Chapitre 9 : listes de contrôle d'accès

Routage et commutation

Cisco | Networking Academy®
Mind Wide Open™

Chapitre 9

9.1 Fonctionnement des listes de contrôle d'accès IP

9.2 Listes de contrôle d'accès IPv4 standard

9.3 Listes de contrôle d'accès IPv4 étendues

9.4 Module contextuel : le débogage avec les listes de contrôle d'accès

9.5 Dépannage des listes de contrôle d'accès

9.6 Module contextuel : listes de contrôle d'accès IPv6

9.7 Résumé

Chapitre 9 : objectifs

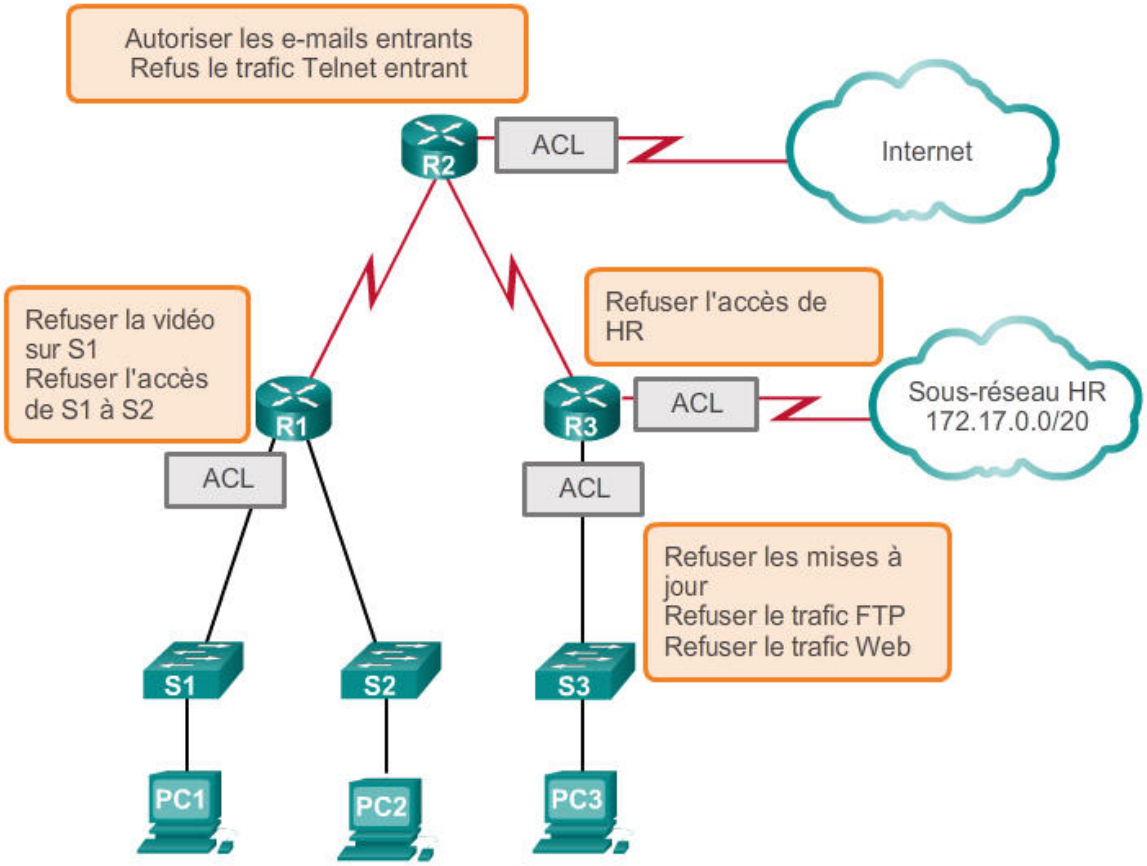
- Expliquer comment les listes de contrôle d'accès sont utilisées pour filtrer le trafic
- Comparer les listes de contrôle d'accès IPv4 standard et étendues
- Expliquer comment les listes de contrôle d'accès utilisent des masques génériques
- Expliquer les directives concernant la création des listes de contrôle d'accès
- Expliquer les directives concernant le placement des listes de contrôle d'accès
- Configurer des listes de contrôle d'accès IPv4 standard pour filtrer le trafic en fonction des besoins du réseau
- Modifier une liste de contrôle d'accès IPv4 standard à l'aide de numéros d'ordre
- Configurer une liste de contrôle d'accès standard pour sécuriser l'accès vty

Chapitre 9 : objectifs (suite)

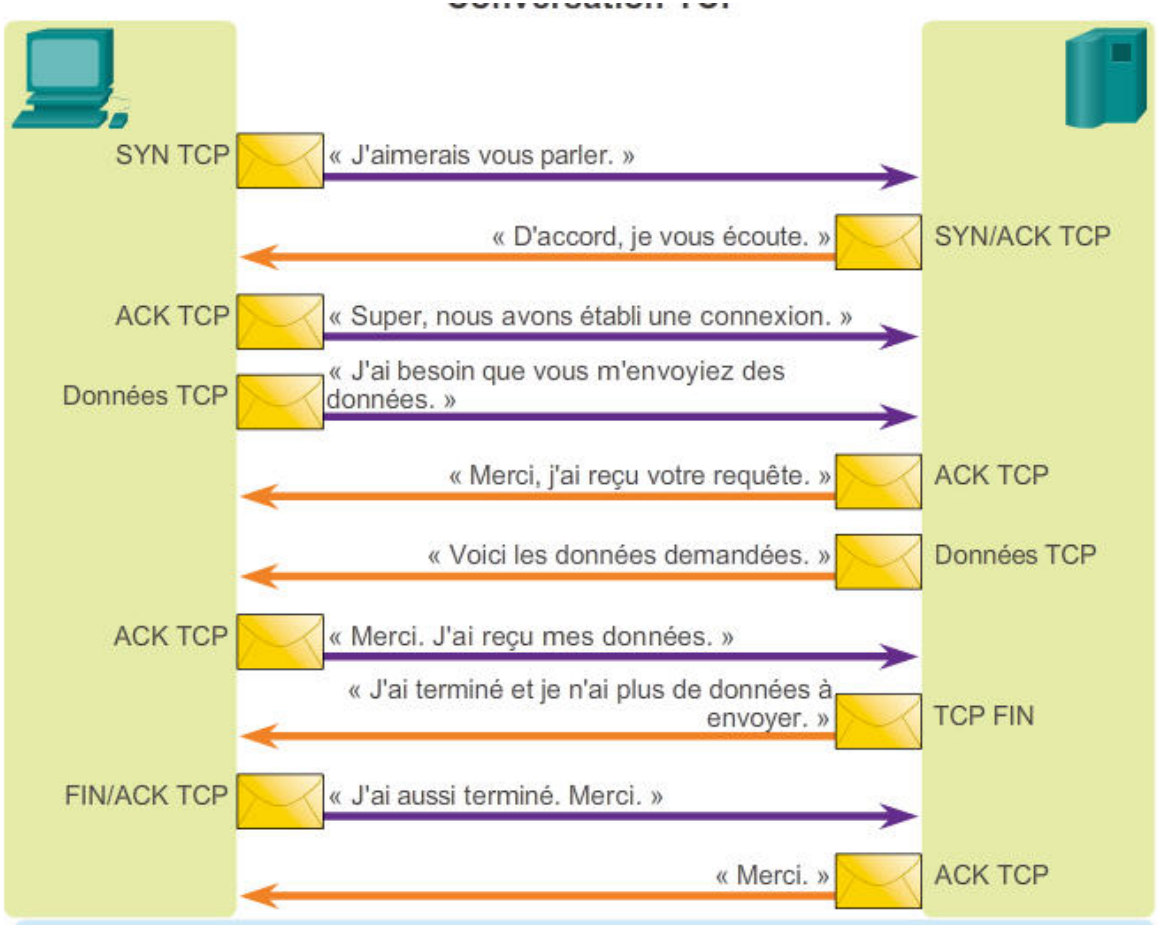
- Expliquer la structure d'une entrée de contrôle d'accès (ACE) étendue
- Configurer des listes de contrôle d'accès IPv4 étendues pour filtrer le trafic en fonction des besoins du réseau
- Configurer une liste de contrôle d'accès pour limiter le résultat de débogage
- Expliquer comment un routeur traite les paquets lorsqu'une liste de contrôle d'accès est appliquée
- Résoudre des erreurs de liste de contrôle d'accès courantes à l'aide de commandes de l'interface en ligne de commande
- Comparer la création de listes de contrôle d'accès IPv4 et IPv6
- Configurer des listes de contrôle d'accès IPv6 pour filtrer le trafic en fonction des besoins du réseau

Objectif des listes de contrôle d'accès

Qu'est-ce qu'une liste de contrôle d'accès ?



