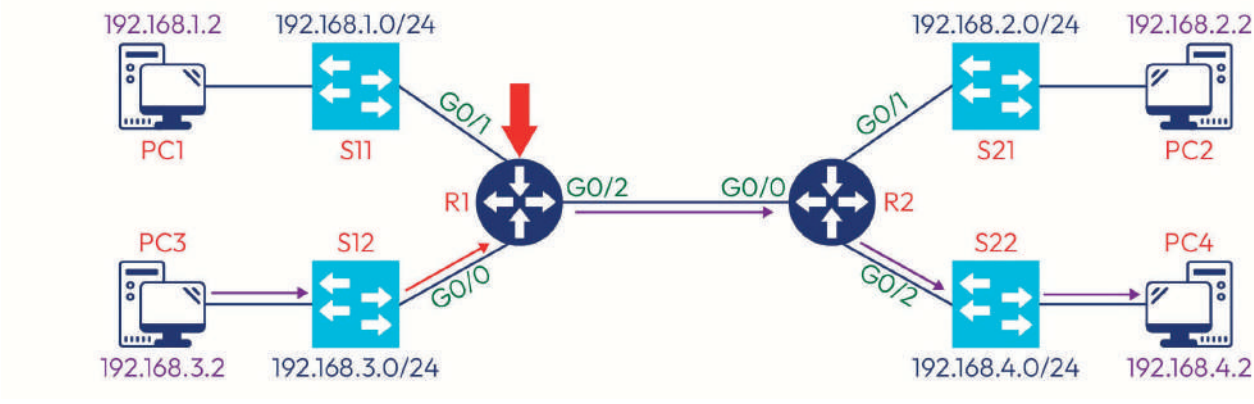
Configuration :

```
R1(config)#ip access-list standard VTY_ACCESS
R1(config-std-nacl)#permit host 192.168.3.2
R1(config-std-nacl)#exit
R1(config)#line vty 0 15
R1(config-line)#access-class VTY-ACCESS in
```

9.4.2. ACL étendue :

ACCÈS D'UN RÉSEAU À UN AUTRE RÉSEAU

Exemple 4 : Refuser l'accès du sous-réseau 192.168.3.0 au sous-réseau 192.168.4.0



Source	192.168.3.0/24	**Routeur**	Le plus proche de la source (R1)
Destination	192.168.4.0/24	**Interface**	La plus proche de la source (G0/0 In)

Configuration :

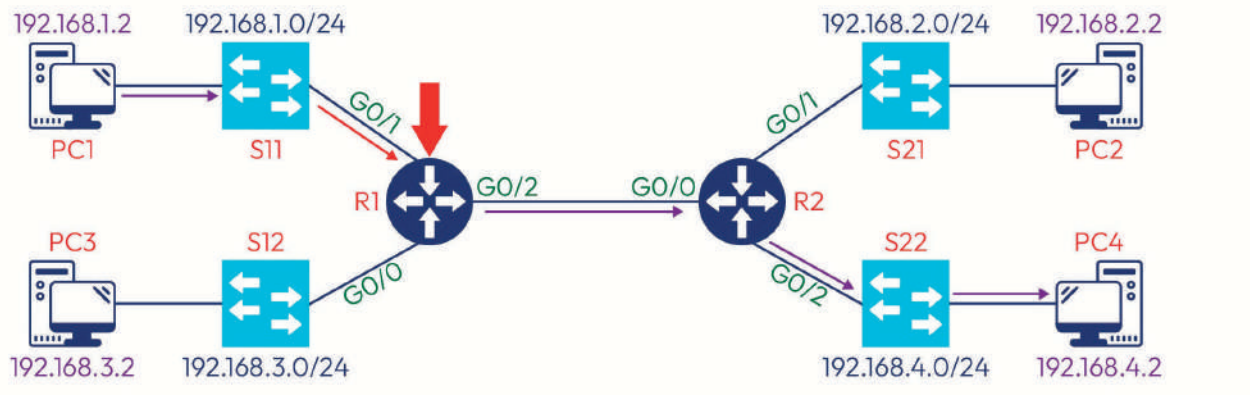
Utilisation d'une ACL nommée :

```
R1(config)#ip access-list extended SR3-Vers-SR4
R1(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#interface G0/0
R1(config-if)#ip access-group SR3-Vers-SR4 in
```

