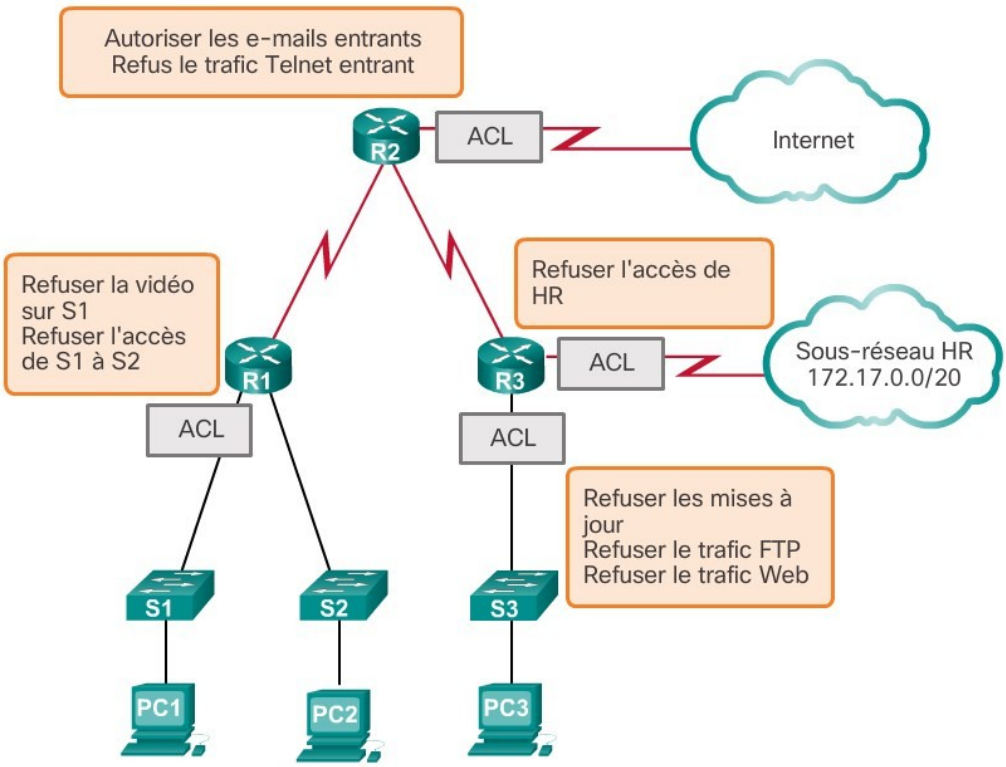
Access Control List

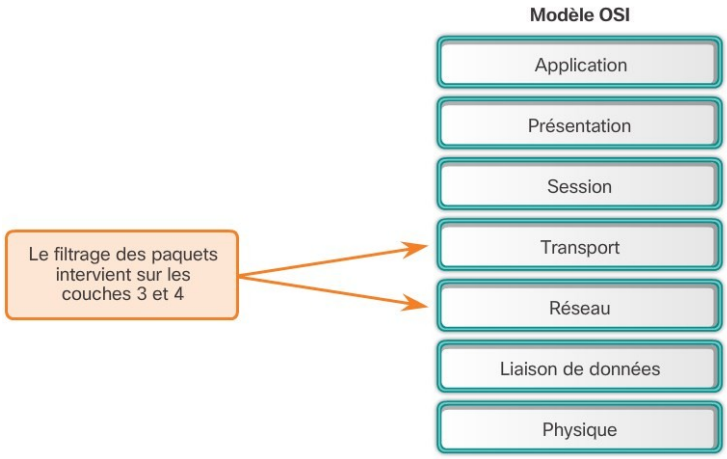
1 Définition

Les ACL (Access Control Lists) permettent de filtrer des paquets suivant des critères définis par l'utilisateur, il est ainsi possible de filtrer les paquets entrants ou sortant d'un routeur en fonction des protocoles (eigrp,icmp,igmp,igrp,ip,ospf,tcp ou udp).

A quoi servent les ACL ?



Les ACL de routage dans le modèle OSI



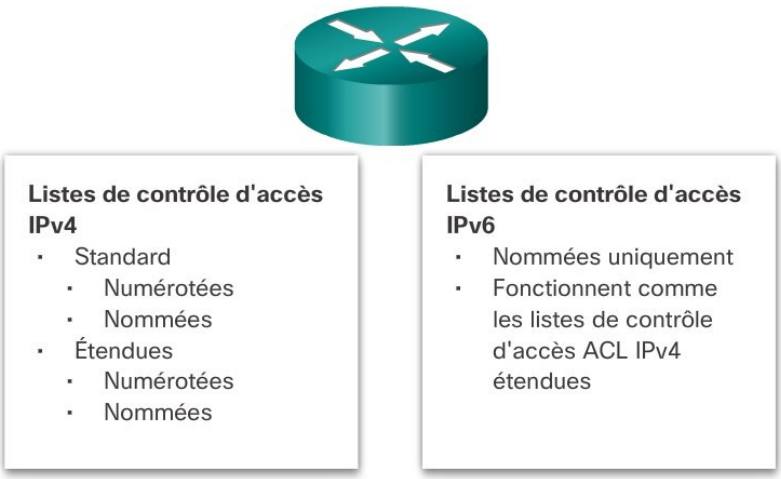
Pour évaluer le trafic réseau, la liste de contrôle d'accès extrait les informations suivantes de l'en-tête de paquet de couche 3 :