Conversation TCP

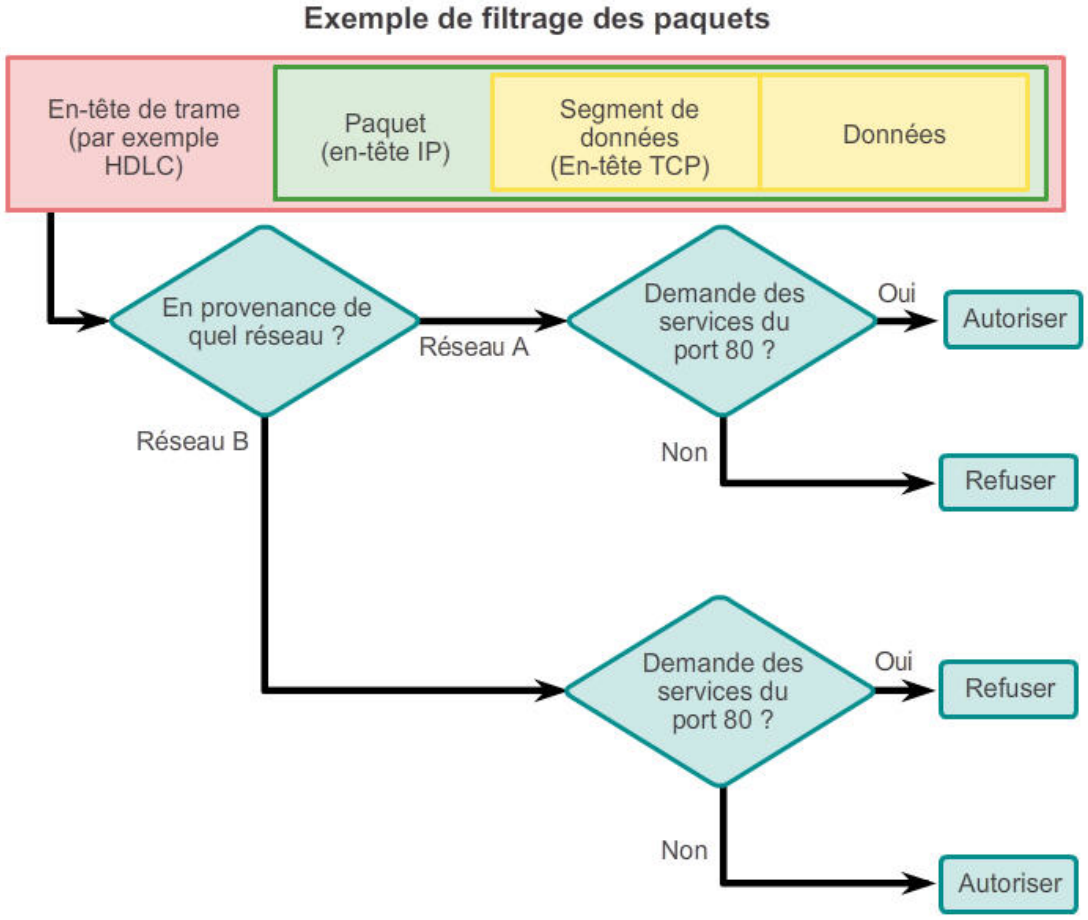


Filtrage des paquets

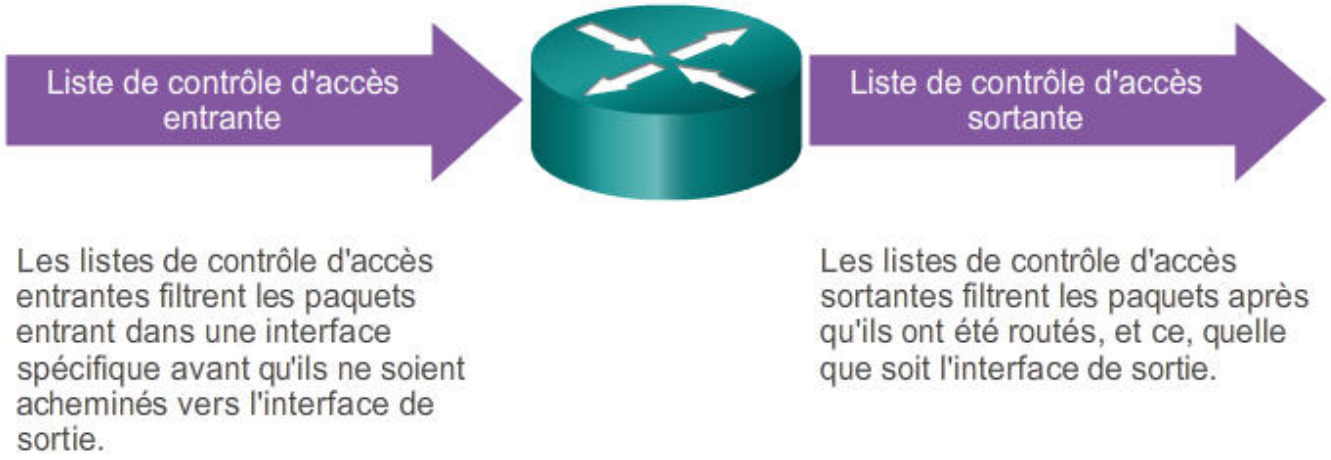
- Le filtrage des paquets, parfois appelé filtrage statique des paquets, contrôle l'accès à un réseau en analysant les paquets entrants et sortants et en les transmettant ou en rejetant selon des critères spécifiques, tels que l'adresse IP source, les adresses IP de destination et le protocole transporté dans le paquet.
- Un routeur filtre les paquets lors de leur transmission ou de leur refus conformément aux règles de filtrage.
- Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus, appelées entrées de contrôle d'accès (ACE).

Objectif des listes de contrôle d'accès

Filtrage des paquets (suite)



Fonctionnement des listes de contrôle d'accès



La dernière instruction d'une liste de contrôle d'accès est toujours implicit deny. Cette instruction est automatiquement ajoutée à la fin de chaque liste de contrôle d'accès, même si elle n'est pas physiquement présente. L'instruction implicit deny bloque l'ensemble du trafic. En raison de ce refus implicite, une liste de contrôle d'accès qui n'a pas au moins une instruction d'autorisation bloquera tout le trafic.

Types de listes de contrôle d'accès IPv4 Cisco

Listes de contrôle d'accès standard

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

Les listes de contrôle d'accès standard filtrent les paquets IP en fonction de l'adresse source uniquement.

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
- Le type ou le numéro de protocole (exemple : IP, ICMP, UDP, TCP, etc.).

Numérotation et nom des listes de contrôle d'accès

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 étendue

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.

Présentation des masques génériques des listes de contrôle d'accès

Les masques génériques et les masques de sous-réseau diffèrent dans leur méthode de mise en correspondance des 1 et des 0 binaires. Les masques génériques respectent les règles suivantes pour faire correspondre les chiffres binaires 1 et 0 :

- Bit 0 de masque générique : permet de vérifier la valeur du bit correspondant dans l'adresse.
- Bit 1 de masque générique : permet d'ignorer la valeur du bit correspondant dans l'adresse.

Les masques génériques sont souvent appelés masques inverses. En effet, contrairement à un masque de sous-réseau, où le chiffre binaire 1 équivaut à une correspondance et le chiffre binaire 0 à une non-correspondance, les masques génériques procèdent de façon inverse.

Exemples de masques génériques : hôtes/sous-réseaux

Exemple 1

	Décimal	Binaire
Adresse IP	192.168.1.1	11000000.10101000.00000001.00000001
Masque générique	0.0.0.0	00000000.00000000.00000000.00000000
Résultats	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
Résultats	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
Résultats	192.168.1.0	11000000.10101000.00000001.00000000

Exemples de masques génériques : correspondance avec des plages

Exemple 1

	Décimal	Binaire
Adresse IP	192.168.16.0	11000000.10101000.00010000.00000000
Masque générique	0.0.15.255	00000000.00000000.00001111.11111111
Plage de résultats	192.168.16.0 à 192.168.31.255	11000000.10101000.00010000.00000000 à 11000000.10101000.00011111.11111111

Exemple 2

	Décimal	Binaire
Adresse IP	192.168.1.0	11000000.10101000.00000001.00000000
Masque générique	0.0.254.255	00000000.00000000.11111110.11111111
Résultat	192.168.1.0	11000000.10101000.00000001.00000000
	Tous les sous-réseaux impairs sur le réseau principal 192.168.0.0	

Calcul du masque générique

Le calcul des masques génériques peut être complexe. La méthode la plus rapide consiste à soustraire le masque de sous-réseau de 255.255.255.255.

Exemple 1

```
  255.255.255.255
- 255.255.255.000
-----------------
  000.000.000.255
```

Exemple 2

```
  255.255.255.255
- 255.255.255.240
-----------------
  000.000.000.015
```

Exemple 3

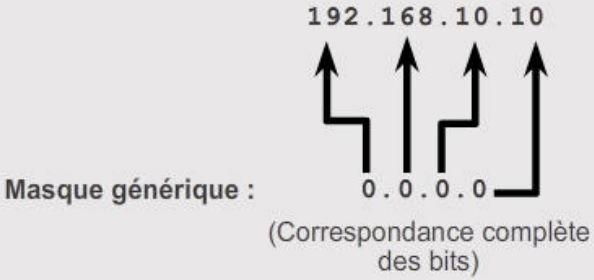
```
  255.255.255.255
- 255.255.254.000
-----------------
  000.000.001.255
```

Masques génériques dans les listes de contrôle d'accès

Mots-clés des masques génériques

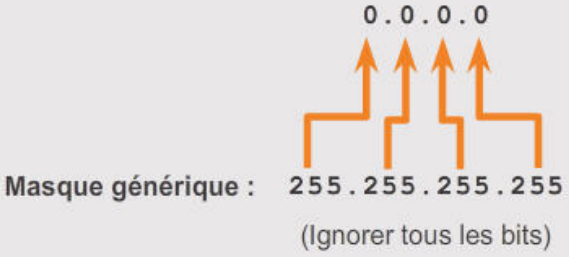
Exemple 1

- 192.168.10.10 0.0.0.0 correspond à tous les bits d'adresse
- Abrégez ce masque générique à l'aide de l'adresse IP précédée du mot-clé **host** (**host 192.168.10.10**)



Exemple 2

- 0.0.0.0 255.255.255.255 ignore tous les bits d'adresse
- Abrégez l'expression avec le mot-clé **any**



Exemples de mots-clés de masque générique

Exemple 1 :

```
R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)#access-list 1 permit any
```

Exemple 2 :

```
R1(config)#access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit host 192.168.10.10
```

Directives générales concernant la création des listes de contrôle d'accès

- Utilisez des listes de contrôle d'accès sur les routeurs pare-feu situés entre votre réseau interne et un réseau externe, par exemple Internet.
- Utilisez des listes de contrôle d'accès sur un routeur situé entre deux parties de votre réseau pour contrôler le trafic entrant ou sortant sur une portion donnée du réseau interne.
- Configurez des listes de contrôle d'accès sur les routeurs périphériques situés à la périphérie de vos réseaux.
- Configurez des listes de contrôle d'accès pour tout protocole réseau configuré sur les interfaces de routeur périphérique.