Utilisation d'une ACL numérotée :

```
R1(config)#access-list 100 deny ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255
R1(config)# access-list 100 permit ip any any
R1(config)#interface G0/0
R1(config-if)#ip access-group 100 in
```

Exemple 5 : Refuser l'accès de l'hôte PC1 au sous-réseau 192.168.4.0



Source	192.168.1.2	**Routeur**	Le plus proche de la source (R1)
Destination	192.168.4.0/24	**Interface**	La plus proche de la source (G0/1 In)

Configuration :

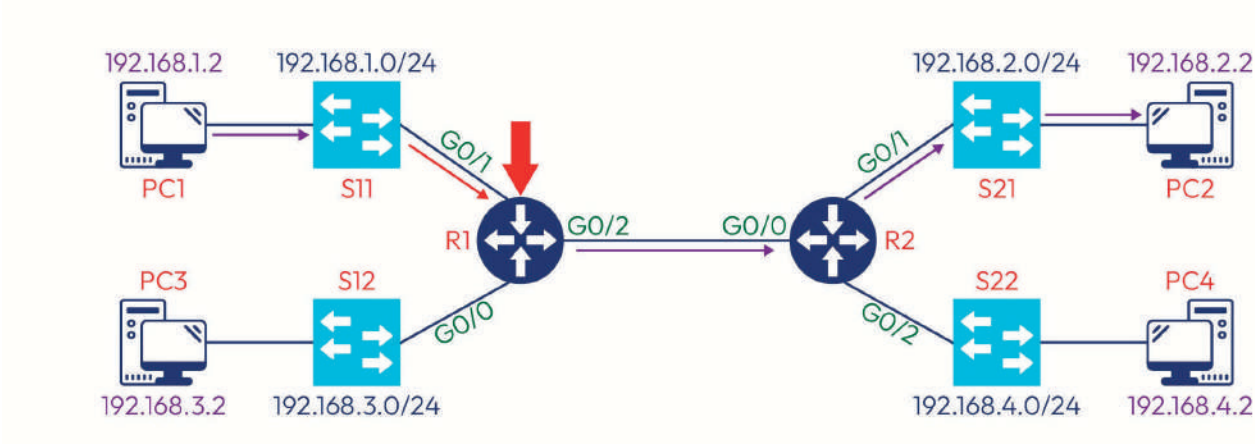
Utilisation d'une ACL nommée :

```
R1(config)#ip access-list extended PC1-Vers-SR4
R1(config-ext-nacl)#deny ip host 192.168.1.2 192.168.4.0 0.0.0.255
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#interface G0/1
R1(config-if)#ip access-group PC1-Vers-SR4 in
```

Utilisation d'une ACL numérotée :

```
R1(config)#access-list 100 deny ip host 192.168.1.2 192.168.4.0 0.0.0.255
R1(config)# access-list 100 permit ip any any
R1(config)#interface G0/1
R1(config-if)#ip access-group 100 in
```

Exemple 6 : Refuser l'accès Web et ICMP de l'hôte PC1 à l'hôte PC2



Source	192.168.1.2	**Routeur**	Le plus proche de la source (R1)
Destination	192.168.2.2	**Interface**	La plus proche de la source (G0/1 In)

Configuration :

Utilisation d'une ACL nommée :

```
R1(config)#ip access-list extended WEB-ET-ICMP
R1(config-ext-nacl)#deny icmp host 192.168.1.2 host 192.168.2.2
R1(config-ext-nacl)#deny tcp host 192.168.1.2 host 192.168.2.2 eq 80
R1(config-ext-nacl)#deny tcp host 192.168.1.2 host 192.168.2.2 eq 443
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#interface G0/1
R1(config-if)#ip access-group WEB-ET-ICMP in
```

