

## Supports du formateur Chapitre 4 : listes de contrôle d'accès



# CCNA Routing and Switching Connecting Networks

Cisco | Networking Academy®  
Mind Wide Open™



# Documents du formateur – Guide de planification pour le chapitre 4

Cette présentation PowerPoint est divisée en deux parties :

## 1. Guide de planification du formateur

- Informations destinées à vous familiariser avec le chapitre
- Outils pédagogiques

## 2. Présentation en classe pour le formateur

- Diapositives facultatives que vous pouvez utiliser en classe
- Commence à la diapositive 9

Remarque : supprimez le guide de planification de cette présentation avant de la partager.



# Connecting Networks

## Guide de planification

### Chapitre 4 : listes de contrôle d'accès



Cisco | Networking Academy®  
Mind Wide Open™



# Chapitre 4 : exercices

Quels sont les exercices associés à ce chapitre ?

N° de page	Type d'exercice	Nom de l'exercice	En option ?
4.1.1.5	Exercice	Détermination du masque générique approprié	-
4.1.1.6	Exercice	Fonctionnement des listes de contrôle d'accès	-
4.1.2.6	Exercice	Positionnement des listes de contrôle d'accès standard et étendues	-
4.1.3.5	Packet Tracer	Configuration des listes de contrôle d'accès IPv4 standard	En option
4.1.3.6	Vidéo	Configuration des listes de contrôle d'accès standard première partie	-
4.1.3.7	Vidéo	Configuration des listes de contrôle d'accès standard deuxième partie	-
4.2.2.7	Exercice	Création d'une instruction de liste de contrôle d'accès étendue	-
4.2.2.8	Exercice	Évaluation d'entrées de contrôle d'accès étendues	-
4.2.2.9	Exercice	Testlet de liste de contrôle d'accès	-
4.2.2.10	Packet Tracer	Configuration des listes de contrôle d'accès étendues - scénario 1	En option
4.2.2.11	Packet Tracer	Configuration des listes de contrôle d'accès étendues - scénario 2	En option
4.2.2.12	Packet Tracer	Configuration des listes de contrôle d'accès étendues - scénario 3	En option
4.2.2.13	Atelier	Configuration et vérification des listes de contrôle d'accès étendues	Recommandé
4.3.2.6	Packet Tracer	Configuration des listes de contrôle d'accès IPv6	En option



# Chapitre 4 : exercices (suite)

Quels sont les exercices associés à ce chapitre ?

N° de page	Type d'exercice	Nom de l'exercice	En option ?
4.3.2.7	Atelier	Configuration et vérification des listes de contrôle d'accès IPv6	Recommandé
4.4.1.5	Exercice	Remettre dans l'ordre les étapes du processus décisionnel des listes de contrôle d'accès	-
4.4.2.9	Packet Tracer	Dépannage des listes de contrôle d'accès IPv4	Recommandé
4.4.2.10	Packet Tracer	Dépannage des listes de contrôle d'accès IPv6	Recommandé
4.4.2.11	Atelier	Dépannage de la configuration et du placement des listes de contrôle d'accès	En option
4.5.1.1	Packet Tracer	Challenge d'intégration des compétences	Recommandé

Le mot de passe utilisé dans les exercices Packet Tracer de ce chapitre est : PT\_ccna5



# Chapitre 4 : évaluation

- Une fois qu'ils ont terminé le chapitre 4, les étudiants doivent se soumettre à l'évaluation correspondante.
- Les questionnaires, les travaux pratiques, les exercices dans Packet Tracer, ainsi que les autres activités peuvent servir à évaluer, de manière informelle, les progrès des élèves.



# Chapitre 4 : bonnes pratiques

Avant d'enseigner le contenu du chapitre 4, l'instructeur doit :

- Terminer la partie « Évaluation » du Chapitre 4.
- S'assurer que tous les exercices sont terminés. C'est un concept très important et le temps passé sur les travaux pratiques est primordial.
- Faire aux élèves de nombreuses activités de création de listes de contrôle d'accès.
- Encourager les élèves à se connecter avec leur identifiant cisco.com et à lire

[http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_data\\_acl/configuration/15-sy/sec-data-acl-15-sy-book/sec-acl-ov-gdl.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/15-sy/sec-data-acl-15-sy-book/sec-acl-ov-gdl.html)



# Chapitre 4 : aide supplémentaire

- Si vous avez besoin de conseils pour améliorer vos stratégies de formation, de plans de cours, d'idées d'analogies pour illustrer des concepts complexes ou encore de sujets de discussion, rendez-vous sur le site de la communauté CCNA sur la page [community.netacad.net](http://community.netacad.net).
- Si vous souhaitez partager des plans de cours ou des ressources, chargez-les sur le site de la communauté CCNA afin d'aider les autres instructeurs.

# Cisco | Networking Academy®

Mind Wide Open™

## Chapitre 4 : listes de contrôle d'accès



## Connecting Networks



# Chapitre 4 - Sections et objectifs

- 4.1 Configuration et fonctionnement des listes de contrôle d'accès standard
  - Configuration des listes de contrôle d'accès IPv4 standard.
- 4.2 Listes de contrôle d'accès IPv4 étendues
  - Configuration de listes de contrôle d'accès IPv4 étendues.
- 4.3 Listes de contrôle d'accès IPv6
  - Configuration des listes de contrôle d'accès IPv6.
- 4.4 Dépannage des listes de contrôle d'accès
  - Dépannage des listes de contrôle d'accès.

## 4.1 Examen de la configuration et du fonctionnement des listes de contrôle d'accès standard





## Présentation du fonctionnement des listes de contrôle d'accès

# Listes de contrôle d'accès et masque générique

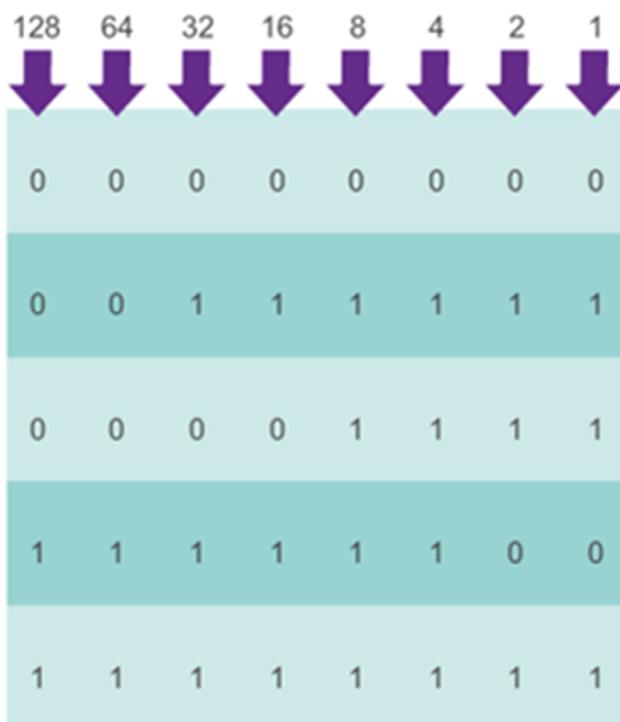
- Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus, appelées entrées de contrôle d'accès (ACE).
- Lorsque le trafic réseau traverse une interface configurée avec une liste de contrôle d'accès, le routeur compare les informations figurant dans le paquet à chaque entrée de contrôle d'accès.
- Une entrée de contrôle d'accès IPv4 comprend l'utilisation d'un masque générique afin de filtrer les adresses IPv4.



# Présentation du fonctionnement des listes de contrôle d'accès Listes de contrôle d'accès et masque générique (suite...)

## Masque générique

Position de bit d'octet et valeur d'adresse du bit



### Exemples

= Correspondance de tous les bits d'adresse (correspondance complète)

= Les 6 derniers bits d'adresse sont ignorés

= Les 4 derniers bits d'adresse sont ignorés

= Les 6 premiers bits d'adresse sont ignorés

= Tous les bits dans l'octet sont ignorés

0 indique d'établir une concordance avec la valeur du bit d'adresse correspondant  
1 indique d'ignorer la valeur du bit d'adresse correspondant



# Présentation du fonctionnement des listes de contrôle d'accès Listes de contrôle d'accès et masque générique (suite...)

## Masques génériques correspondant à des hôtes et sous-réseaux IPv4

### Exemple 1

	Décimal	Binaire
Adresse IP	192.168.1.1	11000000.10101000.00000001.00000001
Masque générique	0.0.0.0	00000000.00000000.00000000.00000000
Résultat	192.168.1.1	11000000.10101000.00000001.00000001

### Exemple 2

	Décimal	Binaire
Adresse IP	192.168.1.1	11000000.10101000.00000001.00000001
Masque générique	255.255.255.255	11111111.11111111.11111111.11111111
Résultat	0.0.0.0	00000000.00000000.00000000.00000000

### Exemple 3

	Décimal	Binaire
Adresse IP	192.168.1.1	11000000.10101000.00000001.00000001
Masque générique	0.0.0.255	00000000.00000000.00000000.11111111
Résultat	192.168.1.0	11000000.10101000.00000001.00000000



# Présentation du fonctionnement des listes de contrôle d'accès

## Application de listes de contrôle d'accès à une interface

### Listes de contrôle d'accès entrantes et sortantes



Les listes de contrôle d'accès entrantes filtrent les paquets entrant dans une interface spécifique avant qu'ils ne soient acheminés vers l'interface de sortie.

Les listes de contrôle d'accès sortantes filtrent les paquets après qu'ils ont été routés, et ce, quelle que soit l'interface de sortie.



# Présentation du fonctionnement des listes de contrôle d'accès

## Application de listes de contrôle d'accès à une interface (suite...)

Filtrage du trafic avec liste de contrôle d'accès sur un routeur



Une liste par interface, par direction et par protocole

Avec deux interfaces et deux protocoles, ce routeur peut avoir un total de 8 listes de contrôle d'accès appliquées.

### Les règles pour appliquer des listes de contrôle d'accès

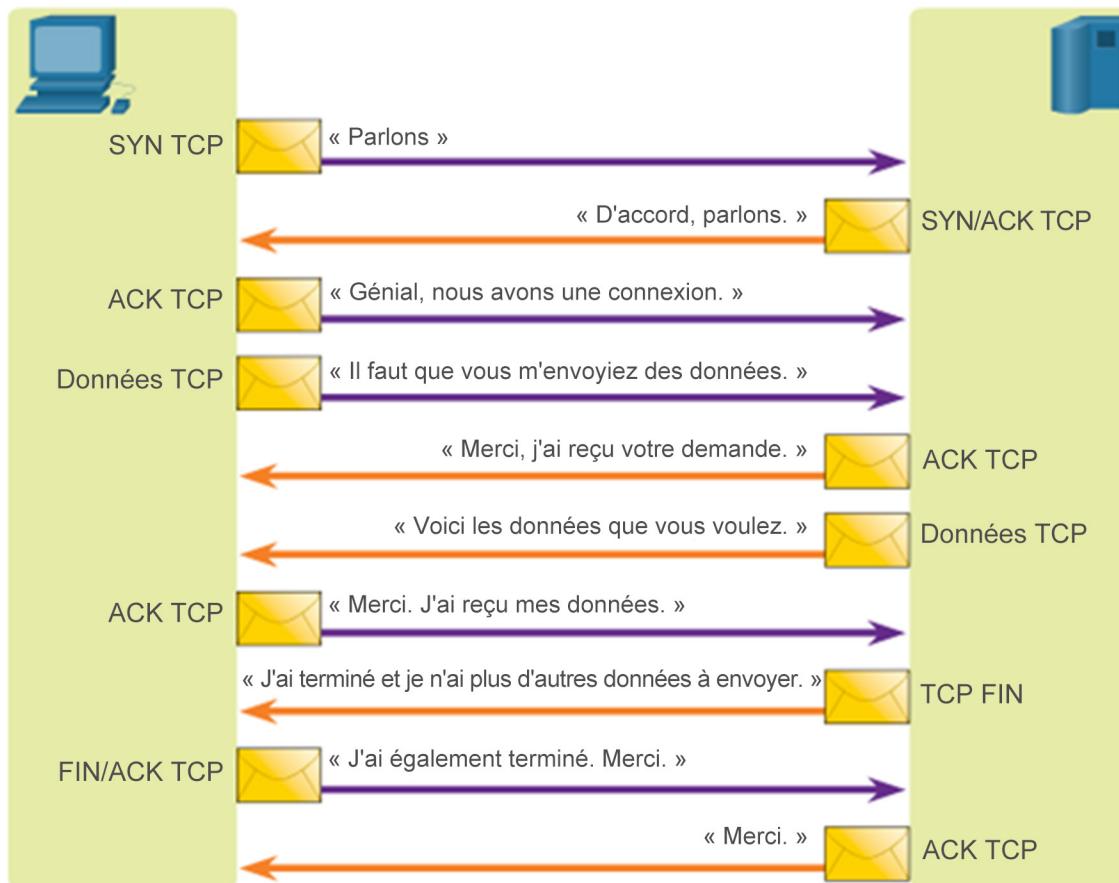
Vous ne pouvez avoir qu'une liste de contrôle d'accès par protocole, par interface et par direction :

- 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., GigabitEthernet0/0)



# Présentation du fonctionnement des listes de contrôle d'accès

## Une conversation TCP



Les segments TCP sont repérés par des indicateurs qui signalent leur objet :

- un **SYN** démarre (**synchronise**) la session
- un **ACK** est un accusé de réception du segment attendu
- un **FIN** termine la session



# Présentation du fonctionnement des listes de contrôle d'accès

## Une conversation TCP (suite...)

- Le segment de données TCP identifie également le port correspondant au service demandé.