- Adresse IP source
- Adresse IP de destination
- Type de message ICMP

La liste de contrôle d'accès peut également extraire des informations de couche supérieure à partir de l'en-tête de couche 4, notamment :

- Port source TCP/UDP
- Port de destination TCP/UDP

Différence entre ACL ipv4 et IPV6



2 Types d'ACL

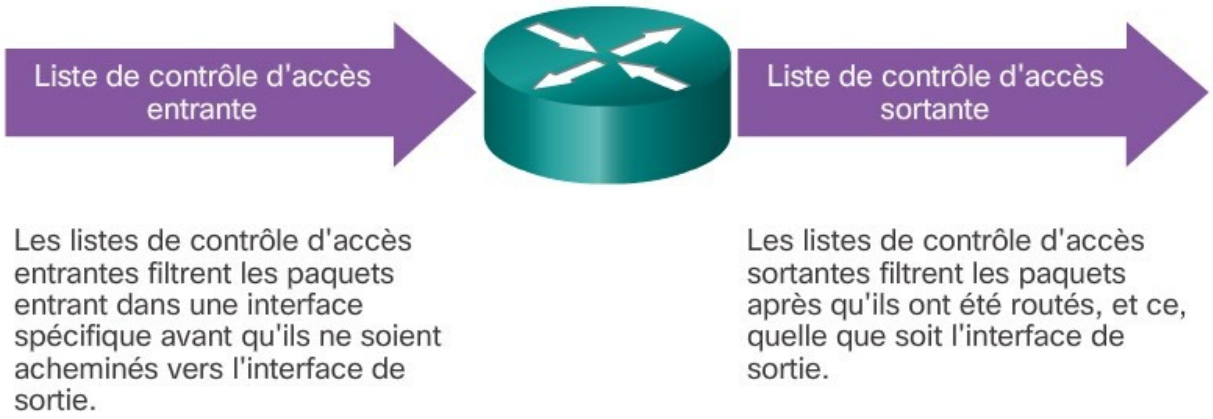
Standard : uniquement sur les «IP sources»

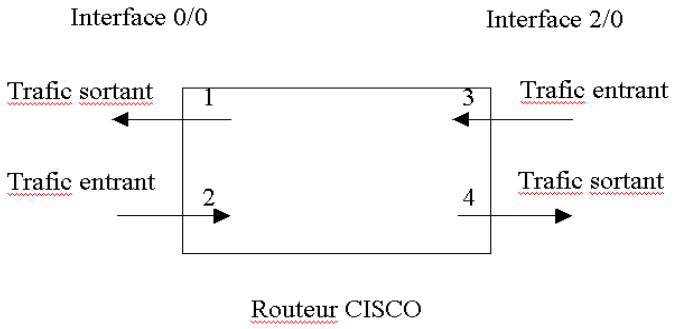
Étendue : sur quasiment tous les champs des en-têtes IP, TCP et UDP

Les filtres les plus utilisés:

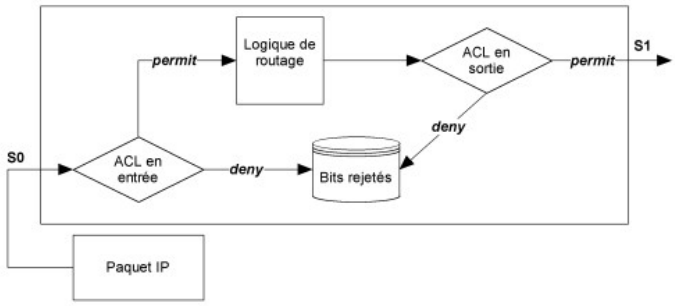
- IP source ou destination
- Du type de protocole (TCP, UDP, ICMP, IGRP, IGMP, …)
- Des Ports Sources et Destination

3 Shéma de principe ACL

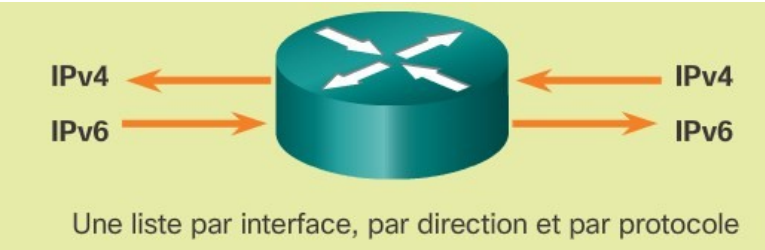




Une ACL peut être appliquée sur une interface du routeur en entrée ou en sortie



Norme sur la création des ACL



Avec 2 interfaces et 2 protocoles le routeur pourra contenir 8 ACL

La règle des 3 P pour l'utilisation d'un des ACL

Vous ne pouvez avoir qu'une liste de contrôle d'accès par protocole, par interface et par direction :

Une liste de contrôle d'accès par protocole (p. ex., IPv4 ou IPv6)

Une liste de contrôle d'accès par direction (c.-à-d., entrant ou sortant)

Une liste de contrôle d'accès par interface (p. ex., FastEthernet0/0)

4 Résumer sur le fonctionnement des ACL :

Le paquet est vérifié par rapport au **1er critère** défini

S'il vérifie le critère, l'action définie est appliquée

Sinon le paquet est comparé successivement par rapport aux ACL suivantes

S'il ne satisfait aucun **critère**, l'action ***deny*** **implicite est appliquée**

Les critères sont définit sur les informations contenues dans les en-têtes IP, TCP ou UDP des paquets

Pourquoi utiliser l'instruction « deny any » en fin d'ACL, elle est implicite lorsque l'on crée un ACL, une bonne pratique consiste a la configurer, cela on faisant la commande « show access-list X » elle apparaîtra dans la liste des ACL.

