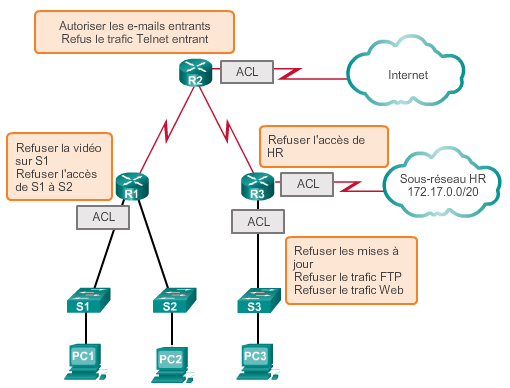
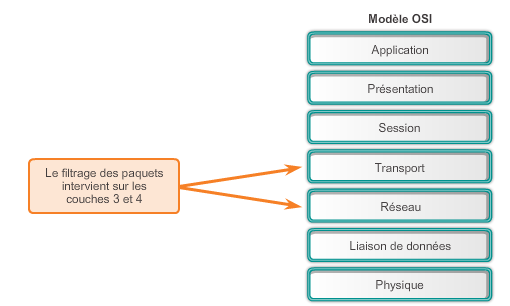
Chapitre 9 : Listes De Contrôle D'accès

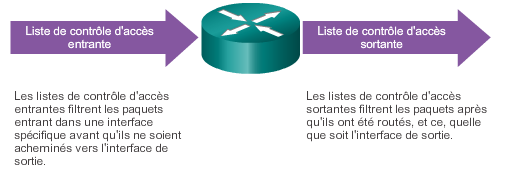
(Acess-list)

1. FONCTIONNEMENT DES LISTES DE CONTROLE D'ACCES IP
2. Objectif des listes de contrôle d'accès
3. Définition



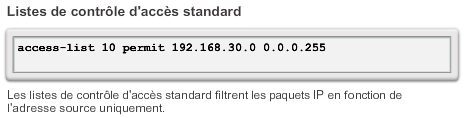
Une liste de contrôle d'accès (ou ACL) est une série de commandes IOS qui déterminent si un routeur autorise ou refuse les paquets entrants ou sortants.

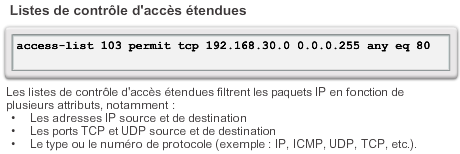
1. Filtrage des paquets
2. Listes de contrôle d’accès entrante et sortante



TP : 9.1.1.6

1. LES TYPES DES LISTES DE CONTROLE D'ACCES IPV4
2. Les types des listes de contrôle d’accès

Il existe deux types de listes de contrôle d'accès IPv4 Cisco : les listes standards et les listes étendues.



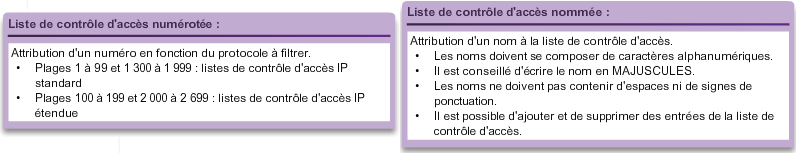
NB :

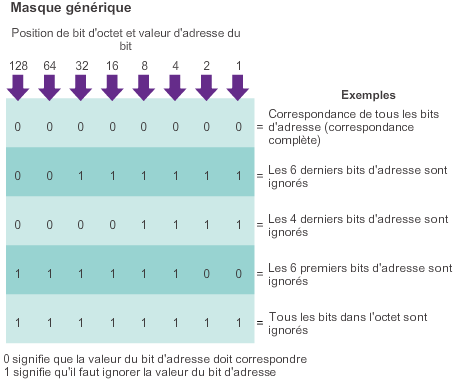
* la liste de contrôle d'accès 103 autorise tout le trafic provenant des adresses du réseau 192.168.30.0/24 à entrer sur n'importe quel réseau IPv4 si le port de destination de l'hôte est 80 (HTTP)

NB :

* La destination du paquet et les ports concernés ne sont pas évalués.
* La liste 10 autorise tout le trafic provenant du réseau 192.168.30.0/24