Numéros de port

Plage de numéros de port	Groupe de ports
De 0 à 1023	Ports réservés
De 1024 à 49151	Ports inscrits
De 49152 à 65535	Ports dynamiques et/ou privés

Numéros de ports reconnus

Numéro de port	Protocole	Application	Acronyme
20	TCP	Protocole FTP (File Transfer Protocol) (données)	FTP
21	TCP	Protocole FTP (File Transfer Protocol) (contrôle)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	-
25	TCP	Protocole SMTP (Simple Mail Transfer Protocol)	SMTP
53	UDP, TCP	Domain Name Service (service de noms de domaines)	DNS
67	UDP	Protocole DHCP (Dynamic Host Configuration Protocol) (serveur)	DHCP
68	UDP	Protocole DHCP (Dynamic Host Configuration Protocol) (client)	DHCP
69	UDP	Protocole TFTP (Trivial File Transfer Protocol)	TFTP
80	TCP	Protocole HTTP (Hypertext Transfer Protocol)	HTTP
110	TCP	Protocole POP (Post Office Protocol) version 3	POP3
143	TCP	Protocole IMAP (Internet Message Access Protocol)	IMAP
161	UDP	Protocole SNMP (Simple Network Management Protocol)	SNMP
443	TCP	Protocole HTTPS (Hypertext Transfer Protocol Secure)	HTTPS

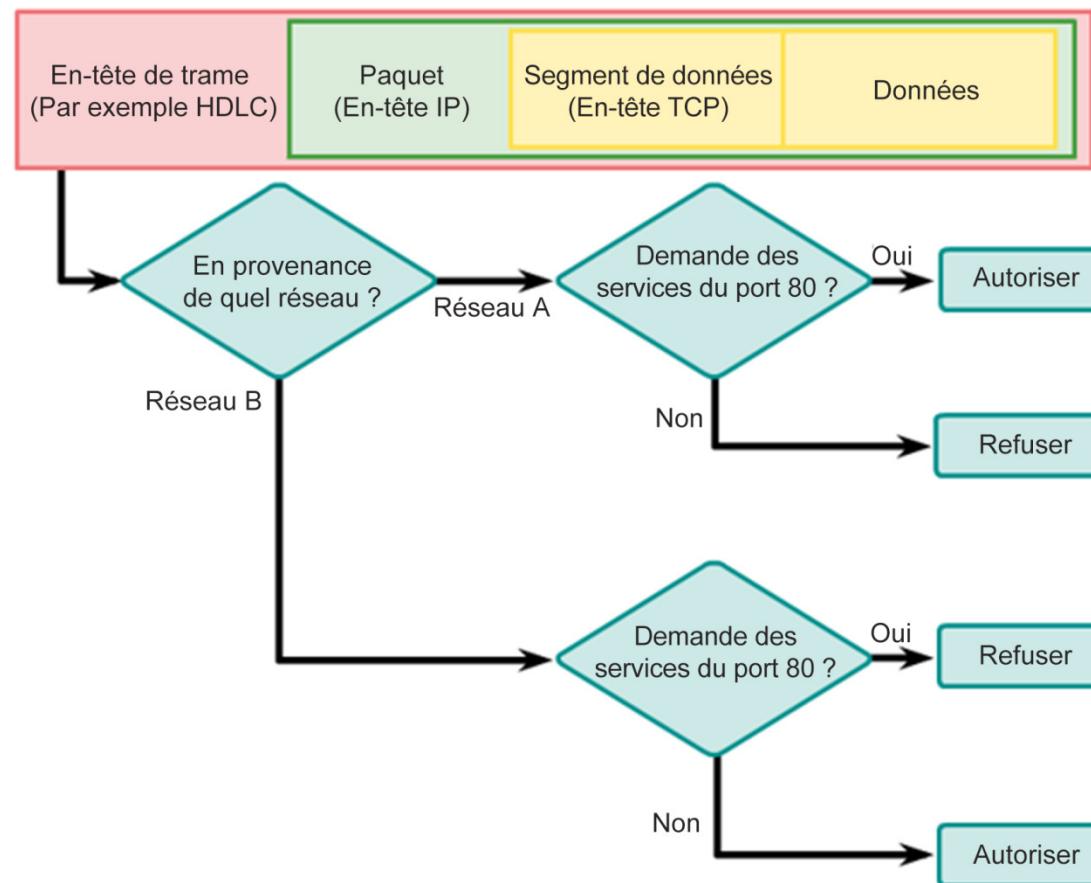


# Présentation du fonctionnement des listes de contrôle d'accès

## Filtrage des paquets par les listes de contrôle d'accès

- Le filtrage des paquets contrôle l'accès à un réseau en analysant les paquets entrants et sortants, puis les transmet ou les rejette selon les critères donnés.

Exemple de filtrage des paquets





## Types de listes de contrôle d'accès IPv4

# Listes de contrôle d'accès IPv4 standard et étendues

- Il y a deux types de listes de contrôle d'accès IPv4 Cisco :
  - Standard
    - Les listes de contrôle d'accès standard peuvent être utilisées pour autoriser ou refuser le trafic uniquement depuis des adresses IPv4 source. La destination du paquet et les ports concernés ne sont pas évalués
  - Étendu
    - Les listes de contrôle d'accès étendues filtrent les paquets IPv4 en fonction de différents critères :
      - Type de protocole
      - Adresse IPv4 source
      - Adresse IPv4 de destination
      - Ports TCP ou UDP source
      - Ports TCP ou UDP de destination
      - Informations facultatives sur le type de protocole pour un contrôle plus précis



## Types de listes de contrôle d'accès IPv4

# Listes de contrôle d'accès IPv4 standard et étendues (suite...)

### Listes de contrôle d'accès standard

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

### Listes de contrôle d'accès étendues

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Les listes de contrôle d'accès étendues filtrent les paquets IP en fonction de plusieurs attributs, notamment :

- Les adresses IP source et de destination
- Les ports TCP et UDP source et de destination
- Type de protocole/numéro de protocole (exemple : IP, ICMP, UDP, TCP, etc.)



## Types de listes de contrôle d'accès IPv4

# Listes de contrôle d'accès numérotées et nommées

- Les listes de contrôle d'accès standard et étendues peuvent être identifiées par un numéro ou par un nom lors de leur création.

## Liste de contrôle d'accès numérotée :

Attribution d'un numéro en fonction du protocole à filtrer.

- Plages 1 à 99 et 1 300 à 1 999 : listes de contrôle d'accès IP standard
- Plages 100 à 199 et 2 000 à 2 699 : listes de contrôle d'accès IP étendues

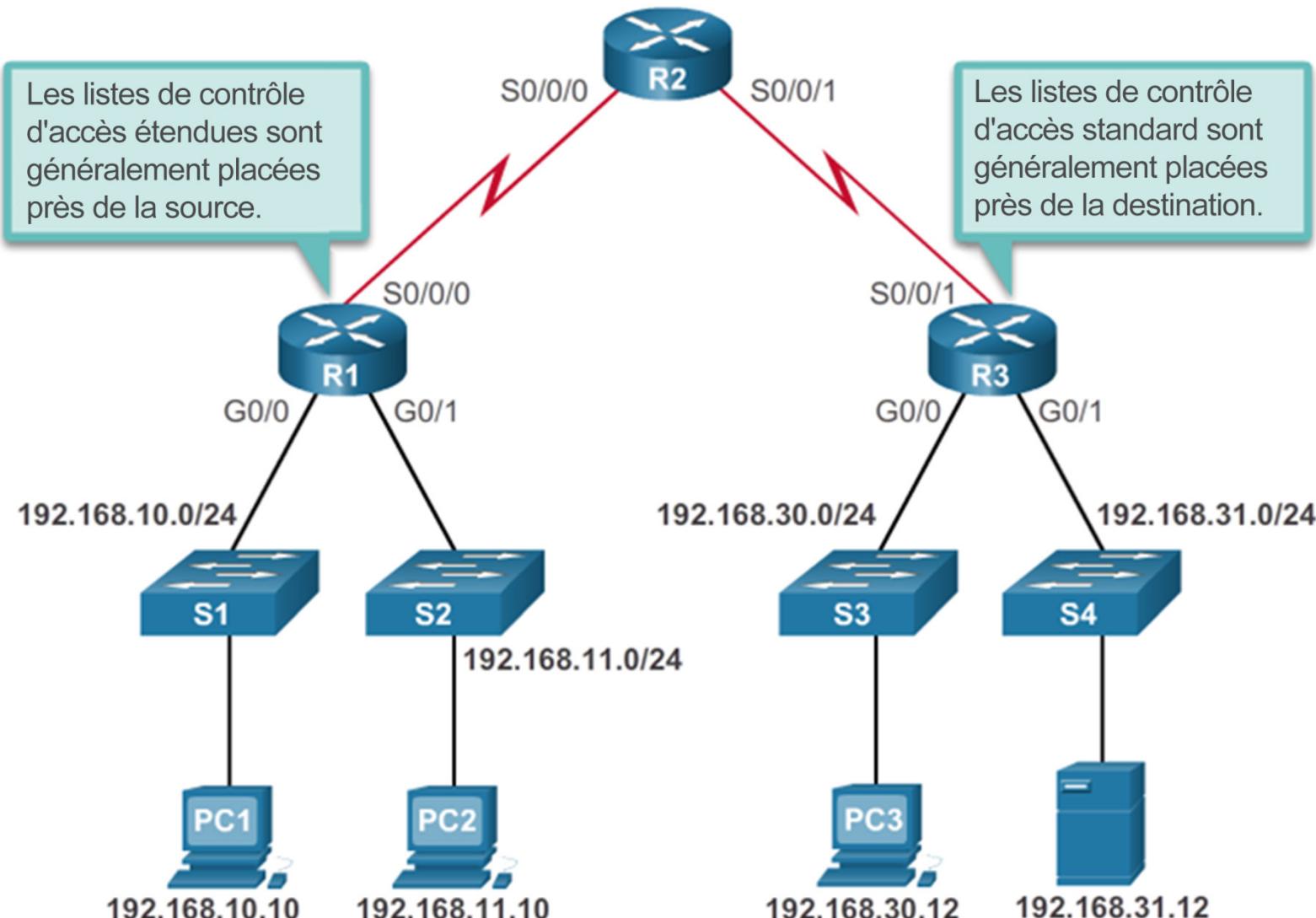
## Liste de contrôle d'accès nommée :

Attribution d'un nom à la liste de contrôle d'accès.

- 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.

# Types de listes de contrôle d'accès IPv4

# Où placer les listes de contrôle d'accès





## Types de listes de contrôle d'accès IPv4

# Où placer les listes de contrôle d'accès (suite...)

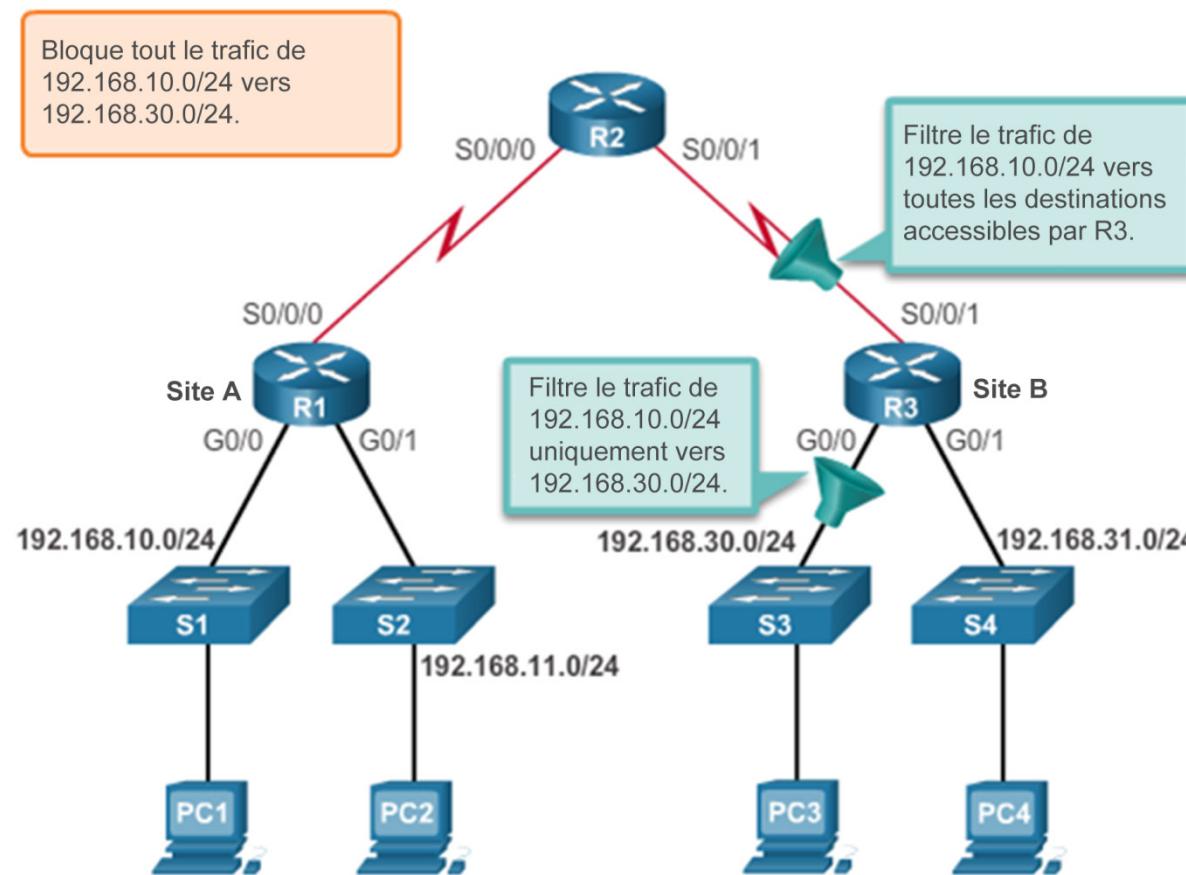
- Chaque liste de contrôle d'accès doit être placée là où elle aura le plus grand impact sur les performances. Règles de base :
  - Listes de contrôle d'accès étendues : placez les listes de contrôle d'accès étendues le plus près possible de la source du trafic à filtrer.
  - Listes de contrôle d'accès standard : étant donné que les listes de contrôle d'accès standard ne précisent pas les adresses de destination, placez-les le plus près possible de la destination.
  - L'emplacement de la liste de contrôle d'accès et donc son type peuvent aussi dépendre de l'étendue du contrôle de l'administrateur réseau, de la bande passante des réseaux concernés et de la facilité de configuration.



# Types de listes de contrôle d'accès IPv4

## Exemple de positionnement d'une liste de contrôle d'accès standard

- L'administrateur souhaite empêcher le trafic provenant du réseau 192.168.10.0/24 d'atteindre le réseau 192.168.30.0/24.