Directives générales concernant la création des listes de contrôle d'accès

Règle des trois P

- Une liste de contrôle d'accès par protocole : pour contrôler le flux du trafic sur une interface, définissez une liste de contrôle d'accès pour chaque protocole activé sur l'interface.
- Une liste de contrôle d'accès par direction : les listes de contrôle d'accès contrôlent le trafic dans une seule direction à la fois sur une interface. Vous devez créer deux listes de contrôle d'accès, la première pour contrôler le trafic entrant et la seconde pour contrôler le trafic sortant.
- Une liste de contrôle d'accès par interface : les listes de contrôle d'accès contrôlent le trafic dans une seule interface, par exemple, Gigabit Ethernet 0/0.

Méthodes recommandées pour les listes de contrôle d'accès

Directive	Avantage
Créez vos listes de contrôle d'accès conformément à la stratégie de sécurité de votre entreprise.	Vous serez ainsi certain d'implémenter les instructions relatives à la sécurité organisationnelle.
Préparez une description des tâches que devront effectuer les listes de contrôle d'accès.	Vous éviterez ainsi de créer d'éventuels problèmes d'accès par mégarde.
Utilisez un éditeur de texte pour créer, modifier et enregistrer les listes de contrôle d'accès.	Vous pourrez ainsi créer une bibliothèque de listes de contrôle d'accès réutilisables.
Testez vos listes de contrôle d'accès sur un réseau de développement avant de les implémenter sur un réseau de production.	Vous éviterez ainsi de commettre des erreurs coûteuses.

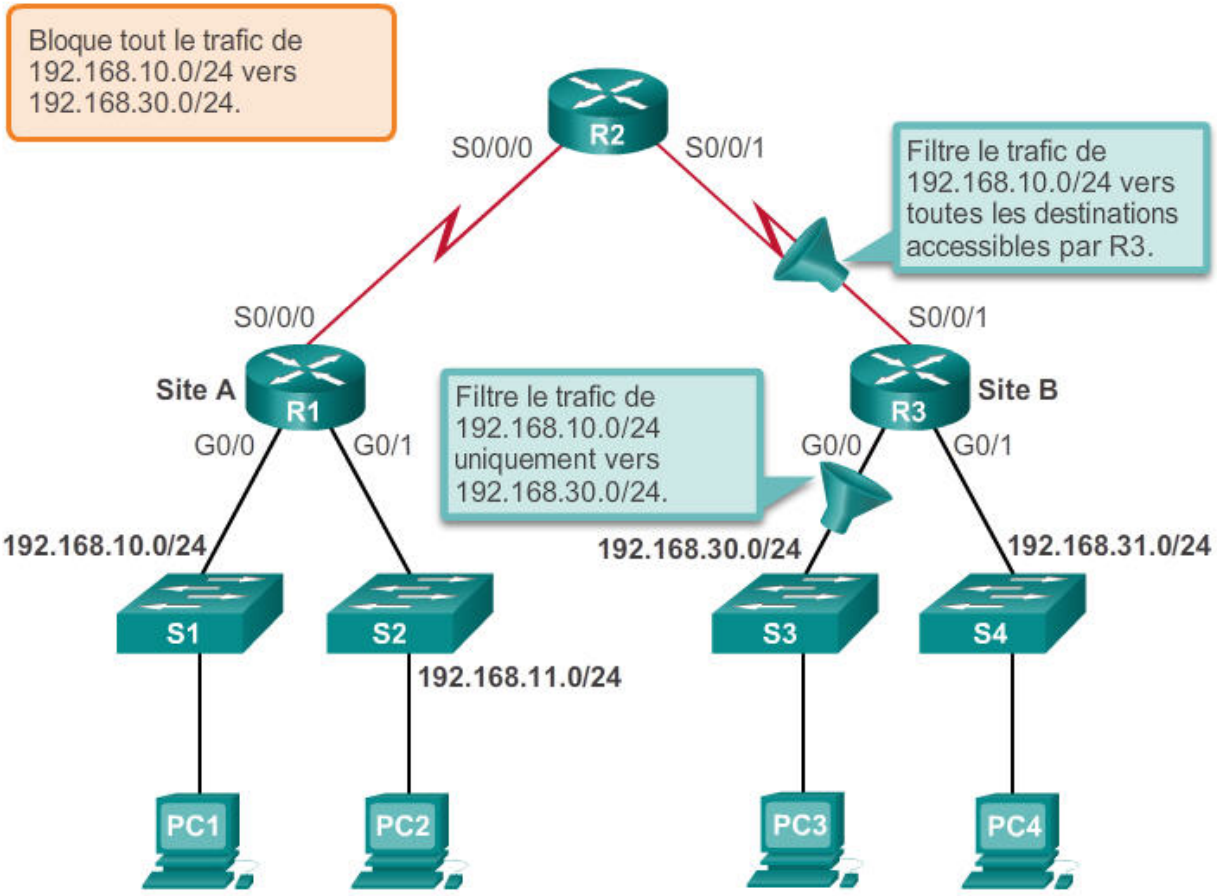
Où placer les listes de contrôle d'accès

Chaque liste de contrôle d'accès doit être placée là où elle aura le plus grand impact sur les performances. Règles de base :

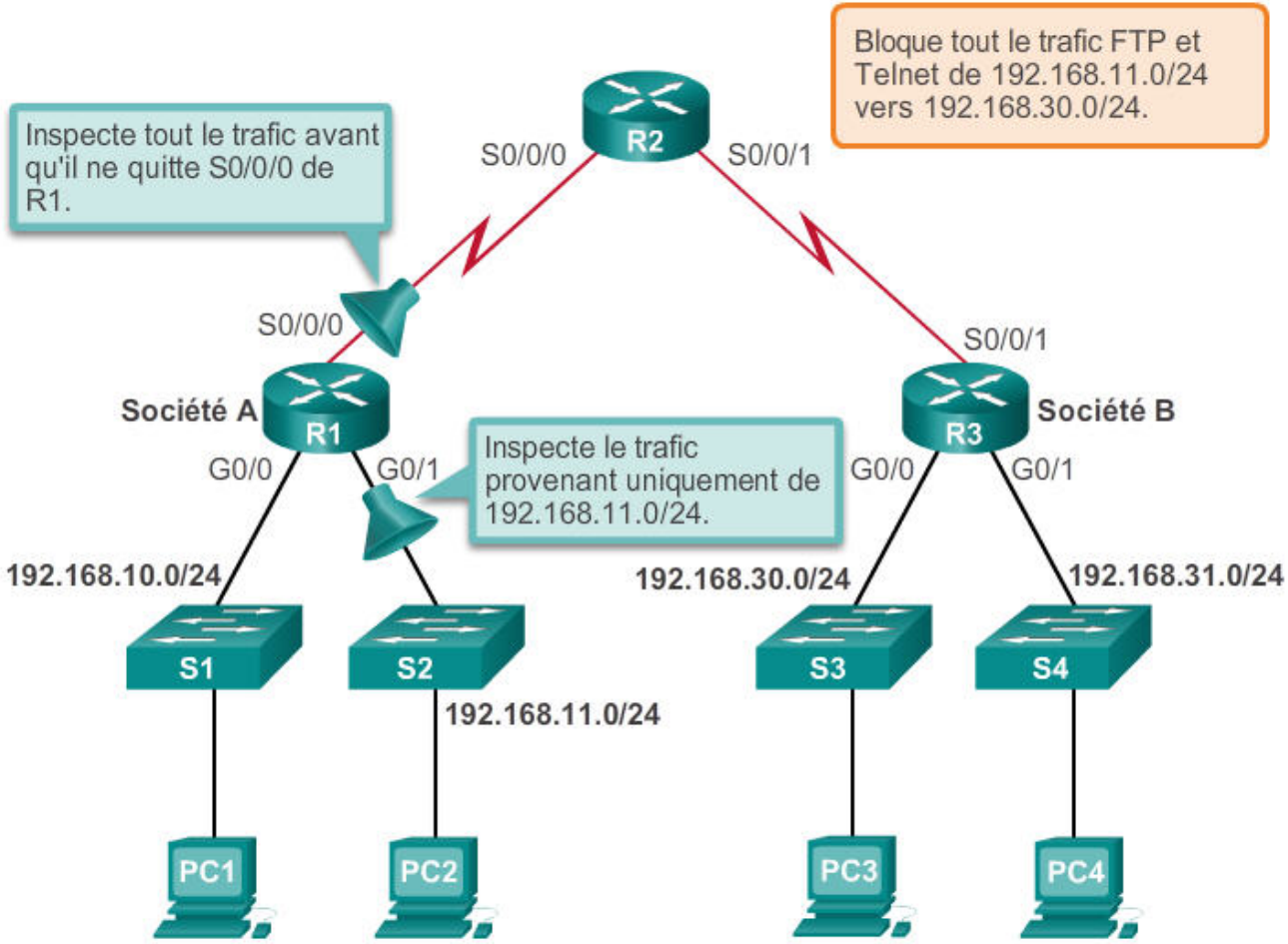
- Listes de contrôle d'accès étendues : placez les listes de contrôle d'accès étendues le plus près possible de la source du trafic à filtrer.
- Listes de contrôle d'accès standard : étant donné qu'elles ne spécifient pas les adresses de destination, placez-les le plus près possible de la destination.

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.