5 Les masques

Distinguez les 2 types de masques :

1. **Le masque générique est un masque de filtrage - utilisé pour les ACL**

   Quand un bit a la valeur 0 dans un mask, il y a **vérification du bits sur l'adresse IP** a contrario lorsque la valeur du **bit sera 1 il n'y aura pas de vérification avec l'@IP.**

Exemple :

Ce masque défini la portion de l'adresse IP qui doit être examinée 0.0.255.255 signifie que seuls les 2 premiers octets doivent être examinés deny 10.1.3.0 avec 0.0.0.255 : refus de toutes les IP commençant par 10.1.3

2. **le masque de réseau, masque de regroupement - utilisé pour les réseaux**

   L'@ip et le MASK utilisant la fonction ET logique permet de distinguer la partie réseau de la partie hôte.
   Un MASK réseau doit être une continuité de 1 et de 0, **le masque générique peut être une suite quelconque de 1 et de 0 suivant le filtrage** que l'on veut obtenir sur l'adressage IP.

6 Fonctionnement des ACL

Test des règles les unes après les autres
Si aucune règle n'est applicable, rejet du paquet

7 Access-list standart

La mise en place d'une ACL se déroule en 2 étapes :

1. Création de l' ACL
2. Application sur une ou plusieurs interfaces en entrée ou en sortie

a. Création de l'ACL - Définition d'une règle

access-list « *number »* [**deny**|**permit**|**remark line**] *source* [source-wildcard] [log]

« Number » compris entre 1 et 99 ou entre 1300 et 1999

access-list « *number »* **remark** *test*

log : ajoute un message dans la console pour chaque paquet correspondant

b. Activation d'une ACL sur une interface

ip access-group [*number* | *name* [**in** | **out**]]

Visualiser les ACL

show access-lists [*number* | *name*] : toutes les ACL quelque soit l'interface

show ip access-lists [*number* | *name*] : les ACL uniquement liés au protocole IP

Exemple 1

```
interface Ethernet0
ip address 172.16.1.1 255.255.255.0
ip access-group 1 out

access-list 1 remark stop tous les paquets d'IP source 172.16.3.10
access-list 1 deny 172.16.3.10 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255
```

access-list 1 deny 172.16.3.10 0.0.0.0	Refuse les paquets d'IP source 172.16.3.10 Le masque - wildcard mask signifie ici que tous les bits de l'adresse IP sont significatifs
access-list 1 permit 0.0.0.0 255.255.255.255	Tous les paquets IP sont autorisés Le masque 255.255.255.255 signifie qu'aucun bit n'estcsignificatif

Exemple 1 autre écriture

```
interface Ethernet0
ip address 172.16.1.1 255.255.255.0
ip access-group 1 out

access-list 1 remark stop tous les paquets d'IP source 172.16.3.10
access-list 1 deny host 172.16.3.10
access-list 1 permit any
```

Une notation améliorée est possible pour remplacer le masque 255.255.255.255 qui désigne une machine ou autrement dit comme les bits sont a 1 il n'y a pas de vérification avec @source.

Utilisation du terme host 0.0.0.0 avec le wildcard masque à 255.255.255.255 qui désigne tout le monde : **permit 0.0.0.0**

255.255.255.255

comme tous les bits du masque sont a 1 il n'y aura pas de vérification avec @ip_source qui est 0.0.0.0 tout le monde
Utilisation du terme **permit any**

Exemple 3

```
interface Ethernet0
ip address 172.16.1.1 255.255.255.0
ip access-group 1 out

interface Ethernet1
ip address 172.16.2.1 255.255.255.0
ip access-group 2 in

access-list 1 remark Stoppe tous les paquets d'IP source 172.16.3.10
access-list 1 deny host 172.16.3.10
access-list 1 permit any

access-list 2 remark Autorise que les trames d'IP source 172.16.3.0/24
access-list 2 permit 172.16.3.0 0.0.0.255
```

8 Les extended ACL:

Les ACL étendues permettent filtrer des paquets en fonction:

-L'adresse IP « source »
-L'adresse IP de « destination »
-Du type de protocole « TCP, UDP, ICMP, IGRP, IGMP, ... »
-Le numéro de Port « source »
-Le numéro de Port « destination »
-et autre cf fichier commande access-list

9 Syntaxe acces-list extended

La différence entre les ACL standards et étendues est le « number »

« number » :

Protocole	Plage
IP	1 - 99 et 1300 - 1999
IP étendu	100 - 199 et 2000 - 2699

a. Définition de la règle

access-list « ***number*** » { **deny** | **permit** } « *protocol* » « *source* » « *sourcewildcard* » [*opérateur port + numéro de port*] « *destination* » « *dest.-wildcard* » [*opérateur port+numéro de port*] [**log**]

Étape de création de l'ACL :