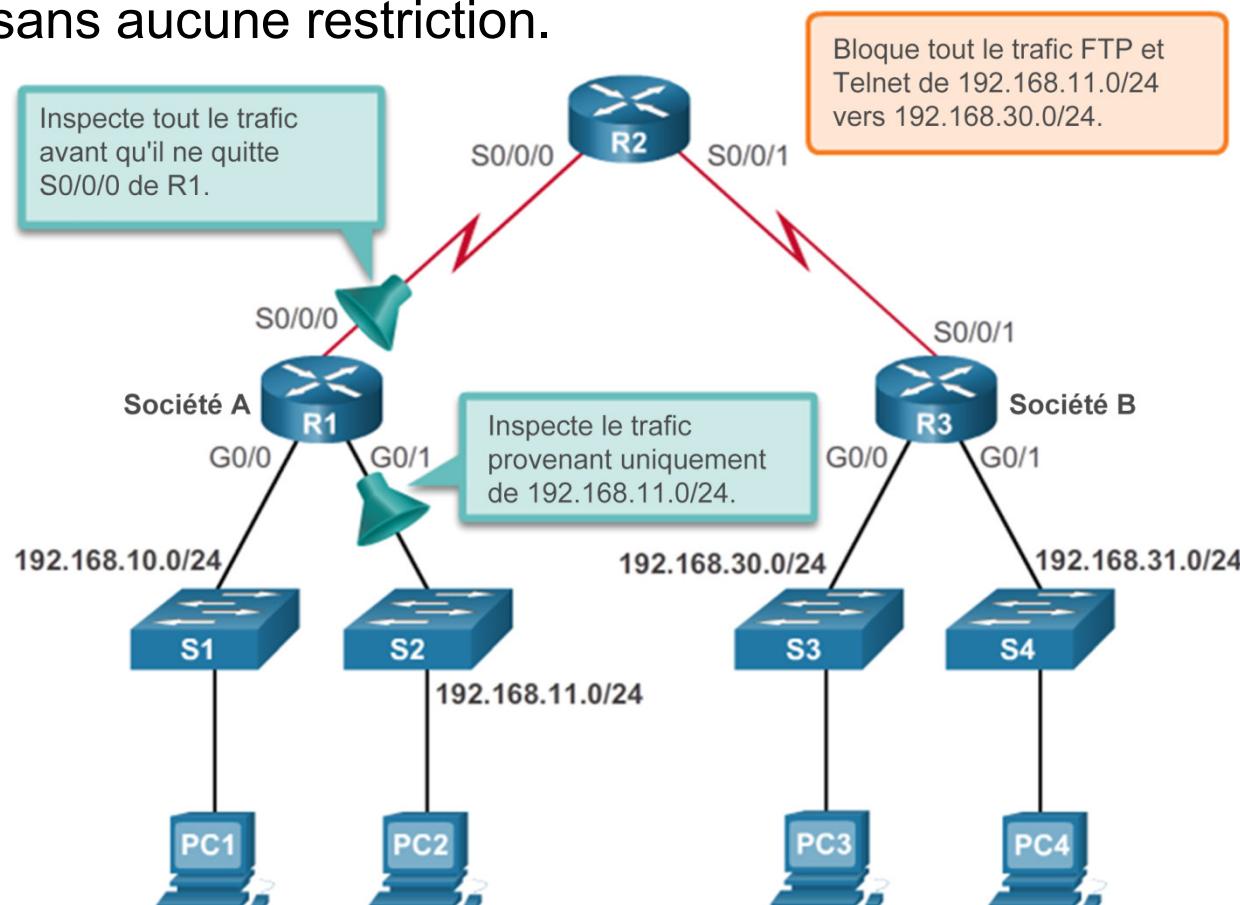




# Types de listes de contrôle d'accès IPv4

## Exemple de positionnement d'une liste de contrôle d'accès étendue

- L'administrateur souhaite refuser l'accès du trafic Telnet et FTP provenant du réseau 192.168.11.0/24 au réseau 192.168.30.0/24 de la société B. Le reste du trafic provenant du réseau .11 doit être autorisé à quitter la société A sans aucune restriction.





## Configuration d'une liste de contrôle d'accès IPv4 standard

# Configurer une liste de contrôle d'accès IPv4 standard

- Router(config)# **access-list access-list-number { deny | permit | remark } source [ source-wildcard ] [ log ]**

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
R1# show access-lists
Standard IP access list 10
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line. End with
CTRL/Z.
R1(config)# no access-list 10
R1(config)# exit
R1# show access-lists
R1#
```

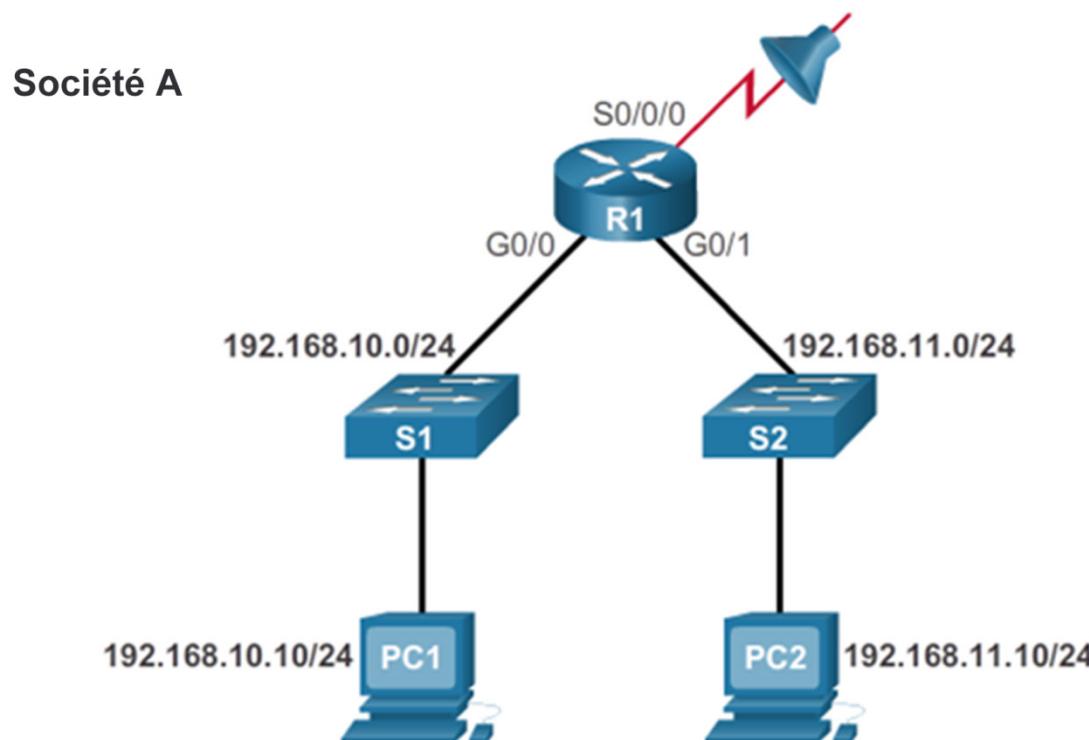
```
R1(config)# access-list 10 remark Permit hosts from the
192.168.10.0 LAN
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)# exit
R1# show running-config | include access-list 10
access-list 10 remark Permit hosts from the 192.168.10.0 LAN
access-list 10 permit 192.168.10.0 0.0.0.255
R1#
```



Configuration d'une liste de contrôle d'accès IPv4 standard

# Application d'une liste de contrôle d'accès IPv4 standard

Autoriser un sous-réseau spécifique



```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255  
R1(config)# interface s0/0/0  
R1(config-if)# ip access-group 1 out
```



# Configuration d'une liste de contrôle d'accès IPv4 standard

## Listes de contrôle d'accès IPv4 standard nommées

### Exemple de liste de contrôle d'accès nommée

```
Router(config)# ip access-list [standard | extended] name
```

La chaîne du nom alphanumérique doit être unique et ne peut pas commencer par un nombre.

```
Router(config-std-nacl)# [permit | deny | remark] {source  
[source-wildcard]} [log]
```

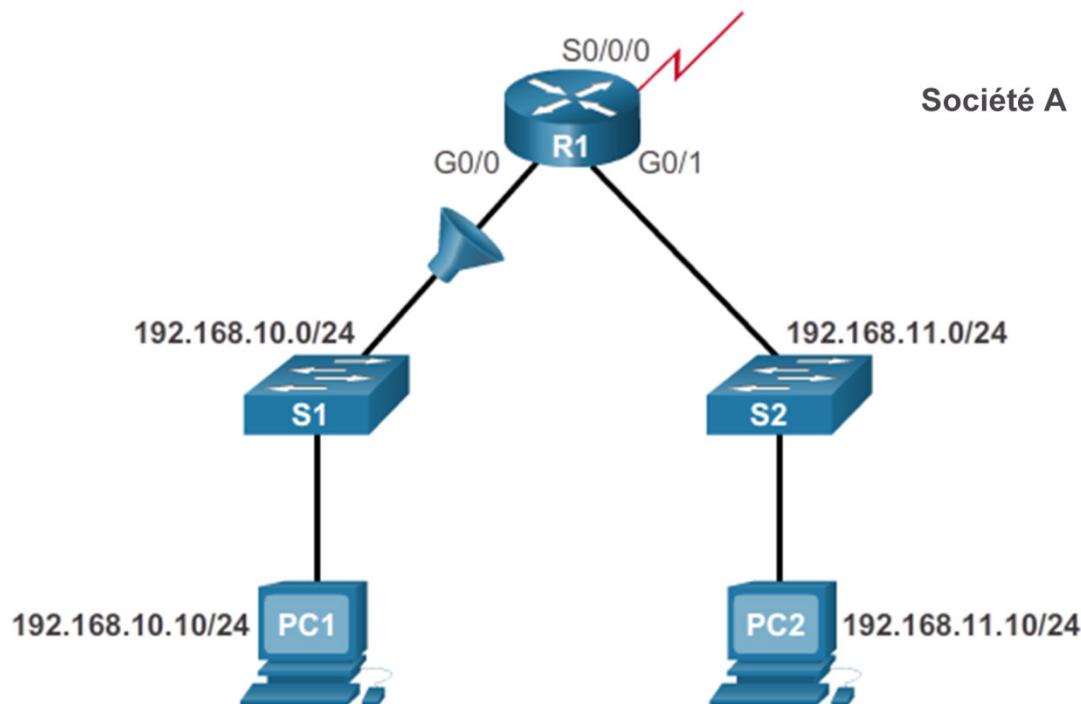
```
Router(config-if)# ip access-group name [in | out]
```

Active la liste de contrôle d'accès IP nommée sur une interface.



# Configuration d'une liste de contrôle d'accès IPv4 standard

## Listes de contrôle d'accès IPv4 standard nommées (suite...)



```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```



# Configuration d'une liste de contrôle d'accès IPv4 standard Vérification des listes de contrôle d'accès

```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
<output omitted>
  Outgoing access list is 1
    Inbound  access list is not set
<output omitted>

R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted>
  Outgoing access list is NO_ACCESS
    Inbound  access list is not set
<output omitted>
```

```
R1# show access-lists
Standard IP access list 1
  10 deny   192.168.10.10
  20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
  15 deny   192.168.11.11
  10 deny   192.168.11.10
  20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

## 4.2 Listes de contrôle d'accès IPv4 étendues





## Structure d'une liste de contrôle d'accès IPv4 étendue

# Listes de contrôle d'accès étendues

- Les listes de contrôle d'accès étendues sont plus répandues que les listes de contrôle d'accès standard, car elles fournissent un degré supérieur de contrôle.



**Les listes de contrôle d'accès étendues peuvent filtrer en fonction des paramètres suivants :**

- Adresse source
- Adresse de destination
- Protocole
- Numéro de port



# Structure d'une liste de contrôle d'accès IPv4 étendue

## Filtrage des ports et des services

- La possibilité de filtrer en fonction des protocoles et des numéros de port permet aux administrateurs réseau de créer des listes de contrôle d'accès étendues très précises.
- Une application peut être spécifiée soit par le numéro de port soit par le nom d'un port réservé.

Avec les numéros de port

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

Avec des mots-clés

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```



## Configuration des listes de contrôle d'accès IPv4 étendues

# Configuration des listes de contrôle d'accès étendues

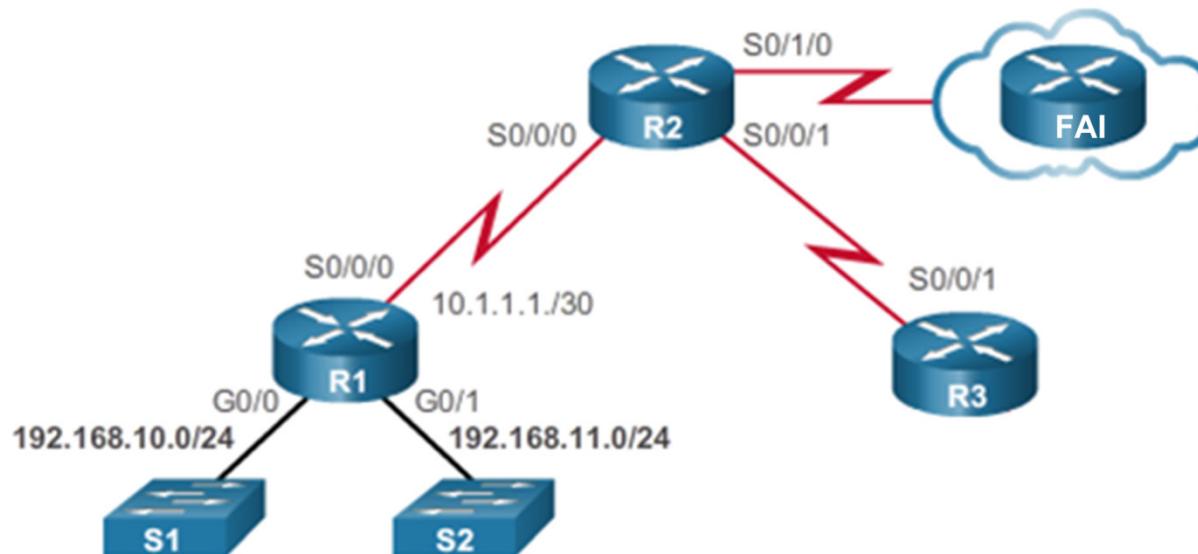
- Les procédures de configuration des listes de contrôle d'accès étendues sont les mêmes que pour les listes de contrôle d'accès standard. La liste de contrôle d'accès étendue est d'abord configurée, puis elle est activée sur une interface. La syntaxe et les paramètres de commande sont plus complexes, car ils prennent en charge des fonctions supplémentaires fournies par les listes de contrôle d'accès étendues.