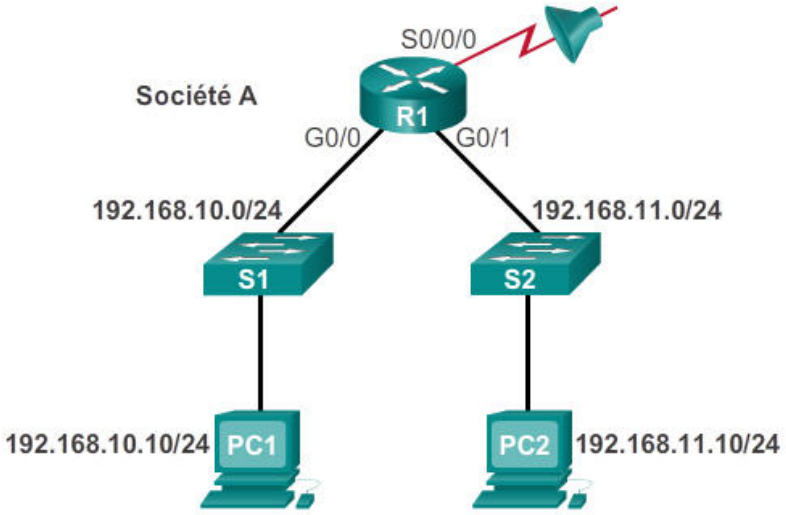
Emplacement d'une liste de contrôle d'accès standard



Emplacement d'une liste de contrôle d'accès étendue



Saisie des instructions pour les critères



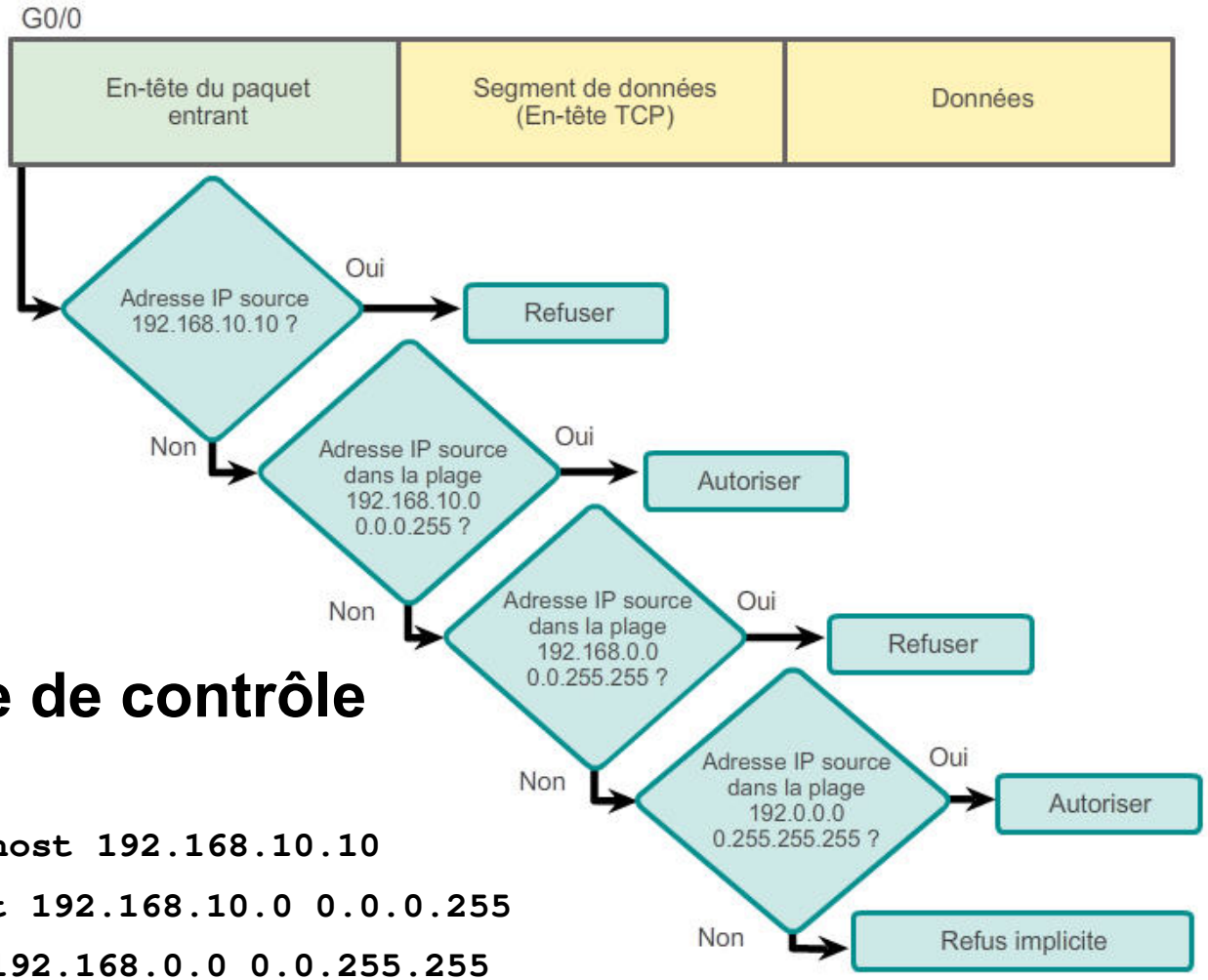
ACL 1

```
R1(config)#access-list 1 permit ip 192.168.10.0 0.0.0.255
```

ACL 2

```
R1(config)#access-list 2 permit ip 192.168.10.0 0.0.0.255
R1(config)#access-list 2 deny any
```

Configuration d'une liste de contrôle d'accès standard



Exemple de liste de contrôle d'accès :

- `access-list 2 deny host 192.168.10.10`
- `access-list 2 permit 192.168.10.0 0.0.0.255`
- `access-list 2 deny 192.168.0.0 0.0.255.255`
- `access-list 2 permit 192.0.0.0 0.255.255.255`

Configuration d'une liste de contrôle d'accès standard (suite)

La syntaxe complète de la commande des listes de contrôle d'accès standard est la suivante :

```
Router(config)# access-list access-list-number
deny permit remark source [ source-wildcard ]
[ log ]
```

Pour supprimer la liste de contrôle d'accès, la commande de configuration globale **no access-list** est utilisée.

Le mot-clé **remark** est utilisé à des fins de documentation et rend les listes de contrôle d'accès bien plus simples à comprendre.

Logique interne

- Cisco IOS applique une logique interne lors de l'acceptation et du traitement des instructions des listes de contrôle d'accès standard. Comme nous l'avons vu, les instructions des listes de contrôle d'accès sont traitées dans l'ordre. Par conséquent, l'ordre dans lequel elles sont fournies est important.

```
R1(config)#access-list 3 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 3 permit host 192.168.10.10
% Access rule can't be configured at higher sequence num as
it is part of the existing rule at sequence num 10
R1(config)#
```

ACL 3 : l'instruction d'hôte est en conflit avec l'instruction de plage précédente.

Application de listes de contrôle d'accès standard aux interfaces

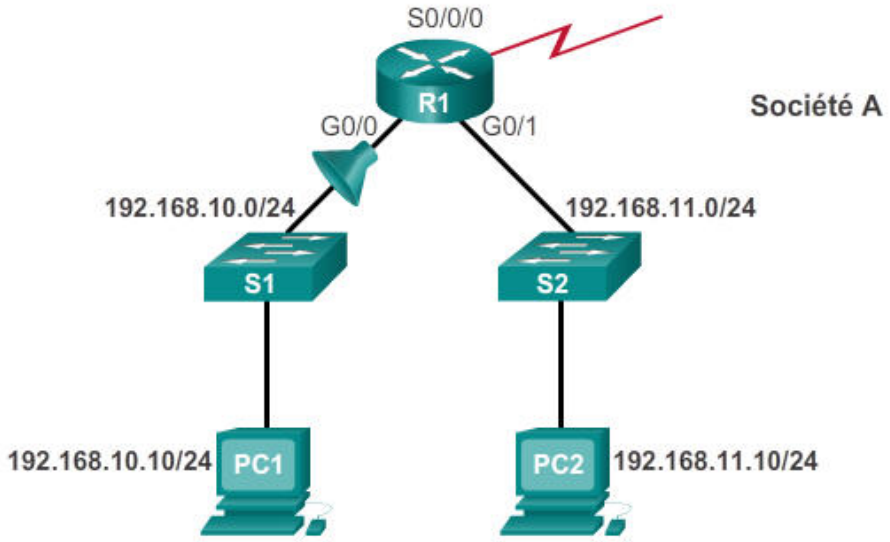
Une fois qu'une liste de contrôle d'accès standard est configurée, elle est associée à une interface à l'aide de la commande **ip access-group** en mode de configuration d'interface :

- `Router(config-if)# ip access-group { access-list-number | access-list-name } { in | out }`

Pour supprimer une liste de contrôle d'accès d'une interface, entrez d'abord la commande **no ip access-group** sur l'interface, puis la commande globale **no access-list** pour supprimer l'ensemble de la liste.

Application de listes de contrôle d'accès standard aux interfaces (suite)

Refuser un certain hôte




```
R1(config)#access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 permit any
R1(config)#interface g0/0
R1(config-if)#ip access-group 1 in
```

Création des listes de contrôle d'accès standard nommées

```
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.

Commentaires dans les listes de contrôle d'accès

Exemple 1 : Commentaires sur une liste de contrôle d'accès numérotée

```
R1(config)# access-list 1 remark Do not allow Guest workstation
through
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 remark Allow devices from all other
192.168.x.x subnets
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
R1(config-if)#
```

Exemple 2 : Commentaires sur une liste de contrôle d'accès nommée

```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# remark Do not allow access from Lab
workstation
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# remark Allow access from all other networks
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config-std-nacl)# interface G0/0
R1(config-if)# ip access-group NO_ACCESS out
R1(config-if)#
```

Modification des listes de contrôle d'accès numérotées

Modification des listes de contrôle d'accès numérotées dans un éditeur de texte

Configuration

```
R1(config)# access-list 1 deny host 192.168.10.99
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Étape 1

```
R1# show running-config | include access-list 1
access-list 1 deny host 192.168.10.99
access-list 1 permit 192.168.0.0 0.0.255.255
```

Étape 2

```
<Éditeur de texte>
access-list 1 deny host 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Étape 3

```
R1# config t
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Étape 4

```
R1# show running-config | include access-list 1
access-list 1 deny host 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Modification des listes de contrôle d'accès numérotées (suite)

Modification des listes de contrôle d'accès numérotées à l'aide des numéros d'ordre

Configuration

```
R1(config)#access-list 1 deny host 192.168.10.99
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
```

Étape 1

```
R1#show access-lists 1
Standard IP access list 1
    10 deny   192.168.10.99
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
R1#
```

Étape 2

```
R1#conf t
R1(config)#ip access-list standard 1
R1(config-std-nacl)#no 10
R1(config-std-nacl)#10 deny host 192.168.10.10
R1(config-std-nacl)#end
R1#
```

Étape 3

```
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
R1#
```

Modification des listes de contrôle d'accès nommées standard

Ajout d'une ligne à une liste de contrôle d'accès nommée

```
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# 15 deny host 192.168.11.11
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    15 deny   192.168.11.11
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Remarque : la commande d'ACL nommée **no** *sequence-number* permet de supprimer des instructions spécifiques.