1. numéro d'acl entre 100-199 et 2000-2699
2. action que l'on veut, deny ou permit
3. Le protocole qui nous intéresse
4. adresse source d'ou provient le paquet
5. le mask générique pour définir la parti de l'ip source qui nous intéresse
6. tout protocole réseau utilise des ports référencés ou pas il va falloir le préciser a la règle, ici on positionne le port du protocole que l'on souhaite autoriser ou bloqué si on ne met pas de port se sera le protocole entier qui sera bloqué, par conséquent tous les port de ce protocoles, un jeu d'opérateur est proposer pour affiner le filtrage des ports, a savoir je veux filtrer tous les ports supérieur au ports 2000 en provenance du protocole TCP
7. adresse destination
8. mask générique, partie ip qui nous intéresse
9. idem étape 4, le ou les ports a bloquer + opérateurs suivant le besoin

number : compris entre 100 et 199 ou 2000 et 2699

« Opérateur port »

lt - less than
gt – greater than
eq – equal
neq – not equal
range - inclusive

b. Activation d'une ACL extended sur une interface

ip access-group [*number* | *name* [**in** | **out**]]

Exemple d'ACL extended

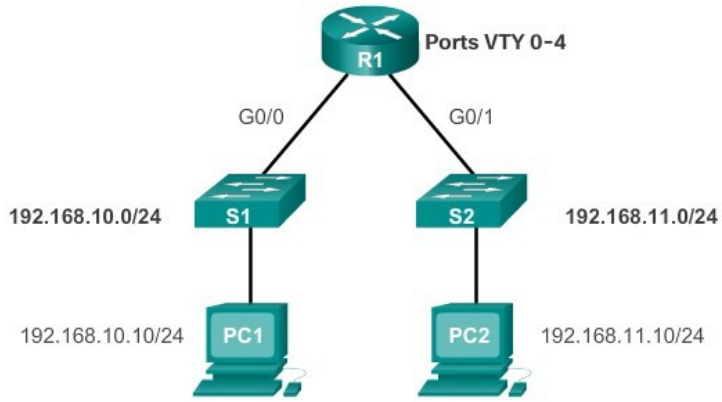
access-list 101 deny ip any host 10.1.1.1	Refus des paquets IP à destination de la machine 10.1.1.1 et provenant de n'importe quelle source
access-list 101 deny tcp any gt 1023 host 10.1.1.1 eq 23	Refus de paquet TCP provenant d'un port > 1023 et à destination du port 23 de la machine d'IP 10.1.1.1
access-list 101 deny tcp any host 10.1.1.1 eq http	Refus des paquets TCP à destination du port 80 de la machine d'IP 10.1.1.1

10 Suppression d'ACL

a-Une ACL numéroté peut être composé de nombreuses règles. La seule façon de la modifier et de faire

> **no access-list «** *number »*
> Puis de la recréé

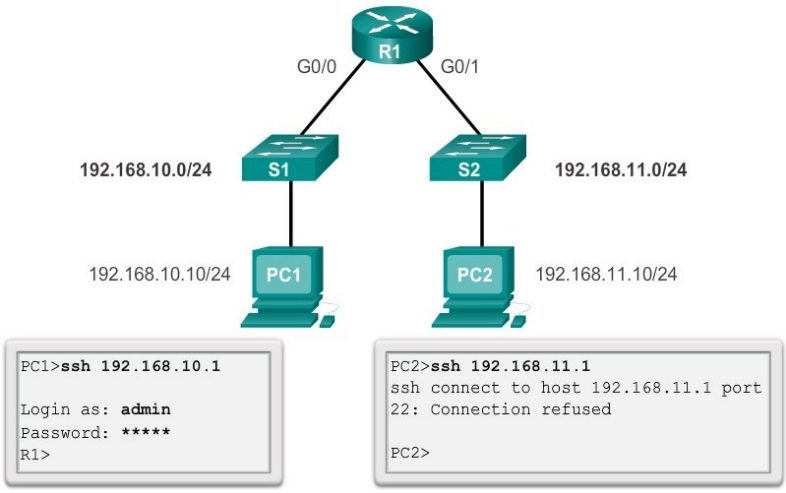
Configuration d'une liste de contrôle d'accès standard pour sécuriser un port VTY




```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class 21 in
R1(config-line)# exit
R1(config)# access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 21 deny any
```

Vérification d'une liste de contrôle d'accès standard utilisée pour sécuriser un port VTY

```
R1# show access-lists
Standard IP access list 21
    10 permit 192.168.10.0, wildcard bits 0.0.0.255 (2 matches)
    20 deny   any (1 match)
R1#
```



11 les ACL nommées standart ou étendues

Les ACL nommée peuvent être utilisée aussi bien sur les ACL standard que sur les ACL étendues, elles permettent de supprimer qu'une seule ligne au lieu de toutes (ACL standard ou étendues numérotées) et elles sont mises en place sur l'interface par le nom affecté pour la création

Attribution d'un nom standart a la liste de contrôle d'accés

Les noms doivent se composer de caractères alphanumériques.
Il est conseillé d'écrire le nom en MAJUSCULES.
Les noms ne doivent pas contenir d'espaces ni de signes de ponctuation.
Il est possible d'ajouter et de supprimer des entrées de la liste de contrôle d'accès.