```
access-list access-list-number {deny | permit | remark} protocol  
{source source-wildcard} [operator port [port-number or name]]  
{destination destination-wildcard} [operator port [port-number or  
name]]
```



# Configuration des listes de contrôle d'accès IPv4 étendues

## Configuration des listes de contrôle d'accès étendues (suite...)



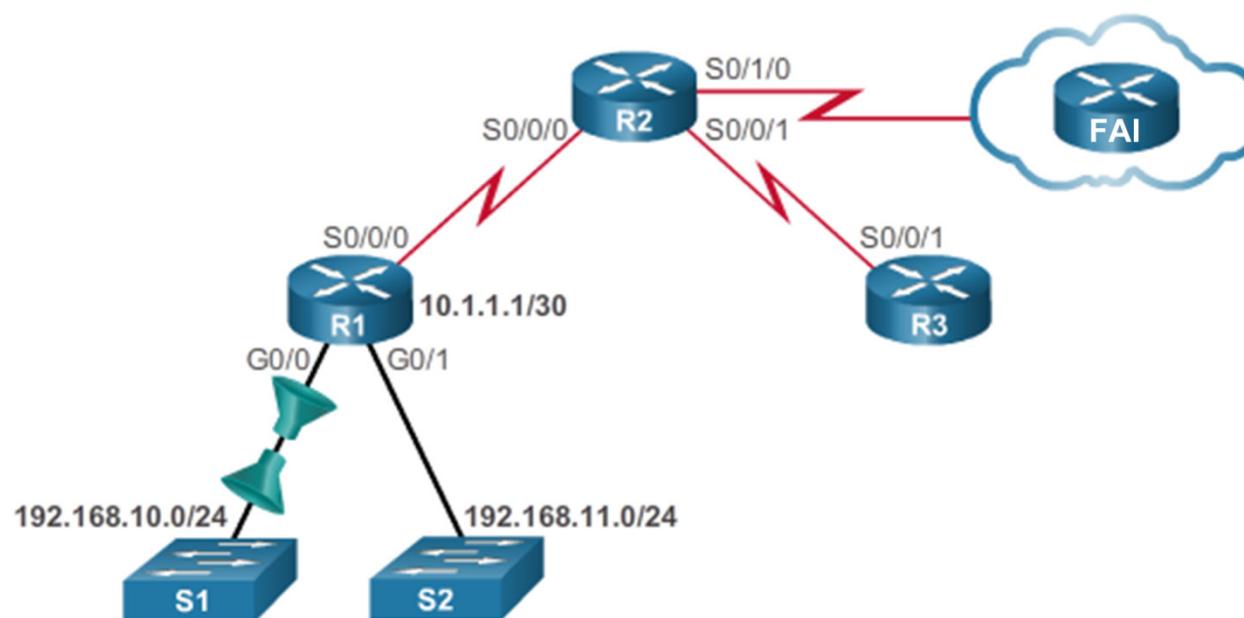
```
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# access-list 104 permit tcp any 192.168.10.0 0.0.0.255
                           established
```

- La liste de contrôle d'accès 103 autorise les requêtes vers les ports 80 et 443.
- La liste de contrôle d'accès 104 autorise les réponses HTTP et HTTPS établies.



# Configuration des listes de contrôle d'accès IPv4 étendues

## Application de listes de contrôle d'accès étendues aux interfaces

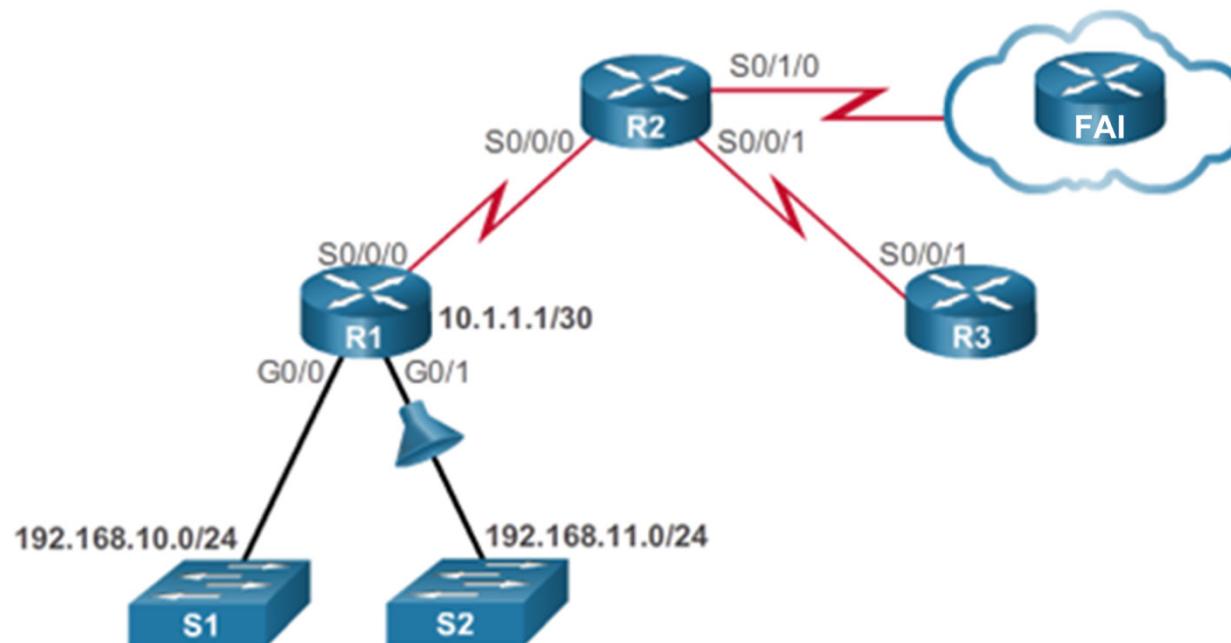


```
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)# interface g0/0
R1(config-if)# ip access-group 103 in
R1(config-if)# ip access-group 104 out
```



# Configuration des listes de contrôle d'accès IPv4 étendues

## Filtrage du trafic à l'aide de listes de contrôle d'accès étendues

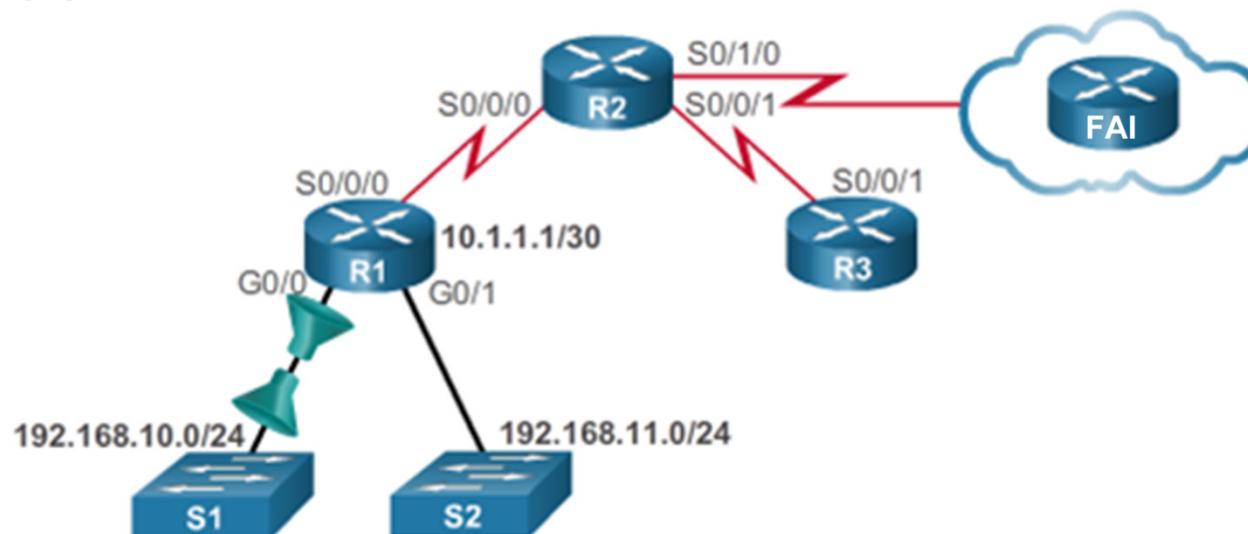


```
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255  
192.168.10.0 0.0.0.255 eq ftp  
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255  
192.168.10.0 0.0.0.255 eq ftp-data  
R1(config)# access-list 101 permit ip any any  
R1(config)# interface g0/1  
R1(config-if)# ip access-group 101 in
```



# Configuration des listes de contrôle d'accès IPv4 étendues

## Création de listes de contrôle d'accès étendues nommées



```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
```



# Configuration des listes de contrôle d'accès IPv4 étendues

## Vérification des listes de contrôle d'accès étendues

```
R1#show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    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
R1#
R1#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted for brevity>
  Outgoing access list is BROWSING
  Inbound   access list is SURFING
<output omitted for brevity>
```



## Configuration des listes de contrôle d'accès IPv4 étendues

# Modification des listes de contrôle d'accès étendues

- La modification d'une liste de contrôle d'accès étendue peut être effectuée de la même manière qu'avec une liste standard. Une liste de contrôle d'accès étendue peut être modifiée comme suit :
  - Méthode 1 : éditeur de texte
    - La liste de contrôle d'accès est copiée et collée dans l'éditeur de texte où les modifications sont effectuées. Il faut ensuite supprimer la liste d'accès actuelle à l'aide de la commande **no access-list**. Une fois modifiée, elle est à nouveau collée dans la configuration.
  - Méthode 2 : numéros d'ordre
    - Des numéros d'ordre peuvent être utilisés pour supprimer ou insérer une instruction de liste de contrôle d'accès.



# Configuration des listes de contrôle d'accès IPv4 étendues

## Modification des listes de contrôle d'accès étendues (suite...)

- Modification d'une liste de contrôle d'accès étendue via des numéros d'ordre :

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.11.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1# configure terminal
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# no 10
R1(config-ext-nacl)# 10 permit tcp 192.168.10.0 0.0.0.255 any eq
www
R1(config-ext-nacl)# end
R1#
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    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
```

Devrait être  
192.168.10.0.

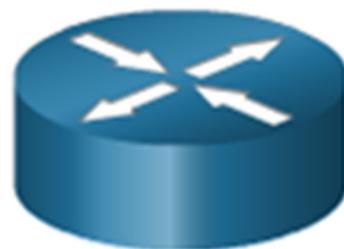
## 4.3 Listes de contrôle d'accès IPv6





## Création d'une liste de contrôle d'accès IPv6

# Types de listes de contrôle d'accès IPv6



### Listes de contrôle d'accès IPv4

- Standard
  - Numérotées
  - Nommées
- Étendues
  - Numérotées
  - Nommées

### Listes de contrôle d'accès IPv6

- Nommées uniquement
- Fonctionnent comme les listes de contrôle d'accès ACL IPv4 étendues



## Création d'une liste de contrôle d'accès IPv6

# Comparaison des listes de contrôle d'accès IPv4 et IPv6

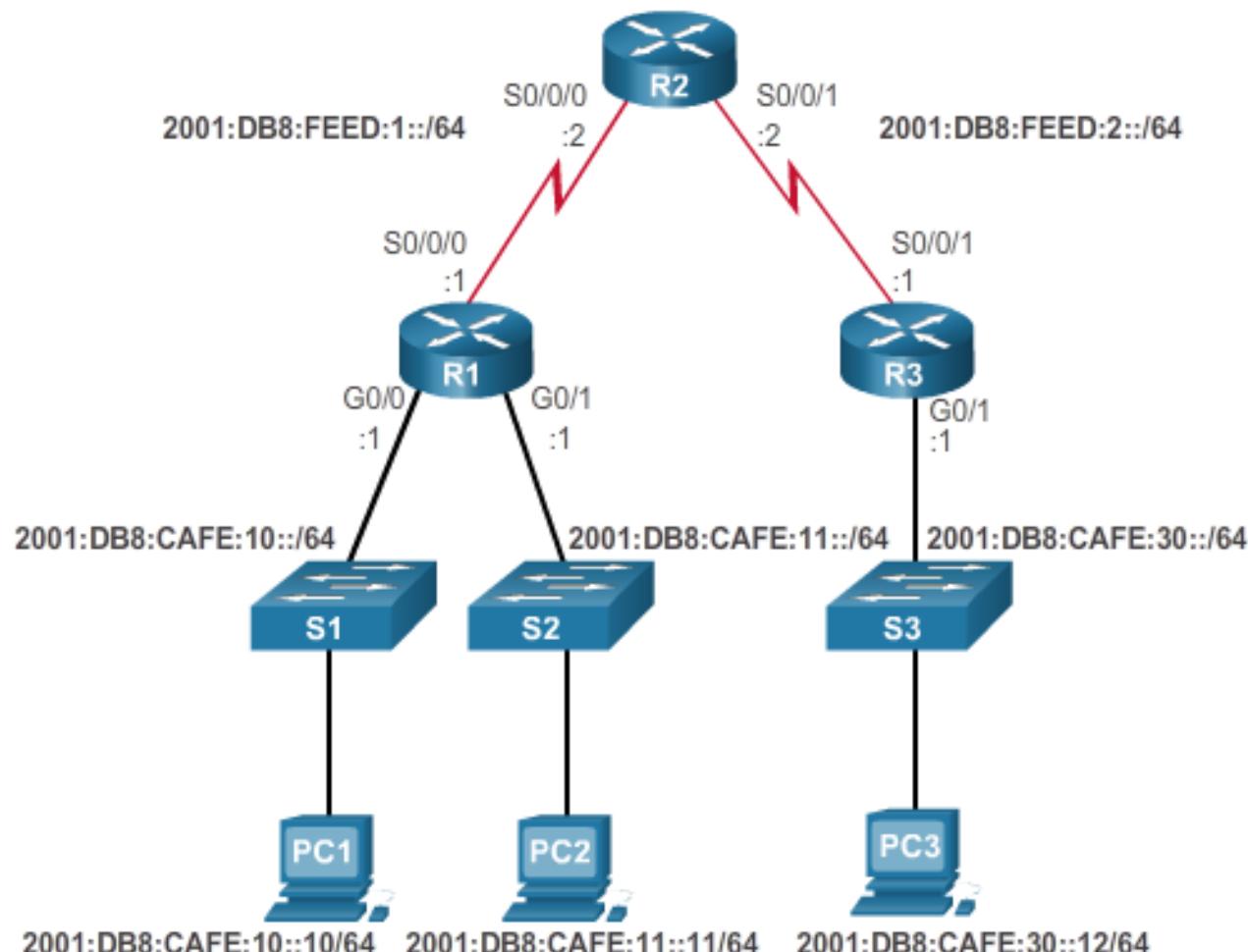
Bien que les listes de contrôle d'accès IPv4 et IPv6 soient très similaires, il existe trois différences entre elles.