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#
```

Modification des listes de contrôle d'accès IPv4

Statistiques des listes de contrôle d'accès

```
R1#show access-lists
Standard IP access list 1
    10 deny   192.168.10.10 (4 match(es))
    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 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Output after pinging PC3 from PC1.

Les correspondances ont été incrémentées.

```
R1#show access-lists
Standard IP access list 1
    10 deny   192.168.10.10 (8 match(es))
    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 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Numéros d'ordre des listes de contrôle d'accès standard

- Une autre partie de la logique interne IOS comprend le séquençage interne des instructions des listes de contrôle d'accès standard. Les instructions de plage qui refusent trois réseaux sont configurées en premier et sont suivies de cinq instructions d'hôte. Les instructions d'hôte sont toutes des instructions valides car leurs adresses IP d'hôte ne font pas partie des instructions de plage précédemment entrées.
- Les instructions d'hôte apparaissent avec la commande show en premier, mais pas nécessairement dans l'ordre dans lequel elles ont été saisies. IOS classe les instructions d'hôte à l'aide d'une fonction de hachage spéciale. Le classement résultant permet d'optimiser la recherche d'une entrée de liste de contrôle d'accès d'hôte.

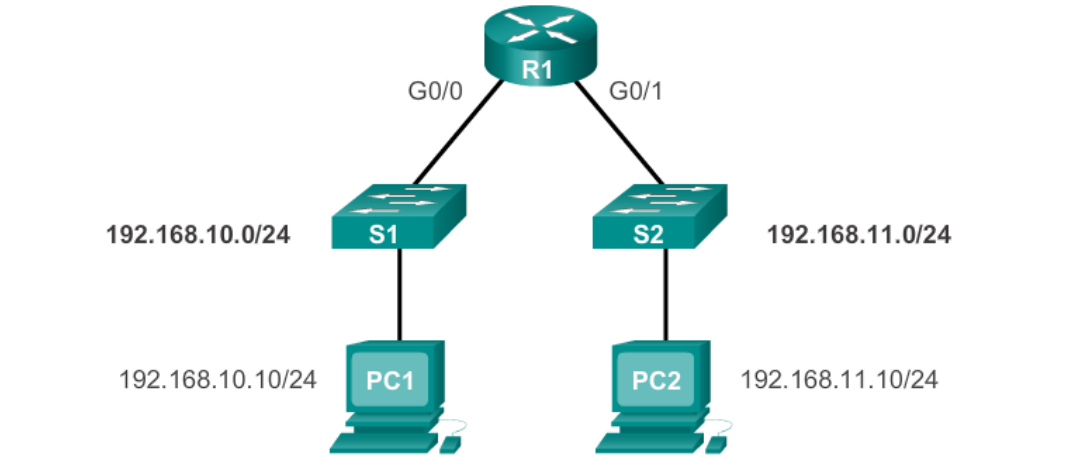
Configuration d'une liste de contrôle d'accès standard pour sécuriser un port VTY

Le filtrage du trafic Telnet ou SSH est généralement considéré comme une fonction de liste de contrôle d'accès IP étendue parce qu'il s'agit de filtrer un protocole de niveau plus élevé. Cependant, étant donné que la commande **access-class** permet de filtrer les sessions Telnet/SSH entrantes ou sortantes par adresse source, une liste de contrôle d'accès standard peut être utilisée.

- `Router(config-line)# access-class` *`access-list-number`* `{ in [ vrf-also ] | out }`

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#
```




```
PC1>ssh 192.168.10.1

Login as: admin
Password: *****
R1>
```

```
PC2>ssh 192.168.11.1
ssh connect to host 192.168.11.1 port
22: Connection refused

PC2>
```

Listes de contrôle d'accès étendues

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

- Adresse source
- Adresse de destination
- Protocole
- Numéros de port

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

Listes de contrôle d'accès étendues (suite)

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

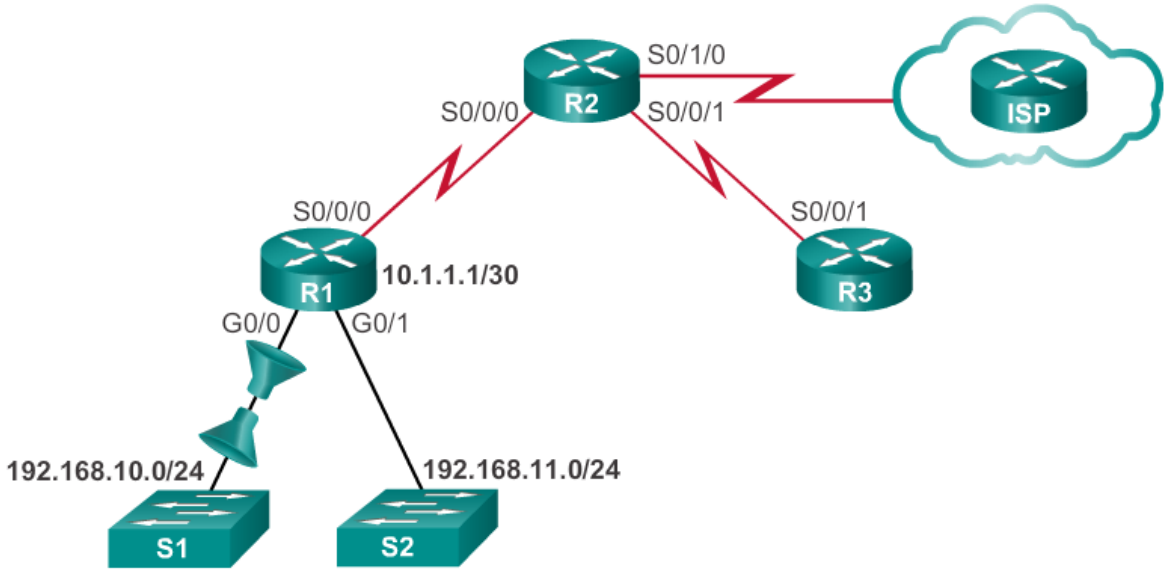
```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

Configuration des listes de contrôle d'accès 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 operand]
[port port-number or name] destination [destination-wildcard]
[operator operand] [port port-number or name][established]
```

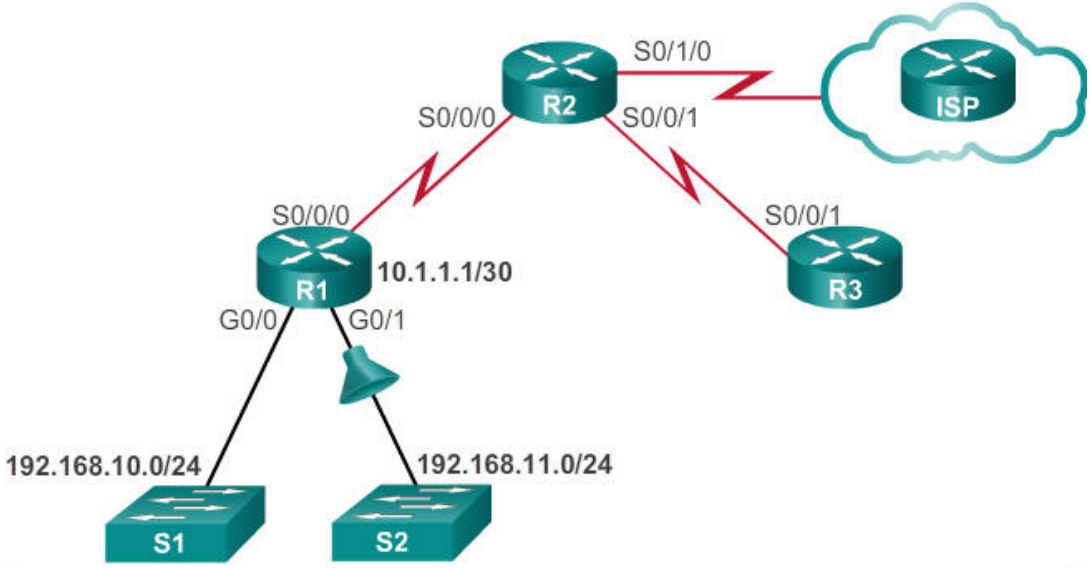
Application des listes de contrôle d'accès étendues aux interfaces




```
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
```