Créer une ACL étendue nommée BLOCK_R1

ip access-list extended BLOCK_R1

deny ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
permit ospf any any
permit icmp any host 10.3.0.2
permit icmp any host 10.13.205.1
permit tcp any any eq www established
permit icmp any host 10.1.0.2

Mise en place sur une interface en entrée / in

interface Serial0/0/0

ip address 10.1.0.2 255.255.255.0
ip access-group BLOCK_R1 in

Vérification de l'ACL BLOCK_R1 et visualisation de leur numérotation automatique

R2#show access-lists

Extended IP access list BLOCK_R1
10 deny ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
20 permit ospf any any (318 match(es))
30 permit icmp any host 10.1.0.2
40 permit icmp any host 10.3.0.2
50 permit icmp any host 10.13.205.1
60 permit tcp any any eq www established

ou sans lnumérotation

R2#show access-lists BLOCK_R1

Extended IP access list BLOCK_R1
deny ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
permit ospf any any (327 match(es))
permit icmp any host 10.1.0.2
permit icmp any host 10.3.0.2
permit icmp any host 10.13.205.1
permit tcp any any eq www established

Voir l'ACL BLOCK_R1 posée sur l'interface en entée

R2#sh ip interface serial 0/0/0

Serial0/0/0 is up, line protocol is up (connected)
Internet address is 10.1.0.2/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is BLOCK_R1

Suppression de l'ACL 30 permit icmp any host 10.1.0.2

R2(config)#ip access-list extended BLOCK_R1

R2(config-ext-nacl)#no 30 permit icmp any host 10.1.0.2
R2(config-ext-nacl)#do show access-list
Extended IP access list BLOCK_R1
10 deny ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
20 permit ospf any any (396 match(es))
40 permit icmp any host 10.3.0.2 //la ligne 30 a était supprimée
50 permit icmp any host 10.13.205.1
60 permit tcp any any eq www established

insertion de « permit icmp any host 10.1.0.2 » supprimer précédemment est positionnée en fin de l'ACL nommée

R2(config-ext-nacl)#do show access-list

Extended IP access list BLOCK_R1
10 deny ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
20 permit ospf any any (406 match(es))
40 permit icmp any host 10.3.0.2
50 permit icmp any host 10.13.205.1
60 permit tcp any any eq www established
70 permit icmp any host 10.1.0.2

Suppression de l'ACL 70 et repositionnement d'origine sur la ligne 30

R2(config-ext-nacl)#no 70 permit icmp any host 10.1.0.2

R2(config-ext-nacl)#30 permit icmp any host 10.1.0.2
R2(config-ext-nacl)#do show access-list
Extended IP access list BLOCK_R1
10 deny ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
20 permit ospf any any (420 match(es))
30 permit icmp any host 10.1.0.2
40 permit icmp any host 10.3.0.2
50 permit icmp any host 10.13.205.1
60 permit tcp any any eq www established

11 Pose d'une ACL sur les Lignes VTY (telnet)

```
access-list 3 permit 10.1.1.0 0.0.0.255

line vty 0 4
login
password Cisco
access-class 3 in          //      access-class number { in | out }
```

12 Le Tshoot / dépannage

Comment vérifier la syntaxe et l'emplacement des Acl sur votre routeurs

Show access-list num_acl ou Show access-list

Savoir ou l'ACL a été appliquée et dans qu'elle direction

Show ip intreface g0/1 ou show ip interface

Exemple :

Sur R3, exécutez la commande **show access-lists 1**.

```
R3# show access-list 1
Standard IP access list 1
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
    30 deny   any
```

Sur R3, exécutez la commande **show ip interface g0/1**.

```
R3# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 1
  Inbound access list is not set
  Output omitted
```

La requête ping envoyée depuis un routeur, utilise l'interface la plus proche de destination comme @ip source

13 Les conseils sur les ACL

La création, la mise à jour, le débogage nécessitent beaucoup de temps et de rigueur dans la syntaxe Il est donc conseillé

De créer les ACL à l'aide d'un éditeur de texte et de faire un copier/coller dans la configuration du routeur

Placer les extended ACL au plus près de la source du paquet que possible pour le détruire le plus vite possible

Placer les ACL standard au plus près de la destination sinon, vous risquez de détruire un paquet trop top