- Application d'une liste de contrôle d'accès IPv6
  - IPv6 utilise la commande **ipv6 traffic-filter** pour exécuter la même fonction pour les interfaces IPv6.
- Aucun masque générique
  - La longueur de préfixe est utilisée pour indiquer dans quelle mesure l'adresse IPv6 source ou de destination doit correspondre.
- Instructions supplémentaires par défaut
  - **permit icmp any any nd-na**
  - **permit icmp any any nd-ns**



# Configuration de listes de contrôle d'accès IPv6

# Configuration de la topologie IPv6





## Configuration de listes de contrôle d'accès IPv6

# Configuration de listes de contrôle d'accès IPv6

La configuration d'une liste de contrôle d'accès IPv6 s'effectue en trois étapes :

1. À partir du mode de configuration global, utilisez la commande **ipv6 access-list nom** pour créer une liste de contrôle d'accès IPv6.
2. En mode de configuration des listes de contrôle d'accès nommées, utilisez les instructions **permit** ou **deny** afin de spécifier une ou plusieurs conditions pour déterminer si un paquet est transféré ou abandonné.
3. Retournez en mode d'exécution privilégié.

```
R1(config)# ipv6 access-list access-list-name
R1(config-ipv6-acl)# deny | permit protocol {source-ipv6-
prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/prefix-length | any |
host destination-ipv6-address} [operator [port-number]]
```



## Configuration de listes de contrôle d'accès IPv6

# Configuration de listes de contrôle d'accès IPv6 - Suite...

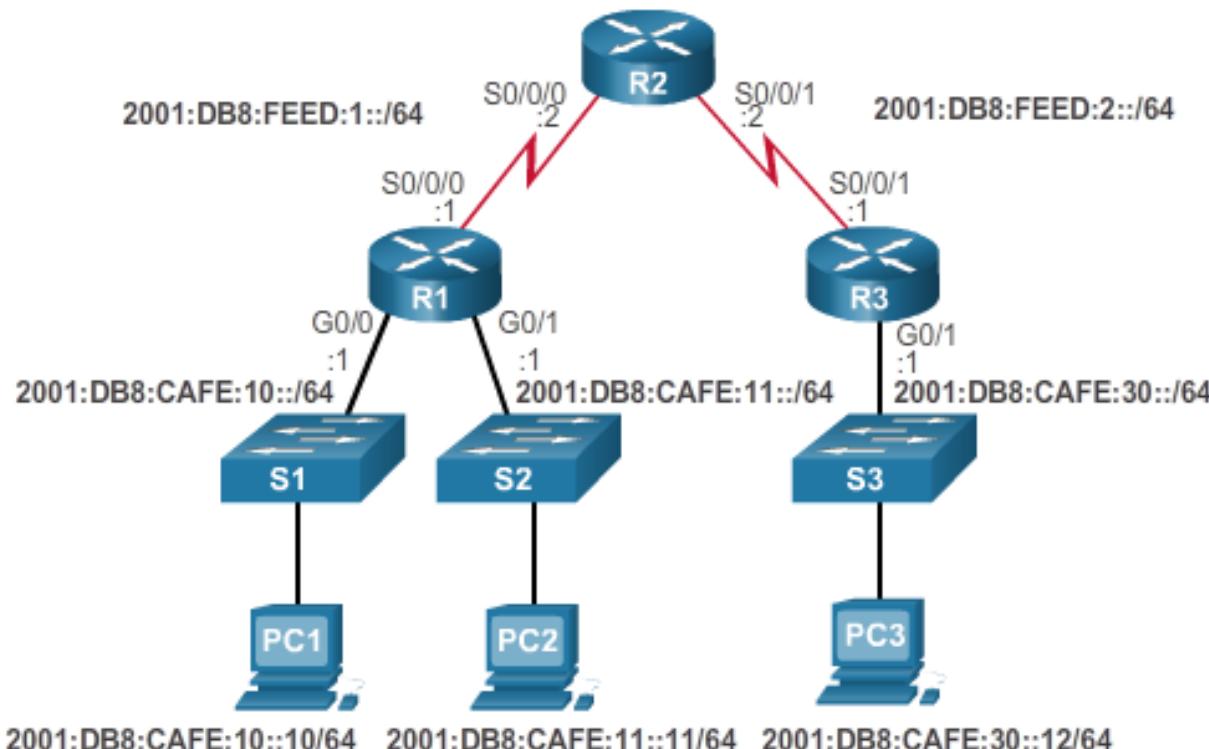
- Cette liste de contrôle d'accès IPv6 fait ce qui suit :
  - La première instruction nomme la liste d'accès IPv6 NO-R3-LAN-ACCESS.
  - La seconde instruction refuse tous les paquets IPv6 de 2001:DB8:CAFE:30::/64 destinés à un réseau IPv6.
  - La troisième instruction autorise tous les autres paquets IPv6.

```
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
R1(config-ipv6-acl)# end
R1#
```



## Configuration de listes de contrôle d'accès IPv6

# Configuration de listes de contrôle d'accès IPv6 - Suite...

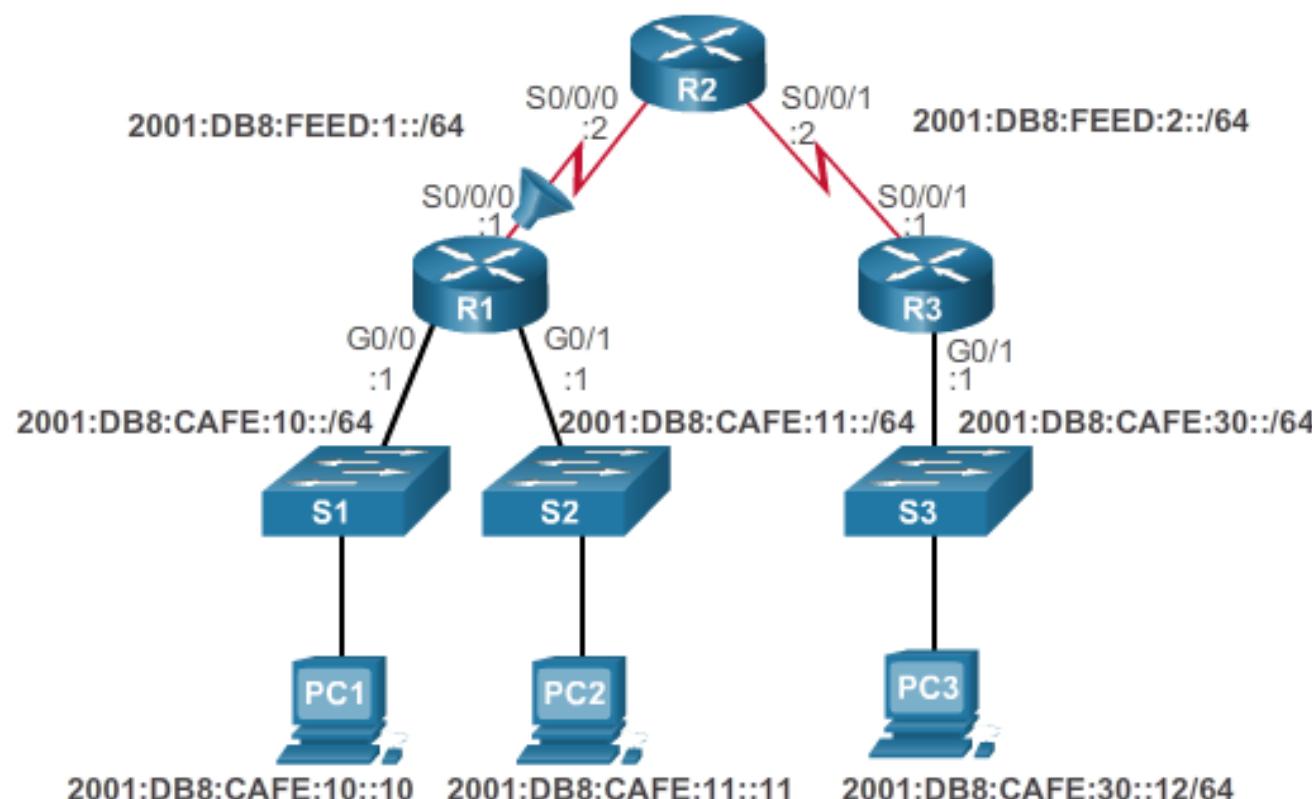


```
R1(config) # ipv6 access-list NO-R3-LAN-ACCESS
R1(config-ipv6-acl) # deny ipv6 2001:db8:cafe:30::/64 any
R1(config-ipv6-acl) # permit ipv6 any any
R1(config-ipv6-acl) # end
R1#
```



## Configuration de listes de contrôle d'accès IPv6

# Application d'une liste de contrôle d'accès IPv6 à une interface

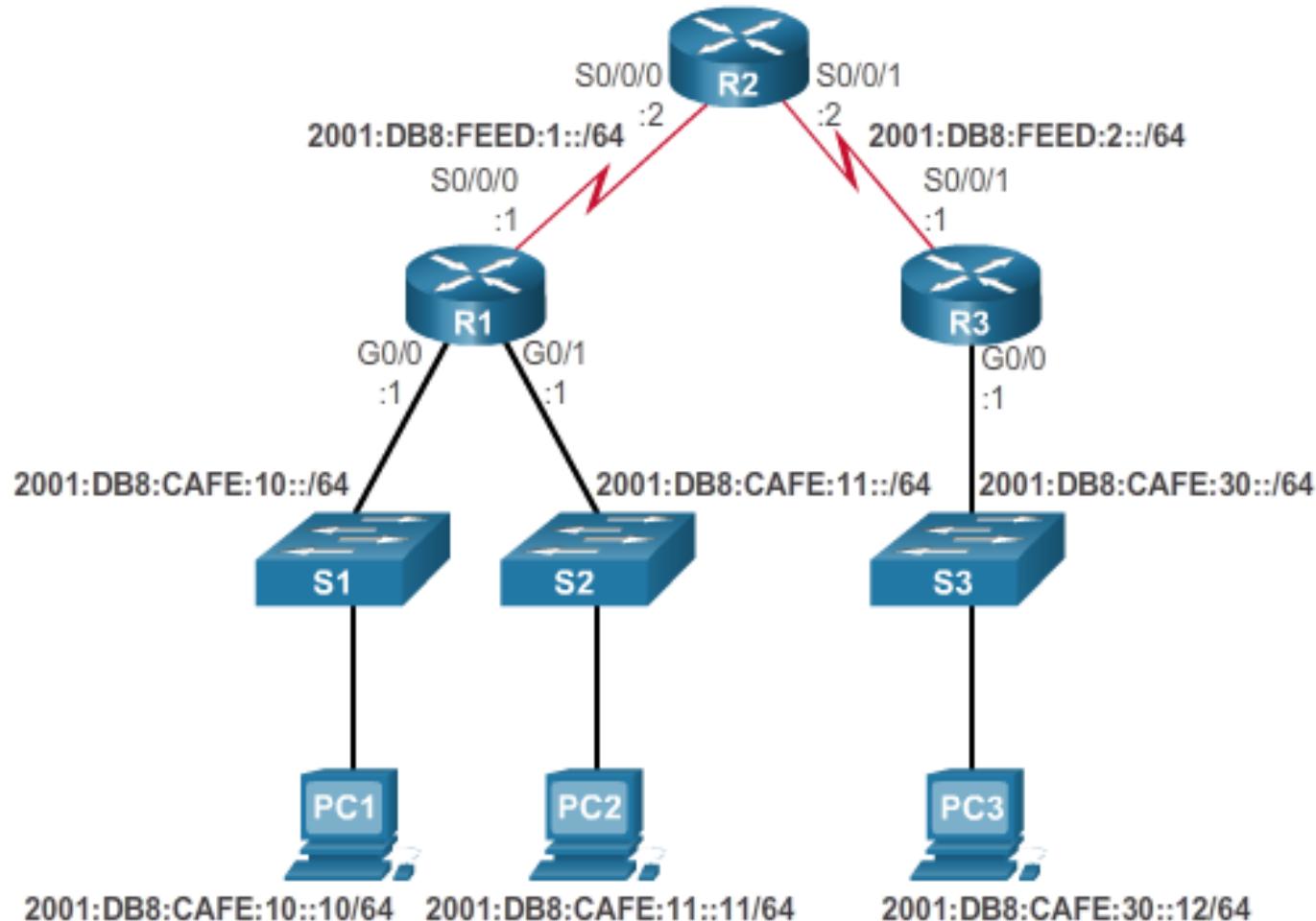


```
R1(config)# interface s0/0/0
R1(config-if)# ipv6 traffic-filter NO-R3-LAN-ACCESS in
```