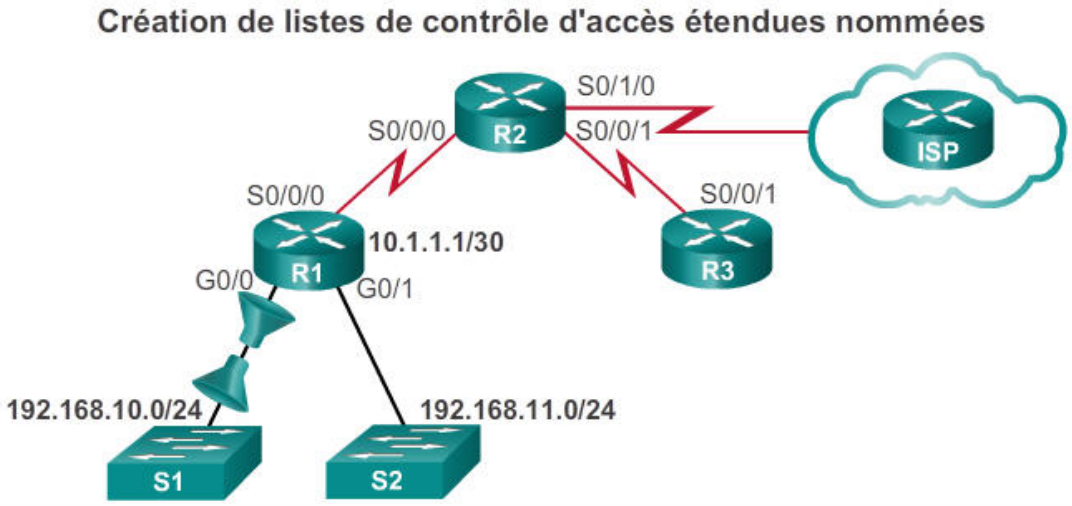
Filtrage du trafic avec des listes de contrôle d'accès étendues

Liste de contrôle d'accès étendue pour refuser le trafic 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
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
```

Création des 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
```

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>
```

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 :

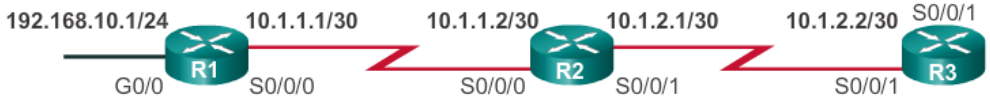
- Méthode 1 : éditeur de texte
- Méthode 2 : numéros d'ordre

Objectif de la limitation des résultats du débogage avec les listes de contrôle d'accès

- Les commandes debug sont des outils destinés à vérifier et à dépanner le réseau.
- Si vous les utilisez avec des options, les résultats risquent de contenir beaucoup plus d'informations que nécessaire ou d'être difficiles à lire.
- Dans un environnement de production, cela risque de saturer le réseau et d'entraîner des interruptions.
- Certaines commandes debug peuvent être associées à une liste d'accès pour limiter les résultats et afficher uniquement les informations requises pour la vérification ou la résolution d'un problème.

Configuration des listes de contrôle d'accès pour limiter les résultats du débogage

L'administrateur de R2 souhaite s'assurer que le trafic est acheminé correctement grâce à la commande **debug ip packet**. Pour limiter les résultats du débogage et inclure uniquement le trafic ICMP entre R1 et R3, la liste de contrôle d'accès ACL 101 sera appliquée.




```
R2(config)#ip access-list extended 101
R2(config-ext-nacl)#permit icmp host 10.1.1.1 host 10.1.2.2
R2(config-ext-nacl)#permit icmp host 10.1.2.2 host 10.1.1.1
R2(config-ext-nacl)#exit
R2(config)#interface s0/0/0
R2(config-if)#no ip route-cache
R2(config-if)#exit
R2(config)#interface s0/0/1
R2(config-if)#no ip route-cache
R2(config-if)#end
R2#
R2#debug ip packet 101
IP packet debugging is on for access list 101
R2#
```

Vérification des listes de contrôle d'accès qui limitent les résultats du débogage


```
R2# debug ip packet 101
IP packet debugging is on for access list 101
R2#

<ping 10.1.2.2 command entered on R1>

*Jan 25 20:49:26.910: IP: s=10.1.1.1 (Serial0/0/0), d=10.1.2.2
(Serial0/0/1), g=10.1.2.2, len 100, forward
*Jan 25 20:49:26.910: IP: s=10.1.1.1 (Serial0/0/0), d=10.1.2.2
(Serial0/0/1), len 100, sending full packet
*Jan 25 20:49:26.938: IP: s=10.1.2.2 (Serial0/0/1), d=10.1.1.1
(Serial0/0/0), g=10.1.1.1, len 100, forward
*Jan 25 20:49:26.938: IP: s=10.1.2.2 (Serial0/0/1), d=10.1.1.1
(Serial0/0/0), len 100, sending full packet

<output omitted>
```

Logique d'une liste de contrôle d'accès pour le trafic entrant

- Les paquets sont comparés à une liste de contrôle d'accès pour le trafic entrant, s'il en existe une, avant d'être acheminés.
- Si un paquet entrant correspond à une instruction de la liste de contrôle d'accès avec une autorisation, il est envoyé pour être acheminé.
- Si un paquet entrant correspond à une instruction de la liste de contrôle d'accès avec un refus, il est abandonné et pas acheminé.
- Si un paquet entrant ne correspond à aucune instruction de la liste de contrôle d'accès, il est « implicitement refusé » et abandonné sans être acheminé.

Logique d'une liste de contrôle d'accès pour le trafic sortant

- Une route est d'abord cherchée pour les paquets avant leur envoi à une interface sortante. En l'absence de route, les paquets sont abandonnés.
- Si une interface de sortie n'a pas de liste de contrôle d'accès, les paquets sont envoyés directement vers celle-ci.
- S'il existe une liste de contrôle d'accès sur l'interface de sortie, il y a une vérification avant l'envoi à cette interface.
- Si un paquet sortant correspond à une instruction de la liste de contrôle d'accès avec une autorisation, il est envoyé à l'interface.

Logique d'une liste de contrôle d'accès pour le trafic sortant (suite)

- Si un paquet sortant correspond à une instruction de la liste de contrôle d'accès avec un refus, il est abandonné.
- Si un paquet sortant ne correspond à aucune instruction de la liste de contrôle d'accès, il est « implicitement refusé » et abandonné.

Opérations logiques de la liste de contrôle d'accès

- Lorsqu'un paquet parvient à l'interface d'un routeur, le processus de ce dernier est identique, que des listes de contrôle d'accès soient utilisées ou non. Lorsqu'une trame arrive dans l'interface, le routeur détermine si l'adresse de couche 2 de la destination correspond à l'adresse de couche 2 de l'interface ou si la trame est 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.

Opérations logiques de la liste de contrôle d'accès (suite)

- 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.
- 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.

Processus de décision avec les listes de contrôle d'accès standard

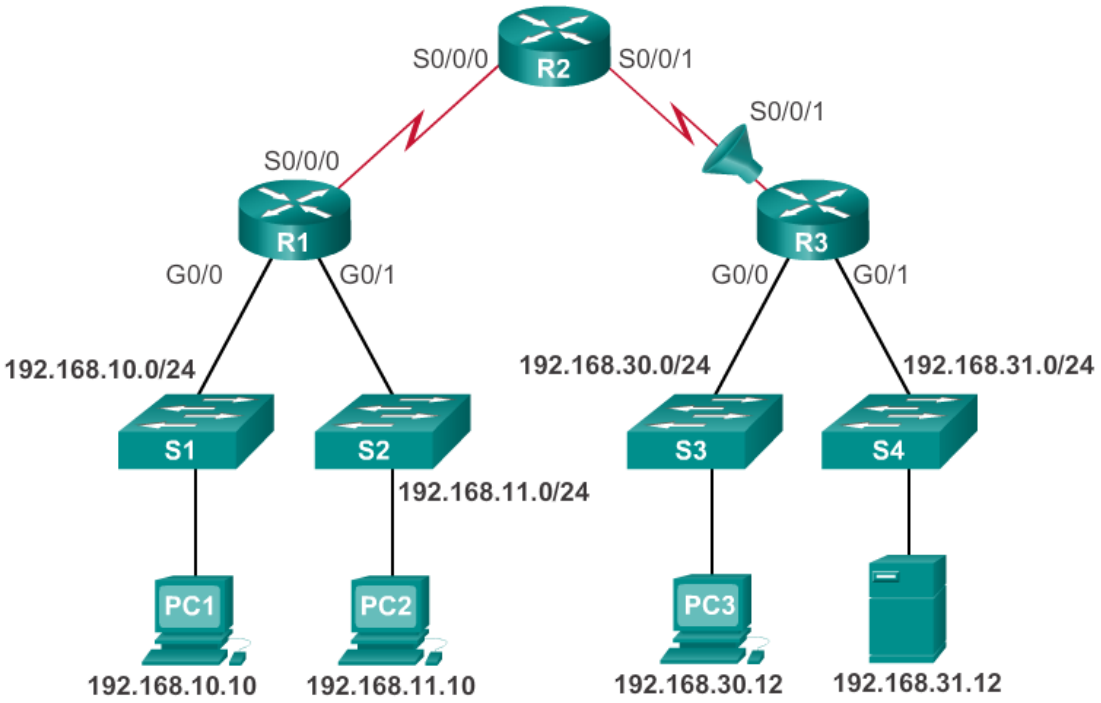
- Les listes de contrôle d'accès standard examinent uniquement l'adresse IPv4 source. La destination du paquet et les ports concernés ne sont pas pris en compte.
- Le logiciel Cisco IOS vérifie les correspondances d'adresses dans les listes de contrôle d'accès les unes après les autres. La première correspondance détermine si le logiciel accepte ou refuse l'adresse. Dans la mesure où le logiciel ne vérifie plus les conditions après la première correspondance, l'ordre des conditions est primordial. En cas de non-concordance des conditions, l'adresse est rejetée.

Processus de décision avec les listes de contrôle d'accès étendues

- Dans cet exemple, la liste de contrôle d'accès filtre en fonction de l'adresse source avant de passer au port et au protocole de la source. Elle filtre en fonction de l'adresse de destination, du port et du protocole de destination, avant de prendre une décision finale d'autorisation ou de refus.

Résolution des erreurs courantes avec listes de contrôle d'accès – Exemple 1

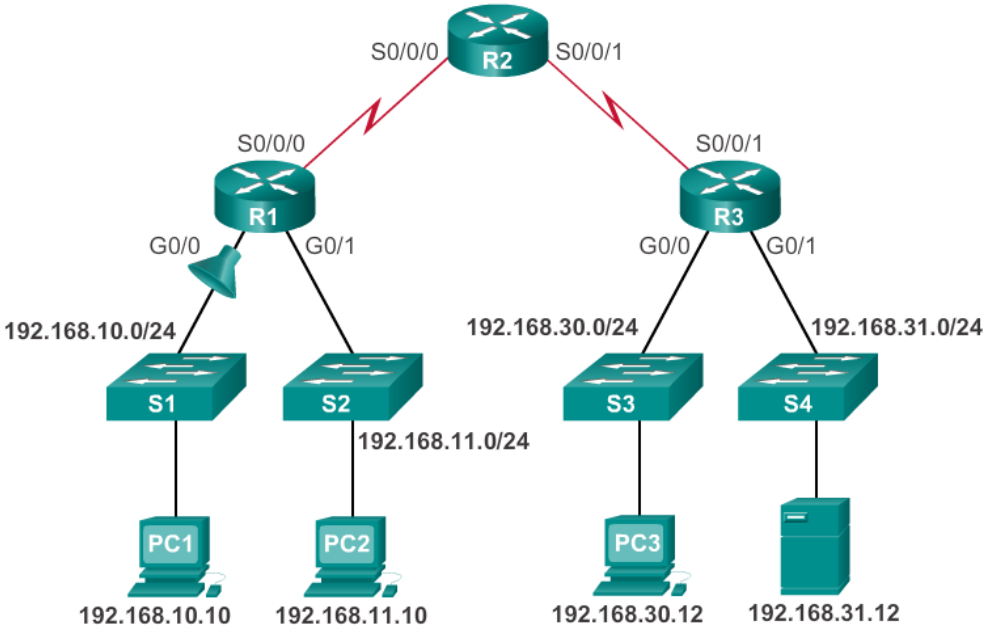
L'hôte 192.168.10.10 n'a aucune connectivité avec 192.168.30.12.