Rappel : les ACL standard ne regardent que l'IP source du paquet

Placer la règle la plus spécifique en premier

Avant de faire le moindre changement sur une ACL, désactiver sur l'interface concerné celle-ci (no ip access-group)
exemple de fichier de configuration avec des acl's

```
GAD#show running-config
Building configuration...

Current configuration : 1586 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname GAD
!
ip subnet-zero
!
no ip domain-lookup
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 111 in
 ip access-group 112 out
!
interface Serial0/0
 ip address 172.16.1.2 255.255.255.0
 ip access-group 121 in
 no fair-queue
 clockrate 56000
!
interface FastEthernet0/1
 ip address 10.10.10.1 255.255.255.0
 ip access-group 101 in
 ip access-group 102 out
!
interface Serial0/1
 no ip address
 shutdown
!
router rip
 network 10.0.0.0
 network 172.16.0.0
!
ip classless
no ip http server
!
access-list 101 permit ip 10.10.10.0 0.0.0.255 any
access-list 101 deny   ip any any
access-list 102 permit tcp any any established
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any unreachable
access-list 102 deny   ip any any
access-list 111 permit ip 10.1.1.0 0.0.0.255 any
access-list 111 deny   ip any any
access-list 112 permit tcp any host 10.1.1.10 eq www
access-list 112 permit icmp 10.10.10.0 0.0.0.255 host 10.1.1.10
access-list 112 deny   ip any any
access-list 121 deny   ip 10.10.10.0 0.0.0.255 any
access-list 121 deny   ip 127.0.0.0 0.255.255.255 any
access-list 121 deny   ip 224.0.0.0 31.255.255.255 any
access-list 121 permit ip any any
!
line con 0
 password cisco
 login
line aux 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

Les ACL en IPV6

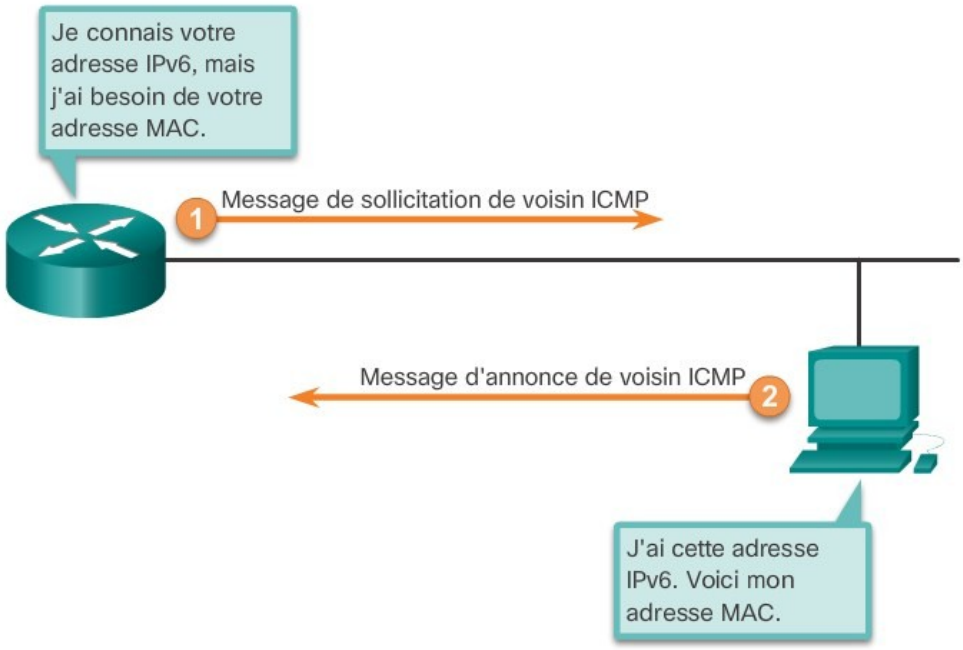
Il n'existe qu'un seul type d'ACL IPV6 il correspond à une ACL étendue IPV4 nommée, il n'y a pas d'ACL IPV6 numérotées.

Les caractéristiques IPV6 :

- Elles sont nommées uniquement
- Leurs fonctionnalités équivaut à celle d'une ACL IP étendue

Une ACL IPV4 et IPV6 ne peuvent portées le même nom

Découverte des voisins



Application d'une ACL ipv6 sur une interface

sous ipv4 – ip access-group
sous ipv6 – ipv6 traffic-filter

Aucun masque générique

la longueur de préfixe est utilisé pour indiquer dans qu'elle mesure l'adresse ipv6 source ou destination doit correspondre

instructions supplémentaires par défaut

a la fin d'une ACL ipv4 il une instruction implicite deny any ou deny any any

il existe également une instruction deny ipv6 any any

en ipv6 2 instructions implicites sont appliquées par défaut :

permit icmp any any nd-na

permit icmp any any nd-ns

Ces instructions permettent au routeur de prendre part à l'équivalent ipv6 du protocole ARP pour ipv4 .
Ipv6 utilise des messages de découvertes de voisins – ND Nieghbor Discovery – ICMP pour effectuer la même opération .

La découverte des voisins fait appel à des messages de sollicitation de voisin ND – NS Neigbor solicitation et d'annonce de voisin ND– NA pour neighbor advertissement

Les messages ND sont encapsulés en paquets ipv6 et nécessite des services de la couche réseau ipv6 tandis que ARP n'utilise pas la couche 3.

Étant donné qu'ipv6 utilise le service de couche 3 pour la découverte des voisins, les ACL doivent autorisée implicitement l'envoi et la réception des paquets ND sur une interface.

Plus précisément les messages ND – NA découverte de voisin-annonce de voisin et ND-NS découverte de voisin-sollicitation de voisin sont autorisés.

Format la commande access-list ipv6

R1(config)# ipv6 access-list access-list-name

R1(config-ipv6-acl) # deny | permit protocol « source-ipv6-prefix/prefix-lengh | any | host source-ipv6-address » [operator [port-number]] « destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address » [operator [port-number]]

deny | permit indique si le paquet doit être refusé ou autorisé

protocol saisir le nom ou le numéro d'un protocol internet ou un nombre entier correspondant à un numéro de protocole ipv6

source-ipv6-prefix/prefix-lenght
destination-ipv6-address réseau source ou destination ipv6 ou catégories de réseau pour lesquelles vous souhaiter définir des conditions de refus ou d'autorisation

any sert d'abréviation du préfixe ipv6 ::/0 , cela correspond a toutes les adresses

host dans host source-ipv6-address ou destination-ipv6-address , saisissez l'@ source ou destination de l'hôte ipv6 pour lequel vous souhaiter définir des conditions de refus ou d'autorisation

operator facultatif – opérande comparant les ports source ou de destination du protocole spécifié . Les opérandes sont IT-inférieur à / gt – supérieur à / neq – non egal à / range – plage

port-number facultatif – nombre décimal ou nom d'un port TCP ou UDP de filtrage de TCP ou UDP respectivement

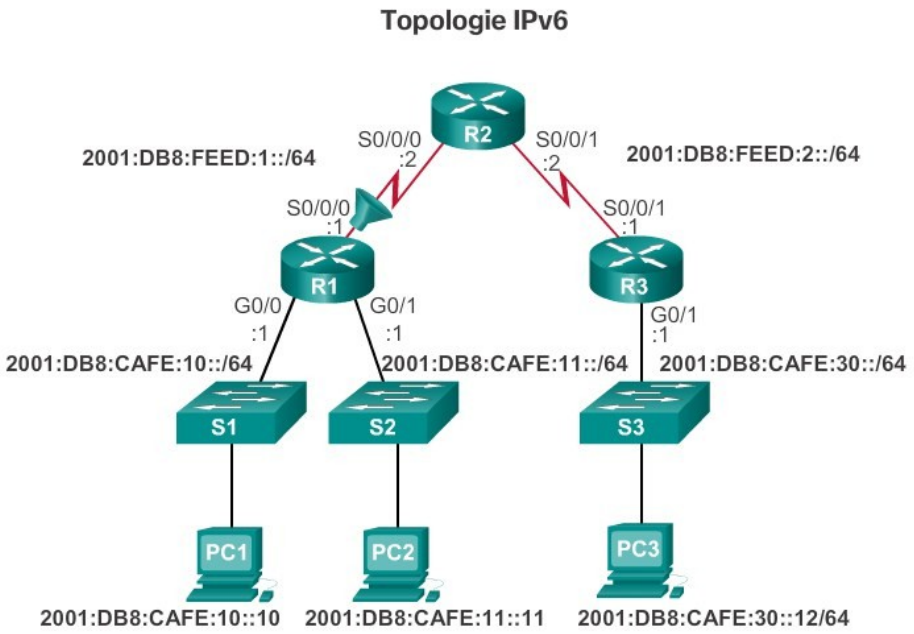
Exemple