## Configuration de listes de contrôle d'accès IPv6

# Exemples de listes de contrôle d'accès IPv6





## Configuration de listes de contrôle d'accès IPv6

# Exemples de listes de contrôle d'accès IPv6 - Suite...

- Le routeur R1 est configuré avec une liste d'accès IPv6 pour refuser le trafic FTP adressé à 2001:DB8:CAFE:11::/64. Les ports de données FTP (port 20) et de commande FTP (port 21) doivent être bloqués.
- Du fait que le filtre est appliqué en entrée sur l'interface G0/0 de R1, seul le trafic du réseau 2001:DB8:CAFE:10::/64 sera refusé.

```
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)# deny tcp any 2001:db8:cafe:11::/64 eq ftp-data
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
R1(config-if)#

```



# Configuration de listes de contrôle d'accès IPv6

## Exemples de listes de contrôle d'accès IPv6 - Suite...

1. Les deux premières instructions d'autorisation permettent l'accès, à partir de n'importe quel appareil, 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. L'accès Telnet de PC3, à l'adresse 2001:DB8:CAFE:30::12, à PC2, dont l'adresse IPv6 est 2001:DB8:CAFE:11::11, est autorisé.

```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# remark Permit access only HTTP and HTTPS to Network 10
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 80 ] 1
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 443 ] 1
R3(config-ipv6-acl)# remark Deny all other traffic to Network 10
R3(config-ipv6-acl)# deny ipv6 any 2001:db8:cafe:10::/64 2
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 3
R3(config-ipv6-acl)# remark Deny telnet access to PC2 for all other devices
R3(config-ipv6-acl)# deny tcp any host 2001:db8:cafe:11::11 eq 23 4
R3(config-ipv6-acl)# remark Permit access to everything else
R3(config-ipv6-acl)# permit ipv6 any any 5
R3(config-ipv6-acl)# exit
R3(config)# interface g0/0
R3(config-if)# ipv6 traffic-filter RESTRICTED-ACCESS in 6
R3(config-if)#

```



# Configuration de listes de contrôle d'accès IPv6

## Exemples de listes de contrôle d'accès IPv6 - Suite...

4. L'accès Telnet à PC2 de tous les autres appareils est refusé.
5. Le reste du trafic IPv6 vers toutes les autres destinations est autorisé.
6. La liste d'accès IPv6 est appliquée à l'interface G0/0 dans la direction entrante, de sorte que seul le réseau 2001:DB8:CAFE:30::/64 est affecté.

```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# remark Permit access only HTTP and HTTPS to Network 10
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 80 ] 1
R3(config-ipv6-acl)# permit tcp any host 2001:db8:cafe:10::10 eq 443
R3(config-ipv6-acl)# remark Deny all other traffic to Network 10
R3(config-ipv6-acl)# deny ipv6 any 2001:db8:cafe:10::/64 2
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 3
R3(config-ipv6-acl)# remark Deny telnet access to PC2 for all other devices
R3(config-ipv6-acl)# deny tcp any host 2001:db8:cafe:11::11 eq 23 4
R3(config-ipv6-acl)# remark Permit access to everything else
R3(config-ipv6-acl)# permit ipv6 any any 5
R3(config-ipv6-acl)# exit
R3(config)# interface g0/0
R3(config-if)# ipv6 traffic-filter RESTRICTED-ACCESS in 6
R3(config-if)#

```



## Configuration de listes de contrôle d'accès IPv6

# Vérification des listes de contrôle d'accès IPv6

```
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
<output omitted>
```



## Configuration de listes de contrôle d'accès IPv6

# Vérification des listes de contrôle d'accès IPv6 - Suite...

```
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
R3#
```



## Configuration de listes de contrôle d'accès IPv6

# Vérification des listes de contrôle d'accès IPv6 - Suite...

```
R3# show running-config
<output omitted>
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
```

## 4.4 Dépannage des listes de contrôle d'accès

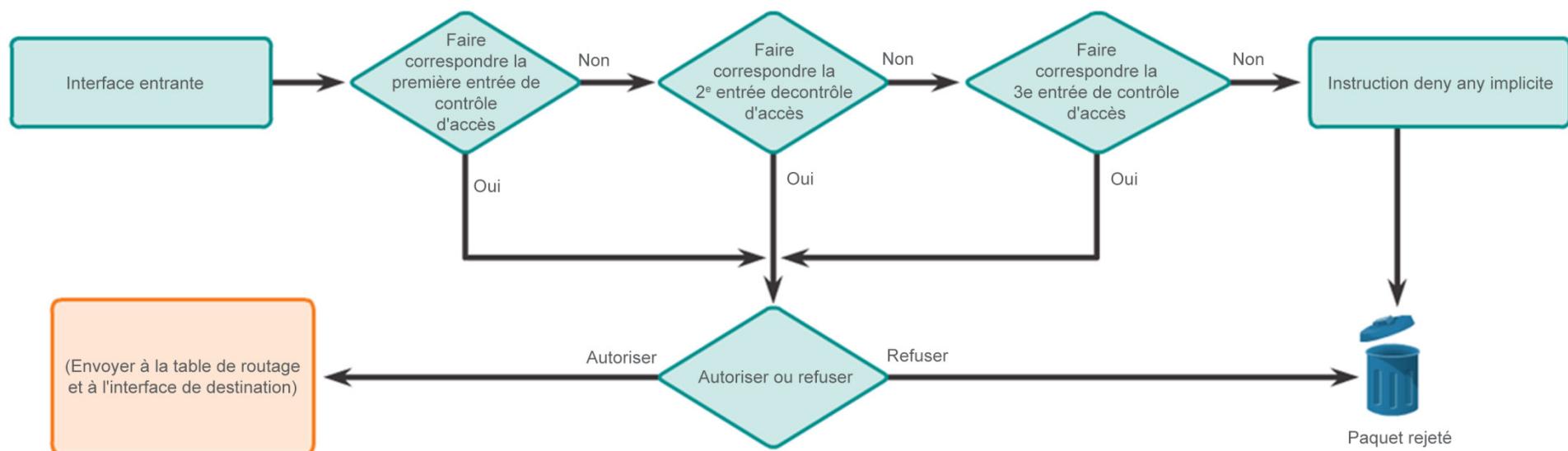




# Traitement des paquets avec les listes de contrôle d'accès

# Logique des listes de contrôle d'accès entrantes et sortantes

Processus des listes de contrôle  
d'accès entrantes

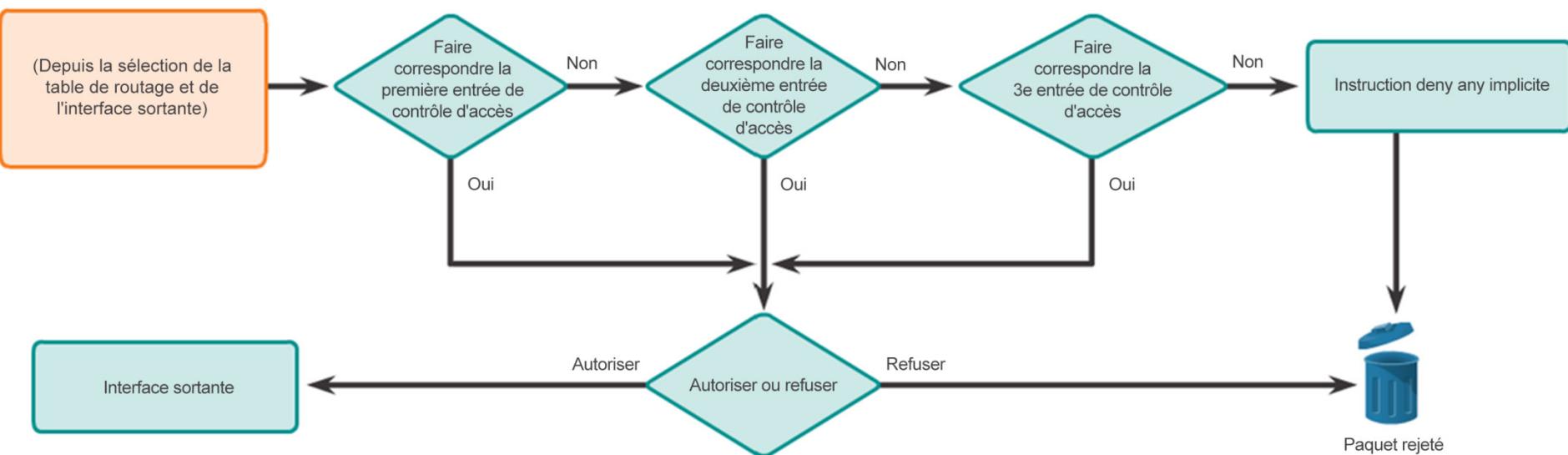




# Traitement des paquets avec les listes de contrôle d'accès

# Logique des listes de contrôle d'accès entrantes et sortantes

Processus des listes de contrôle d'accès sortantes





## Traitement des paquets avec les listes de contrôle d'accès

# Opérations logiques des listes de contrôle d'accès

- À l'entrée d'une trame dans l'interface, le routeur vérifie si l'adresse de couche 2 de destination correspond à la sienne ou s'il s'agit d'une trame de diffusion.
- Si l'adresse de la trame est acceptée, les informations sur la trame sont éliminées et le routeur recherche une liste de contrôle d'accès sur l'interface d'entrée.
- Le cas échéant, le paquet est vérifié pour déceler des correspondances avec les instructions de la liste.
- Si le paquet correspond à une instruction, il est autorisé ou refusé.
- Si le paquet est accepté, il est ensuite comparé aux entrées de la table de routage afin de déterminer l'interface de destination.
- S'il existe une entrée de table de routage pour la destination, le paquet est alors transmis à l'interface sortante. Dans le cas contraire, le paquet est abandonné.
- Le routeur vérifie ensuite si l'interface sortante possède une liste de contrôle d'accès. Le cas échéant, le paquet est vérifié pour déceler des correspondances avec les instructions de la liste. Si le paquet correspond à une instruction, il est autorisé ou refusé.
- En l'absence d'une liste de contrôle d'accès ou si le paquet est autorisé, ce dernier est encapsulé dans le nouveau protocole de couche 2 et acheminé par l'interface jusqu'au périphérique suivant.

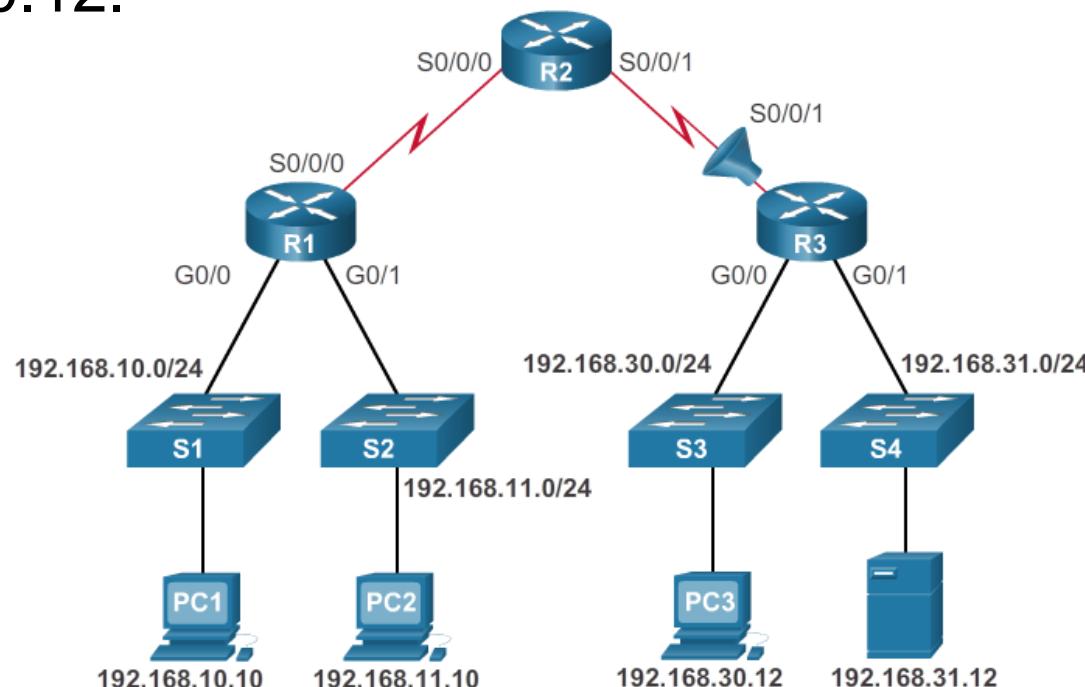


## Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès

## IPv4 - Exemple 1

- L'hôte 192.168.10.10 n'a pas de connectivité Telnet avec 192.168.30.12.