```
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
```

Résolution des erreurs courantes avec listes de contrôle d'accès – Exemple 2

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

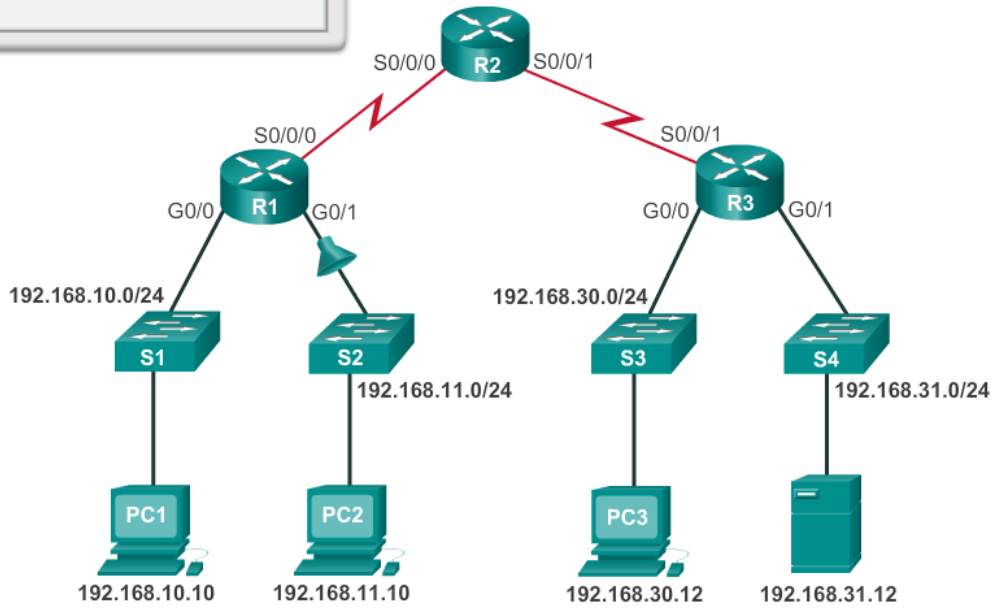



```
R1#show access-lists 120
Extended IP access list 120
    10 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
    20 deny tcp 192.168.10.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any
```

Résolution des erreurs courantes avec listes de contrôle d'accès – Exemple 3

Le réseau 192.168.11.0 /24 peut utiliser Telnet pour se connecter à 192.168.30.0 /24 alors que cette connexion doit être interdite.

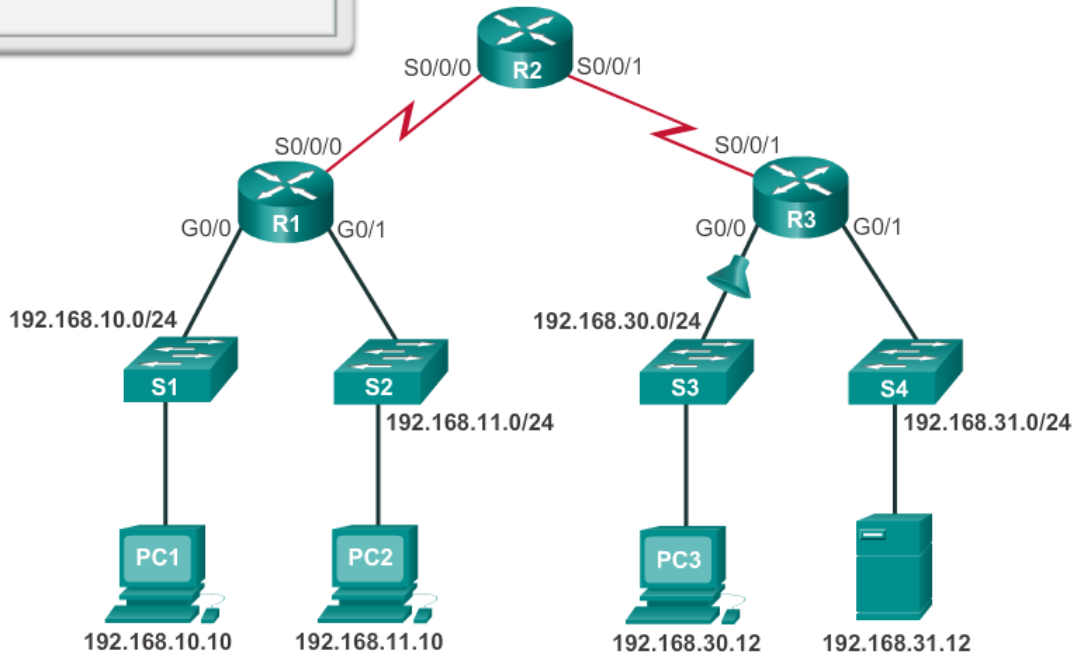
```
R1#show access-lists 130
Extended IP access list 130
    10 deny tcp any eq telnet any
    20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any (12 match(es))
```



Résolution des erreurs courantes avec listes de contrôle d'accès – Exemple 4

L'hôte 192.168.30.12 peut utiliser Telnet pour se connecter à 192.168.31.12, mais la politique de l'entreprise stipule que cette connexion ne doit pas être autorisée.

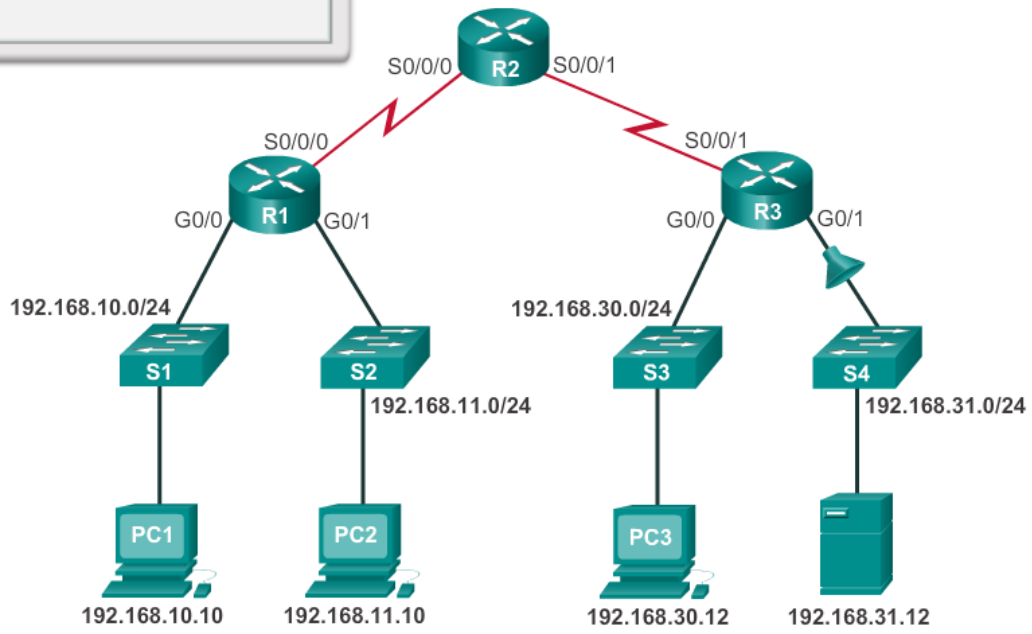
```
R3#show access-lists 140
Extended IP access list 140
    10 deny tcp host 192.168.30.1 any eq telnet
    20 permit ip any any (5 match(es))
```



Résolution des erreurs courantes avec listes de contrôle d'accès – Exemple 5

L'hôte 192.168.30.12 peut utiliser Telnet pour se connecter à 192.168.31.12, mais selon la stratégie de sécurité, 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
```



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

Comparaison des listes de contrôle d'accès IPv4 et IPv6

Bien que les adresses IPv4 et IPv6 liste sont très similaires, il existe trois différences entre eux.

- Application d'une liste de contrôle d'accès IPv6

  IPv6 utilise la commande **`ipv6 traffic-filter`** pour effectuer la même tâche sur les interfaces IPv6.