```
R1(config)#ipv6 access-list NO-R3-LAN-ACCESS
R1(config-ipv6-acl)#deny ipv6 2001:db8:cafe:30 ::/64 any
R1(config-ipv6-acl)#permit ipv6 any any
```

La première instruction nomme la liste d'accès IPv6 NO-R3-LAN-ACCESS. Comme dans le cas d'IPv4, vous n'êtes pas obligé d'écrire les noms des listes de contrôle d'accès en majuscule, mais cela permet de les repérer plus facilement dans le résultat de la commande running-config.

La deuxième instruction refuse tous les paquets IPv6 provenant de 2001:DB8:CAFE:30::/64 destinés à n'importe quel réseau IPv6. La troisième instruction autorise tous les autres paquets IPv6.

Application de l'ACL




```
R1(config)# interface s0/0/0
R1(config-if)# ipv6 traffic-filter NO-R3-LAN-ACCESS in
```

Une fois que la liste de contrôle d'accès IPv6 est configurée, elle est associée à une interface à l'aide de la commande **ipv6 traffic-filter** :

Router(config-if)# **ipv6 traffic-filter***access-list-name* { **in** | **out** }

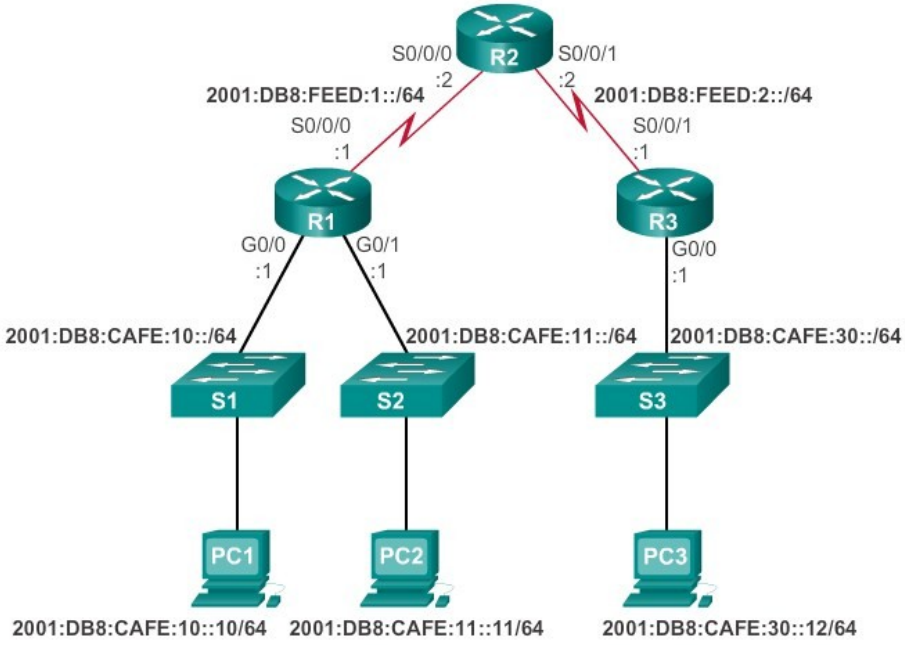
L'application de la liste de contrôle d'accès à l'interface S0/0/0 entrante provoque le refus des paquets provenant de 2001:DB8:CAFE:30::/64 sur les deux réseaux locaux de R1.

Pour supprimer une liste de contrôle d'accès d'une interface, saisissez d'abord la commande **no ipv6 traffic-filter** sur l'interface, puis la commande globale **no ipv6 access-list**.

la commande **access-class** est utilisée à la fois par IPv4 et IPv6 pour appliquer une liste d'accès aux ports VTY.

Exemple d'ACL ipv6

topologie ipv6



refuser les connexions FTP

```
R1(config)#ipv6 access-list NO-FTP-TO-11
R1(config-ipv6-acl)#deny TCP any 2001:DB8:cafe:11 ::/64 eq ftp
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#exit
R1(config)#interface g0/0
R1(config-if)#ipv6 traffic-filter NO-FTP-TO-11 in
```

le routeur R1 est configuré avec une liste d'accès IPv6 pour refuser le trafic FTP vers 2001:DB8:CAFE:11::/64. Les ports utilisés pour les données FTP (port 20) et le contrôle FTP (port 21) doivent être bloqués. Étant donné que le filtre est appliqué en entrée à l'interface G0/0 sur R1, seul le trafic provenant du réseau 2001:DB8:CAFE:10::/64 sera refusé.