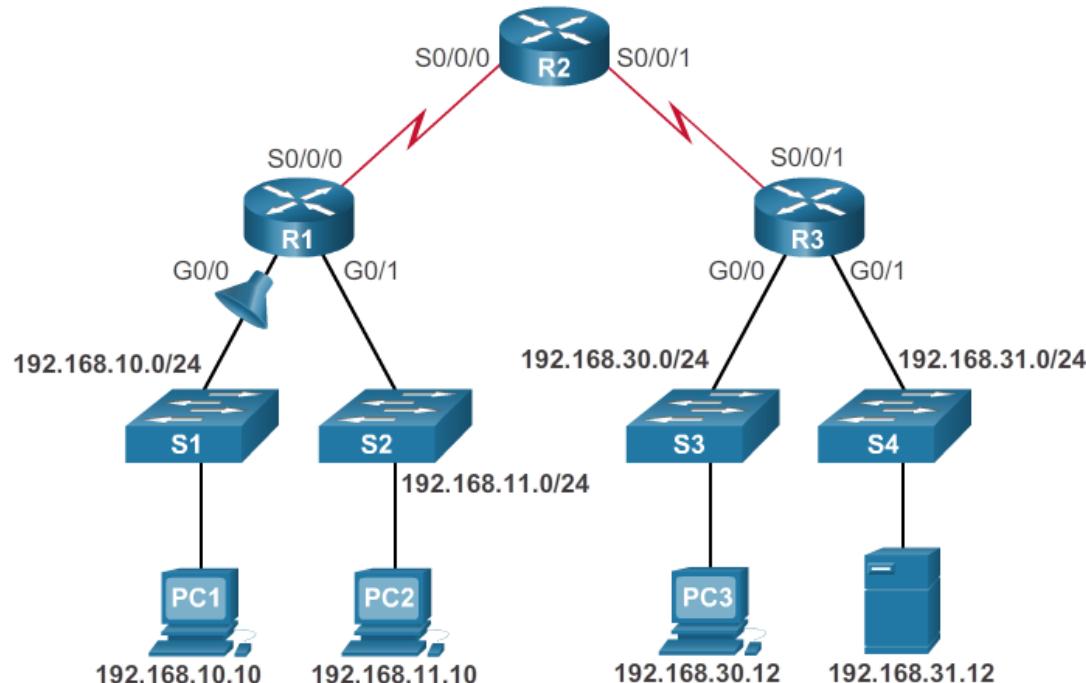
```
R3# show access-lists
Extended IP access list 110
 10 deny tcp 192.168.10.0 0.0.0.255 any (12 match(es))
 20 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
 30 permit ip any any
```



## Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès IPv4 - Exemple 2

- Le réseau 192.168.10.0/24 ne peut pas utiliser TFTP pour se connecter au réseau 192.168.30.0/24.



```
R1# show access-lists 120
Extended IP access list 120
  10 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
  20 deny tcp 192.168.10.0 0.0.0.255 host 192.168.31.12 eq smtp
  30 permit tcp any any
```

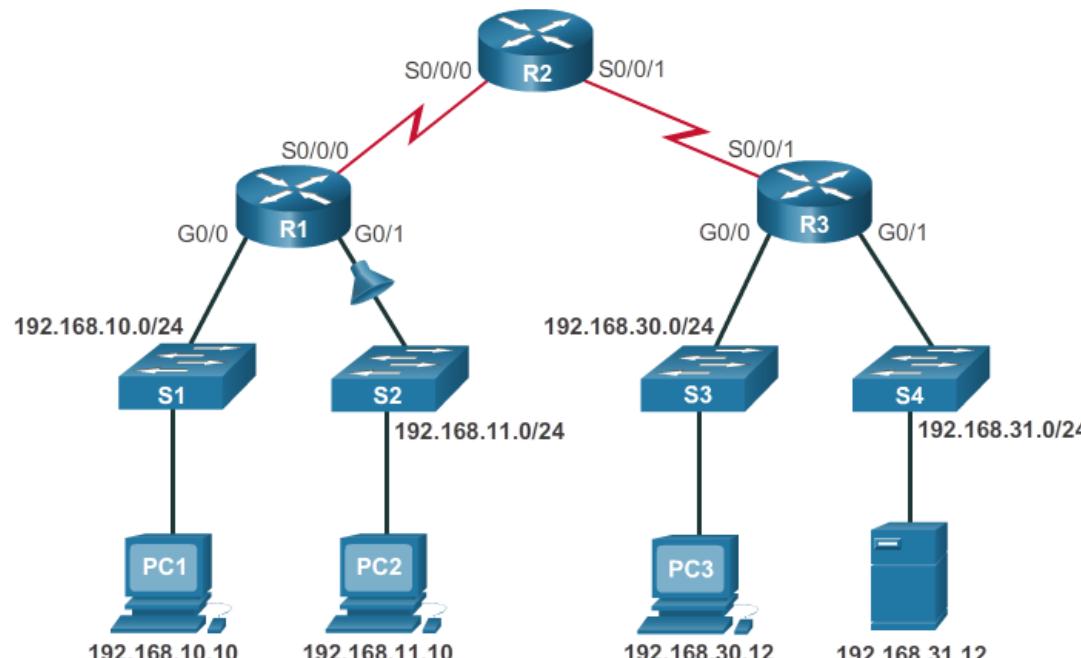


## Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès IPv4 - Exemple 3

- Le réseau 192.168.11.0/24 peut utiliser Telnet pour se connecter à 192.168.30.0/24, mais cette connexion ne doit pas être autorisée.

```
R1# show access-lists 130
Extended IP access list 130
  10 deny tcp any eq telnet any
  20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
  30 permit tcp any any (12 match(es))
```



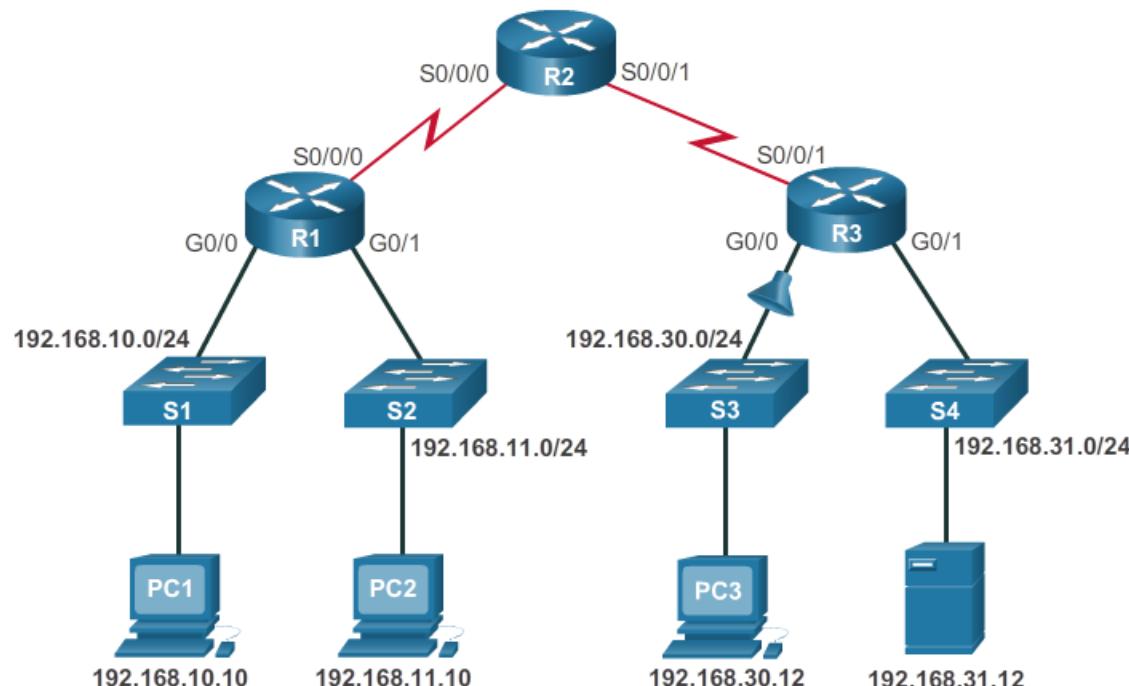


## Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès IPv4 - Exemple 4

- L'hôte 192.168.30.12 peut utiliser Telnet pour se connecter à 192.168.31.12, mais cette connexion ne doit pas être autorisée.

```
R3# show access-lists 140
Extended IP access list 140
  10 deny tcp host 192.168.30.1 any eq telnet
  20 permit ip any any (5 match(es))
```



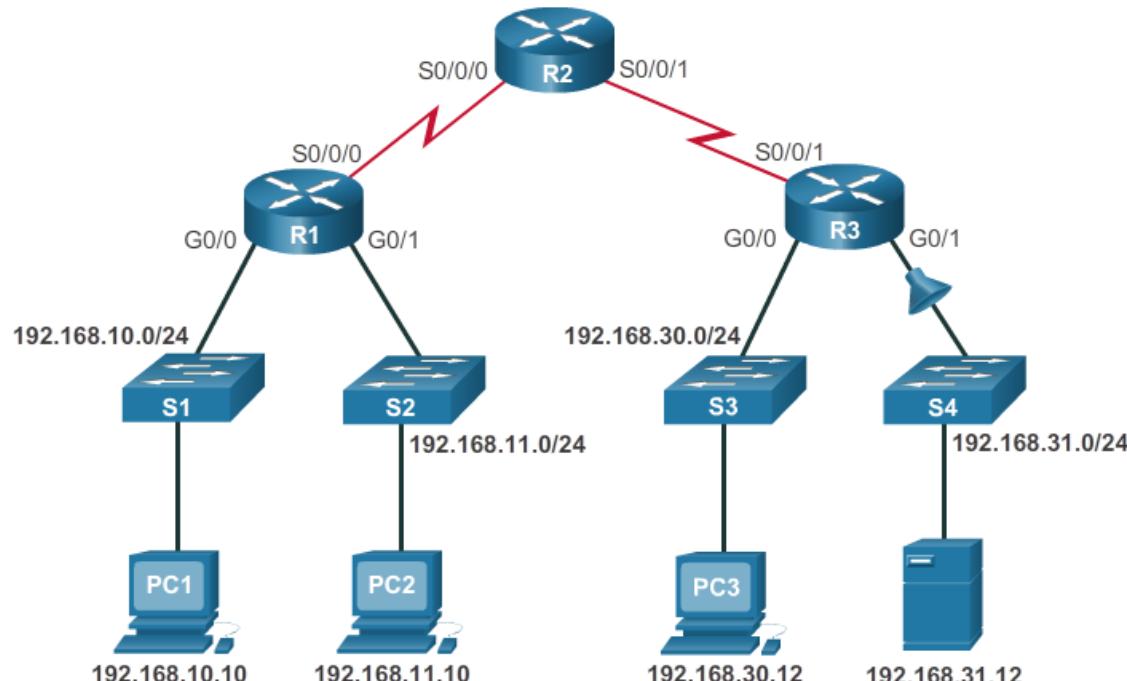


## Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès IPv4 - Exemple 5

- L'hôte 192.168.30.12 peut utiliser Telnet pour se connecter à 192.168.31.12, mais cette connexion ne doit pas être autorisée.

```
R2# show access-lists 150
Extended IP access list 150
  10 deny tcp any host 192.168.31.12 eq telnet
  20 permit ip any any
```

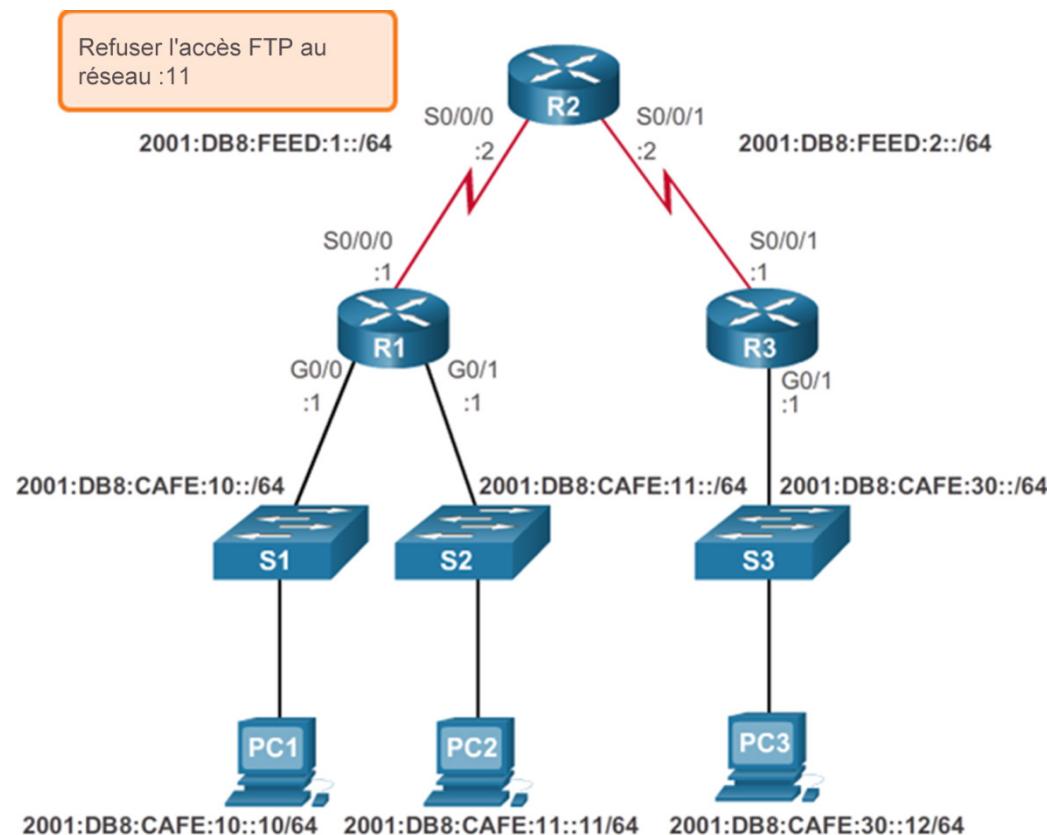




## Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès IPv6 - Exemple 1

- R1 est configuré avec une liste de contrôle d'accès IPv6 pour interdire l'accès FTP du réseau :10 au réseau :11, mais PC1 peut toujours se connecter au serveur FTP qui s'exécute sur PC2.





# Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès

## IPv6 - Exemple 1 - Suite...

Vérifiez la configuration et l'application de la liste de contrôle d'accès IPv6

```
R1# show ipv6 access-list
IPv6 access list NO-FTP-TO-11
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp sequence 10
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp-data sequence 20
    permit ipv6 any any (11 matches) sequence 30
R1# show running-config | begin interface G
interface GigabitEthernet0/0
    no ip address
    ipv6 traffic-filter NO-FTP-TO-11 out
    duplex auto
    speed auto
    ipv6 address FE80::1 link-local
    ipv6 address 2001:DB8:1:10::1/64
    ipv6 eigrp 1
<output omitted>
R1#
```



Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès

## IPv6 - Exemple 1 - Suite...

Corrigez et vérifiez la liste de contrôle d'accès IPv6

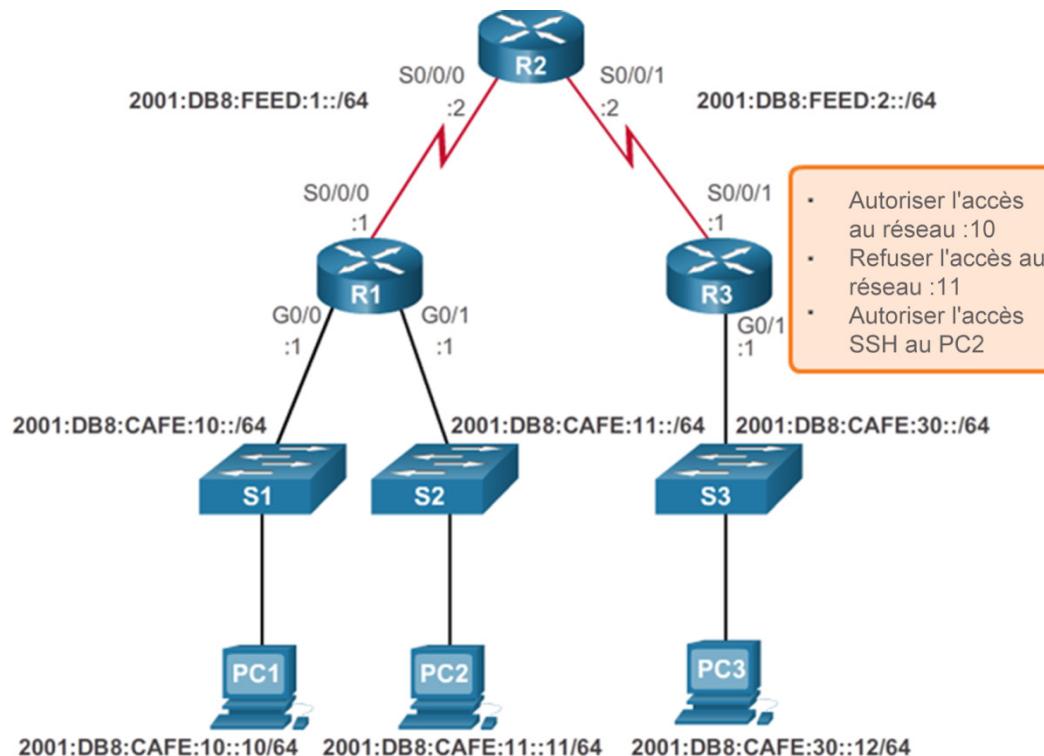
```
R1(config)# interface g0/0
R1(config-if)# no ipv6 traffic-filter NO-FTP-TO-11 out
R1(config-if)# ipv6 traffic-filter NO-FTP-TO-11 in
R1(config-if)# end
R1#
!PC1 attempts to access the FTP server again.
R1# show ipv6 access-list
IPv6 access list NO-FTP-TO-11
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp (37 matches) sequence 10
    deny tcp any 2001:DB8:CAFE:11::/64 eq ftp-data sequence 20
    permit ipv6 any any (11 matches) sequence 30
```



## Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès IPv6 - Exemple 2

- R3 est configuré avec la liste de contrôle d'accès IPv6 RESTRICTED-ACCESS qui doit appliquer la politique suivante pour le réseau local R3 :



- Cependant, après configuration de la liste de contrôle d'accès, PC3 ne peut atteindre ni le réseau 10, ni le réseau 11, et ne peut pas non plus accéder via SSH à l'hôte à l'adresse 2001:DB8:CAFE:11::11.



Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès

## IPv6 - Exemple 2 - Suite...

Vérifiez la configuration et l'application de la liste  
de contrôle d'accès IPv6

```
R3# show running-config | section interface GigabitEthernet0/0
interface GigabitEthernet0/0
    no ip address
    duplex auto
    speed auto
    ipv6 address FE80::3 link-local
    ipv6 address 2001:DB8:1:30::1/64
    ipv6 eigrp 1
    ipv6 traffic-filter RESTRICTED-ACCESS in

R3# show ipv6 access-list
IPv6 access list RESTRICTED-ACCESS
    permit ipv6 any host 2001:DB8:CAFE:10:: sequence 10
    deny ipv6 any 2001:DB8:CAFE:11::/64 sequence 20
    permit tcp any host 2001:DB8:CAFE:11::11 eq 22 sequence 30

R3#
```



Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès

## IPv6 - Exemple 2 - Suite...

```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# permit ipv6 any 2001:db8:cafe:10::/64 sequence 10
R3(config-ipv6-acl)# end
R3# show access-list
IPv6 access list RESTRICTED-ACCESS
    permit ipv6 any 2001:DB8:CAFE:10::/64 sequence 10
    deny ipv6 any 2001:DB8:CAFE:11::/64 sequence 20
    permit tcp any host 2001:DB8:CAFE:11::11 eq 22 sequence 30
R3#
```



Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès

## IPv6 - Exemple 2 - Suite...

Remplacez l'instruction Host de la liste de contrôle d'accès IPv6

```
R3(config)# ipv6 access-list RESTRICTED-ACCESS
R3(config-ipv6-acl)# no deny ipv6 any 2001:DB8:CAFE:11::/64
R3(config-ipv6-acl)# no permit tcp any host 2001:DB8:CAFE:11::11 eq 22
R3(config-ipv6-acl)# permit tcp any host 2001:DB8:CAFE:11::11 eq 22
R3(config-ipv6-acl)# deny ipv6 any 2001:DB8:CAFE:11::/64
R3(config-ipv6-acl)# end
R3# show access-list
IPv6 access list RESTRICTED-ACCESS
    permit ipv6 any 2001:DB8:CAFE:10::/64 sequence 10
    permit tcp any host 2001:DB8:CAFE:11::11 eq 22 sequence 20
    deny ipv6 any 2001:DB8:CAFE:11::/64 sequence 30
R3#
```

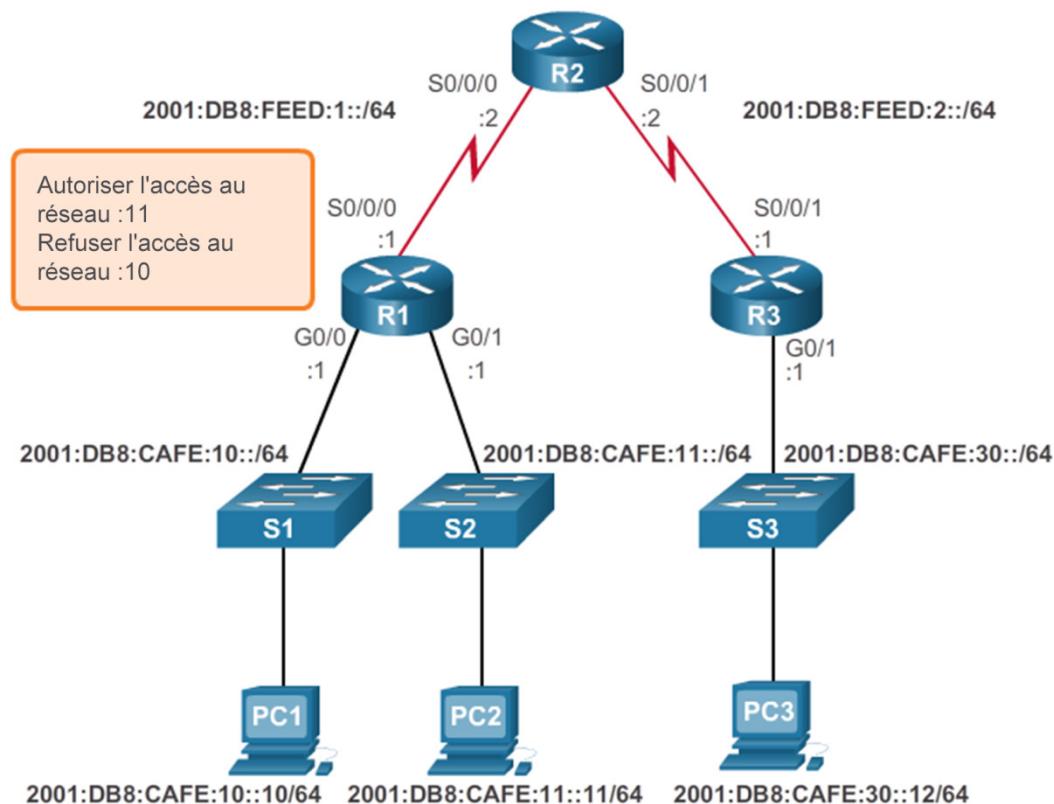


# Erreurs fréquentes liées aux listes de contrôle d'accès

## Dépannage des listes de contrôle d'accès

### IPv6 - Exemple 3

- R1 est configuré avec la liste de contrôle d'accès IPv6 DENY-ACCESS qui doit appliquer la politique suivante pour le réseau local R3 :



- Toutefois, une fois la liste de contrôle d'accès appliquée à l'interface, le réseau :10 est accessible depuis le réseau :30.



Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès

## IPv6 - Exemple 3 - Suite...

Vérifiez la configuration et l'application de la liste  
de contrôle d'accès IPv6

```
R1# show access-list
IPv6 access list DENY-ACCESS
    permit ipv6 any 2001:DB8:CAFE:11::/64 sequence 10
    deny ipv6 any 2001:DB8:CAFE:10::/64 sequence 20
R1# show running-config | section interface GigabitEthernet0/1
interface GigabitEthernet0/1
    no ip address
    duplex auto
    speed auto
    ipv6 address FE80::1 link-local
    ipv6 address 2001:DB8:CAFE:11::1/64
    ipv6 eigrp 1
    ipv6 traffic-filter DENY-ACCESS out
R1#
```



Erreurs fréquentes liées aux listes de contrôle d'accès

# Dépannage des listes de contrôle d'accès

## IPv6 - Exemple 3 - Suite...

Supprimez la liste de contrôle d'accès sur R1, puis configurez et appliquez la liste de contrôle d'accès sur R2

```
R1(config)# no ipv6 access-list DENY-ACCESS
R1(config)# interface g0/1
R1(config-if)# no ipv6 traffic-filter DENY-ACCESS out
R1(config-if)#
!-----
R3(config)# ipv6 access-list DENY-ACCESS
R3(config-ipv6-acl)# permit ipv6 any 2001:DB8:CAFE:11::/64
R3(config-ipv6-acl)# deny ipv6 any 2001:DB8:CAFE:10::/64
R3(config-ipv6-acl)# exit
R3(config)# interface g0/0
R3(config-if)# ipv6 traffic-filter DENY-ACCESS in
R3(config-if)#

```

## 4.5 Synthèse du chapitre





## Synthèse du chapitre

# Synthèse

- Par défaut un routeur ne filtre pas le trafic. Le trafic qui entre dans le routeur est routé uniquement en fonction des informations de la table de routage.
- Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus. La dernière instruction d'une liste de contrôle d'accès est toujours une instruction implicite **deny any** qui bloque tout le trafic. Pour éviter que l'instruction implicite **deny any** à la fin de la liste de contrôle d'accès ne bloque tout le trafic, vous pouvez ajouter l'instruction **permit ip any any**.
- Lorsque le trafic réseau traverse une interface configurée avec une liste de contrôle d'accès, le routeur compare les informations du paquet à chaque entrée, dans l'ordre séquentiel, pour déterminer si celui-ci correspond à l'une des instructions. Si une correspondance est trouvée, le paquet est traité en conséquence.
- Les listes de contrôle d'accès peuvent être appliquées au trafic entrant ou sortant.
- Les listes de contrôle d'accès standard peuvent uniquement servir à autoriser ou refuser le trafic à partir d'une adresse IPv4 source. La règle de base pour le placement des listes de contrôle d'accès standard consiste à les placer aussi près que possible de la destination.
- Les listes de contrôle d'accès étendues filtrent les paquets en fonction de plusieurs attributs : type de protocole, adresse IPv4 source ou de destination et ports source ou de destination. La règle de base pour le placement des listes de contrôle d'accès étendues consiste à les placer aussi près que possible de la source.



# Suite du résumé

- La commande de configuration globale **access-list** définit une liste de contrôle d'accès standard avec un numéro compris dans la plage 1-99 ou une liste de contrôle d'accès étendue avec un numéro compris dans la plage 100-199. La commande **ip access-list standard nom** sert à créer une liste de contrôle d'accès standard nommée, tandis que la commande **ip access-list extended nom** est destinée à une liste de contrôle d'accès étendue.
- Une fois configurée, une liste de contrôle d'accès est liée à une interface à l'aide de la commande **ip access-group** en mode de configuration d'interface. Un appareil ne peut avoir qu'une liste de contrôle d'accès par protocole, par direction et par interface.
- Pour supprimer une liste de contrôle d'accès d'une interface, saisissez d'abord la commande **no ip access-group** sur l'interface, puis saisissez la commande globale **no access-list** pour supprimer la liste de contrôle d'accès complète.
- Les commandes **show running-config** et **show access-lists** servent à vérifier la configuration de la liste de contrôle d'accès. La commande **show ip interface** permet de vérifier la liste de contrôle d'accès sur l'interface et la direction dans laquelle elle a été appliquée.
- La commande **access-class** configurée en mode de configuration de ligne est utilisée pour lier une liste de contrôle d'accès à une ligne VTY donnée.
- Contrairement à IPv4, il n'est pas nécessaire d'utiliser d'option standard ou étendue pour les listes de contrôle d'accès IPv6.
- À partir du mode de configuration global utilisez la commande **ipv6 access-list nom** pour créer une liste de contrôle d'accès IPv6. Contrairement aux listes de contrôle d'accès IPv4, les listes de contrôle d'accès IPv6 n'utilisent pas de masques génériques. Au lieu de cela, la longueur du préfixe est utilisée pour indiquer avec quelle proportion d'une adresse IPv6 source ou de destination la correspondance doit être établie.
- Une fois qu'une liste de contrôle d'accès IPv6 est configurée, elle est liée à une interface avec la commande **ipv6 traffic-filter**.



# Suite du résumé

- Contrairement aux listes de contrôle d'accès IPv4, les listes de contrôle d'accès IPv6 ne prennent pas en charge l'option standard ou étendue.
- À partir du mode de configuration global utilisez la commande **ipv6 access-list nom** pour créer une liste de contrôle d'accès IPv6.
- Contrairement aux listes de contrôle d'accès IPv4, les listes de contrôle d'accès IPv6 n'utilisent pas de masques génériques. Au lieu de cela, la longueur du préfixe est utilisée pour indiquer avec quelle proportion d'une adresse IPv6 source ou de destination la correspondance doit être établie.
- Une fois qu'une liste de contrôle d'accès IPv6 est configurée, elle est liée à une interface avec la commande **ipv6 traffic-filter**.

# Cisco | Networking Academy®

Mind Wide Open™