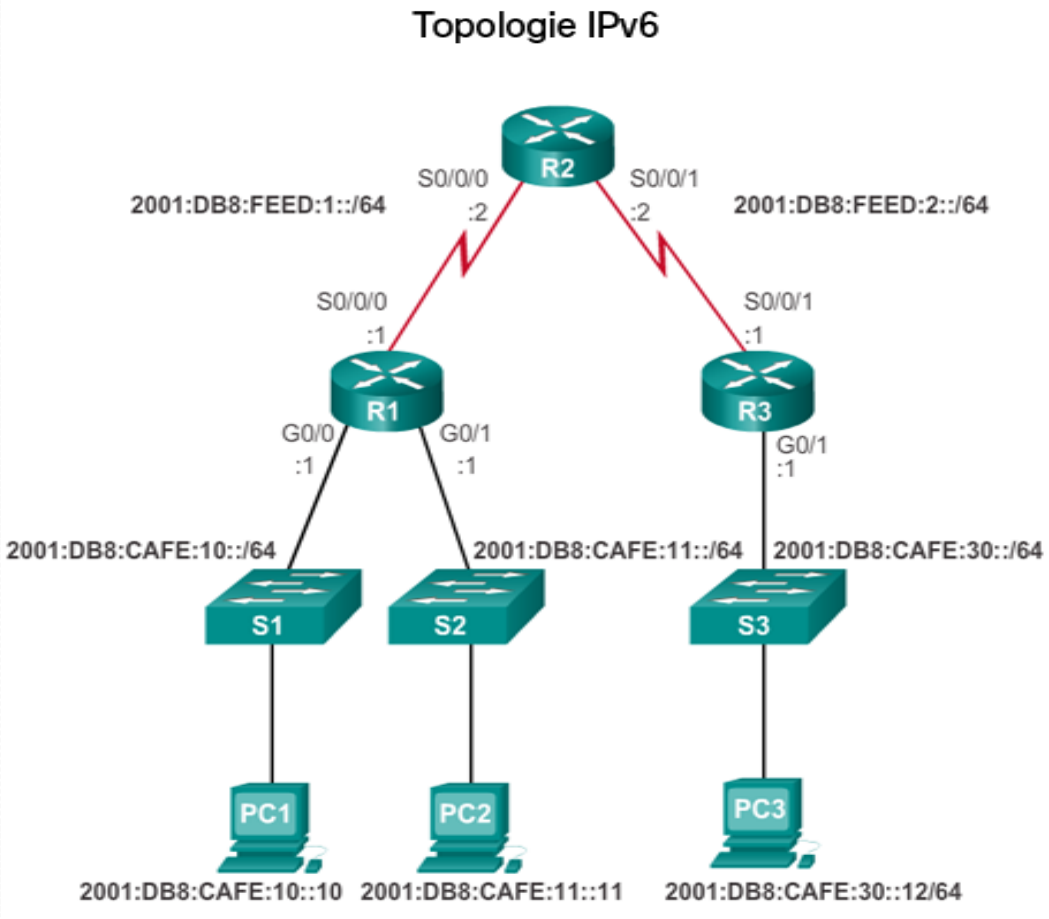
- Aucun masque générique

  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 la topologie IPv6



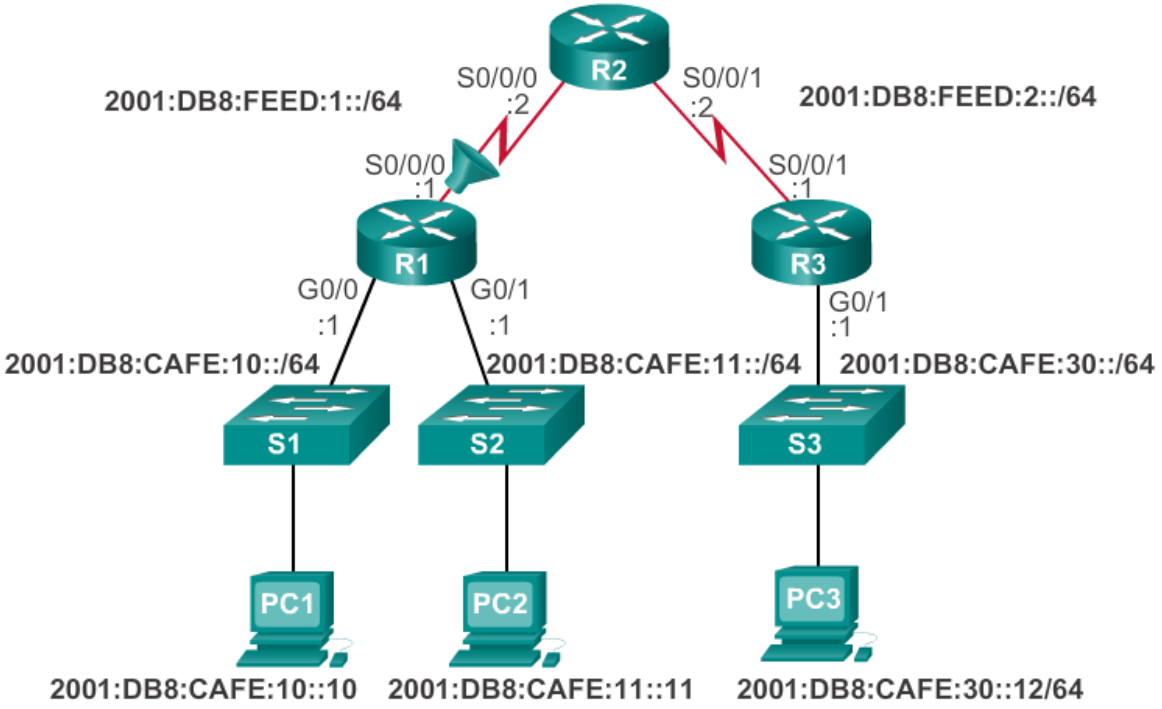
Configuration des listes de contrôle d'accès IPv6

Il existe trois étapes de base pour configurer une liste de contrôle d'accès IPv6 :

- En mode de configuration globale, utilisez la commande **ipv6 access-list** *name* pour créer une liste de contrôle d'accès IPv6.
- En mode de configuration des listes de contrôle d'accès nommées, utilisez les instructions **permit** ou **deny** pour spécifier une ou plusieurs conditions pour déterminer si un paquet est transféré ou abandonné.
- Retournez au mode d'exécution privilégié à l'aide de la commande **end**.

```
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]]
```

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
```

Exemples de listes de contrôle d'accès IPv6

Refuser 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)#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)#
```

Restriction de l'accès

```
R3(config)#ipv6 access-list RETRICTED-ACCESS
R3(config-ipv6-acl)#remark Permit access only HTTP and HTTPS to Network 1
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   (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:CA
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   (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)#
```

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
<some output omitted for brevity>
```

```
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#
```

Chapitre 9 : résumé

- 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.
- Le filtrage des paquets consiste à contrôler l'accès à un réseau en analysant les paquets entrants et sortants et en les transmettant ou en les rejetant selon des critères spécifiques, tels que l'adresse IP source, les adresses IP de destination et le protocole transporté dans le paquet.
- Un routeur de filtrage de paquets utilise des règles pour déterminer s'il doit autoriser ou refuser le trafic. Un routeur peut également effectuer le filtrage des paquets au niveau de la couche 4, la couche transport.
- Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus.

Résumé du chapitre 9 (suite)

- La dernière instruction d'une liste de contrôle d'accès est toujours une instruction deny implicite bloquant tout le trafic. Pour empêcher l'instruction deny any implicite à la fin de la liste de contrôle d'accès de bloquer 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, afin de déterminer si le paquet correspond à l'une des instructions. Si une correspondance est trouvée, le paquet est traité en conséquence.
- Les listes de contrôle d'accès sont configurées pour s'appliquer au trafic entrant ou sortant.

Résumé du chapitre 9 (suite)

- Les listes de contrôle d'accès standard peuvent être utilisées pour autoriser ou refuser le trafic uniquement depuis les adresses IPv4 source. La destination du paquet et les ports concernés ne sont pas évalués. 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.

Résumé du chapitre 9 (suite)

- La commande de configuration globale **access-list** définit une liste de contrôle d'accès standard avec un numéro compris entre 1 et 99 ou une liste de contrôle d'accès étendue avec des nombres compris entre 100 et 199, et 2000 et 2699. Les listes de contrôle d'accès standard et étendues peuvent être nommées.
- La commande *name* **ip access-list standard** permet de créer une liste de contrôle d'accès standard nommée, tandis que la commande *name* **ip access-list extended** permet de créer une liste de contrôle d'accès étendue. Les instructions des listes de contrôle d'accès IPv4 incluent l'utilisation des masques génériques.
- Une fois qu'une liste de contrôle d'accès est configurée, elle est associée à une interface à l'aide de la commande **ip access-group** en mode de configuration d'interface.

Résumé du chapitre 9 (suite)

- Rappelez-vous de la règle des trois P, une liste de contrôle d'accès par protocole, par direction, par interface.
- Pour supprimer une liste de contrôle d'accès d'une interface, entrez d'abord la commande **`no ip access-group`** sur l'interface, puis la commande globale **`no access-list`** pour supprimer l'ensemble de la liste.
- Les commandes **`show running-config`** et **`show access-lists`** permettent de vérifier la configuration des listes 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.

Résumé du chapitre 9 (suite)

- La commande **access-class** configurée en mode de configuration de ligne limite les connexions entrantes et sortantes entre un VTY spécifique et les adresses renseignées dans une liste de contrôle d'accès.
- Comme avec les ACL IPv4 nommées, les noms IPv6 sont alphanumériques et sensibles à la casse. Ils doivent également être uniques. Contrairement aux listes de contrôle d'accès IPv4, l'option standard ou étendue n'est pas nécessaire.
- En mode de configuration globale, utilisez la commande *name* **ipv6 access-list** pour créer une liste de contrôle d'accès IPv6. La longueur de préfixe est utilisée pour indiquer dans quelle mesure l'adresse IPv6 source ou de destination doit correspondre.
- Une fois qu'une liste de contrôle d'accès IPv6 est configurée, elle est associée à une interface à l'aide de la commande **ipv6 traffic-filter.**