```
R3(config)#ipv6 access-list RESTRICTED-ACCESS

R3(config-ipv6-acl)#remark permit access only HTTP and HTTPS to network

R3(config-ipv6-acl)#permit tcp any host 2001:db8:cafe:10::10 eq 80
R3(config-ipv6-acl)#permit tcp any host 2001:db8:cafe:10::10 eq 443

R3(config-ipv6-acl)#remark deny all other trafic to network 10

R3(config-ipv6-acl)#deny ipv6 any 2001:db8:cafe:10 ::/64

R3(config-ipv6-acl)#remark permit PC3 telnet access to PC2

R3(config-ipv6-acl)#permit tcp host 2001:db8:cafe:30::12 host 2001:db8 :cafe:11::11 eq 23
```

R3(config-ipv6-acl)#remark deny telnet access to pc2 for all other device

R3(config-ipv6-acl)#deny tcp any host 2001:db8 :cafe:11::11 eq 23

R3(config-ipv6-acl)#remark permit access to everything else

R3(config-ipv6-acl)#permit ipv6 any any

R3(config-ipv6-acl)#exit

R3(config)#interface g0/0

R3(config)#ipv6 traffic-filter RESTRICTED-ACCESS in

une liste de contrôle d'accès IPv6 est configurée pour accorder au réseau local sur R3 un accès limité aux réseaux locaux sur R1. Des commentaires sont ajoutés à la configuration pour documenter la liste de contrôle d'accès. Les éléments suivants ont été marqués dans la liste de contrôle d'accès :

1. Les deux premières instructions d'autorisation permettent l'accès de n'importe quel périphérique au serveur Web à l'adresse 2001:DB8:CAFE:10::10.

2. Tous les autres périphériques se voient refuser l'accès au réseau 2001:DB8:CAFE:10::/64.

3. PC3 sur 2001:DB8:CAFE:30::12 est autorisé à accéder via Telnet à PC2 portant l'adresse IPv6 2001:DB8:CAFE:11::11.

4. Tous les autres périphériques se voient refuser l'accès Telnet à PC2.

5. Le reste du trafic IPv6 est autorisé vers toutes les autres destinations.

6. La liste d'accès IPv6 est appliquée à l'interface G0/0 dans la direction entrante, de sorte que seul le réseau

Vérification des ACL

```
R3# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Global unicast address(es):
    2001:DB8:CAFE:30::1, subnet is 2001:DB8:CAFE:30::/64
  Input features: Access List
  Inbound access list RESTRICTED-ACCESS
<résultat omis>
```

Confirmation que l'ACL RESTRICTED-ACCESS est configuré dans la direction entrante de l'interface G0/0

```
R3# show access-lists
IPv6 access list RESTRICTED-ACCESS
    permit tcp any host 2001:DB8:CAFE:10::10 eq www sequence 20
    permit tcp any host 2001:DB8:CAFE:10::10 eq 443 sequence 30
    deny ipv6 any 2001:DB8:CAFE:10::/64 sequence 50
    permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq
    telnet sequence 70
    deny tcp any host 2001:DB8:CAFE:11::11 eq telnet sequence 90
    permit ipv6 any any sequence 110
```

Affiche toutes les ACL du routeur ipv4 et ipv6, notez que pour l'ipv6 , les numéros d'ordre figure a la fin de l'instruction

et non au début comme ipv4.
Bien que les instructions apparaissent dans l'ordre dans lequel elles ont étaient saisies, les incréments ne sont pas toujours de 10. Cela est du au fait que les instructions de remarque saisies étaient identifiées par un numéro d'ordre , mais n'apparaissent dans le résultat de la commande show access-list.

De la même manière que les acl ipv4 étendues , les instructions sont affichées et traitées dans l'ordre dans lequel elles ont été saisies dans l'acl .

```
R3# show running-config
<résultat omis>
ipv6 access-list RESTRICTED-ACCESS
 remark Permit access only HTTP and HTTPS to Network 10
 permit tcp any host 2001:DB8:CAFE:10::10 eq www
 permit tcp any host 2001:DB8:CAFE:10::10 eq 443
 remark Deny all other traffic to Network 10
 deny ipv6 any 2001:DB8:CAFE:10::/64
 remark Permit PC3 telnet access to PC2
 permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11
 eq telnet
 remark Deny telnet access to PC2 for all other devices
 deny tcp any host 2001:DB8:CAFE:11::11 eq telnet
 remark Permit access to everything else
 permit ipv6 any any
```

Affiche toutes les ACE et les instructions de remarque.
Les instructions de remarque peuvent être placées avant ou après les instructions permit ou deny , mais la position doit être homogène.