Utilisation d'une ACL numérotée :

```
R1(config)#access-list 100 deny icmp host 192.168.1.2 host 192.168.2.2
R1(config)#access-list 100 deny tcp host 192.168.1.2 host 192.168.2.2 eq 80
R1(config)#access-list 100 deny tcp host 192.168.1.2 host 192.168.2.2 eq 443
R1(config)# access-list 100 permit ip any any
R1(config)#interface G0/1
R1(config-if)#ip access-group 100 in
```

AUTRES COMMANDES DE CONFIGURATION :

Affichage des ACL :

```
R1#show access-lists
Extended IP access list WEB-ET-ICMP
10  deny icmp host 192.168.1.2 host 192.168.2.2   ← ACE
20  deny tcp host 192.168.1.2 host 192.168.2.2 eq www
30  deny tcp host 192.168.1.2 host 192.168.2.2 eq 443
40  permit ip any any
```

Numéro de l'ACE

Description d'une ACL :

```
R1(config)#ip access-list extended WEB-ET-ICMP
R1(config-ext-nacl)#deny bloquer le PING et le Web   ← Description d'une ACL
R1(config-ext-nacl)#deny icmp host 192.168.1.2 host 192.168.2.2
R1(config-ext-nacl)#deny tcp host 192.168.1.2 host 192.168.2.2 eq 80
R1(config-ext-nacl)#deny tcp host 192.168.1.2 host 192.168.2.2 eq 443
R1(config-ext-nacl)#permit ip any any
```

Suppression des ACL et des ACE :

Suppression de l'ACL standard numéro 1 :

```
R1(config)# no access-list 1
```

Suppression de l'ACL étendue numéro 100 :

```
R1(config)# no access-list 100
```

Suppression de l'ACL étendue « ACL1 » :

```
R1(config)# no ip access-list extended ACL1
```

Suppression de l'ACL standard « ACL2 » :

```
R1(config)# no ip access-list standard ACL2
```

Suppression de l'entrée ACE numéro 10 de l'ACL standard « ACL2 » :

```
R1(config)# ip access-list standard ACL2
R1(config-std-nacl)# no 10
```

Modification d'une ACL :

Ajout d'une entrée ACE numéro entre les deux entrées 10 et 20 au niveau de l'ACL standard 1 qui autorise le trafic de la machine 192.168.1.2 :

```
R1(config)# ip access-list standard 1
R1(config-std-nacl)# 15 permit host 192.168.1.2
```

Ajout d'une entrée ACE numéro entre les deux entrées 10 et 20 au niveau de l'ACL étendue ACL1 qui autorise le trafic de la machine 192.168.1.2 vers tous les réseaux :

```
R1(config)# ip access-list extended ACL1
R1(config-ext-nacl)# 15 permit ip host 192.168.1.2 any
```

> Une liste des numéros de ports des différents protocoles se trouve au niveau du fichier suivant : « C:\Windows\System32\drivers\etc\services»

Pour conclure :

Les listes de contrôle d'accès (ACL) sont un mécanisme de sécurité utilisé pour autoriser ou refuser l'accès à des ressources réseau, comme les routes, les protocoles et les périphériques.

Les ACL peuvent être basées sur des critères tels que l'adresse IP, le port et le protocole, et peuvent être utilisées pour appliquer des politiques de sécurité différentes à différents utilisateurs ou groupes d'utilisateurs.

Les ACL peuvent être utilisées à différents niveaux de la pile de protocoles réseau, notamment au niveau des routeurs, des commutateurs et des périphériques de sécurité réseau.

Les ACL sont un outil essentiel pour la mise en place de politiques de sécurité efficaces dans les réseaux informatiques modernes.