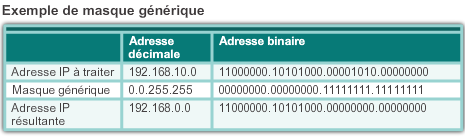
1. les listes de contrôle d’accès Numérotés et nommées

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

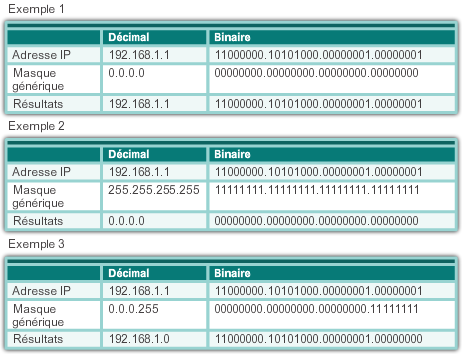
1. MASQUES GENERIQUES DANS LES LISTES DE CONTROLE D'ACCES
2. Règles

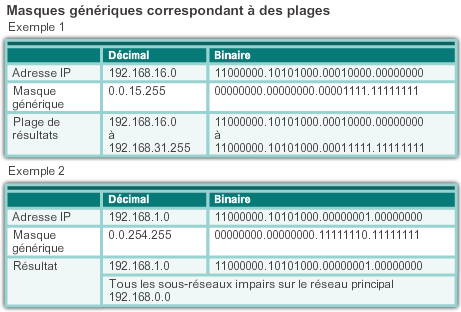
Les masques génériques respectent les règles suivantes pour faire correspondre le chiffre binaire 1 et 0 :

* 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.



1. Exemples de calcul de masque générique





1. Calcul du masque générique (Exercices)

NB :

* La méthode la plus rapide consiste à soustraire le masque de sous-réseau de 255.255.255.255.

**Exercice 1 :**

Calculer le masque générique si nous supposons que vous souhaitiez autoriser l'accès de tous les utilisateurs du réseau 192.168.3.0. Sachant que le masque de sous-réseau est 255.255.255.0 : 0.0.0.255

**Exercice 2 :**

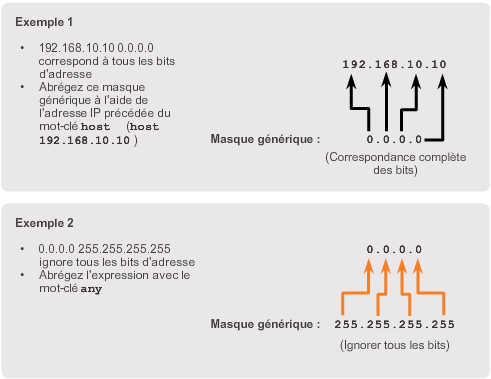
Calculer le masque générique si nous supposons que vous souhaitiez autoriser les 14 utilisateurs du sous-réseau 192.168.3.32/28 à accéder au réseau. Le masque du sous-réseau IP est 255.255.255.240 : 0.0.0.15

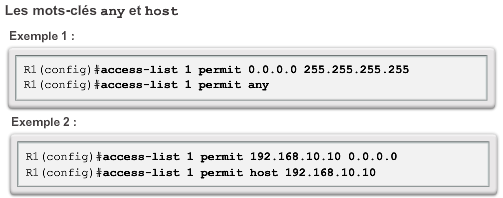
**Exercice 3 :**

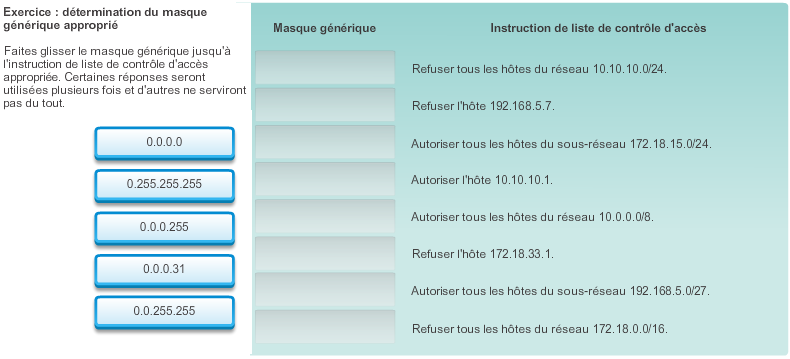
Calculer le masque générique si nous supposons que vous souhaitiez faire correspondre uniquement les réseaux 192.168.10.0 et 192.168.11.0 : 0.0.1.255

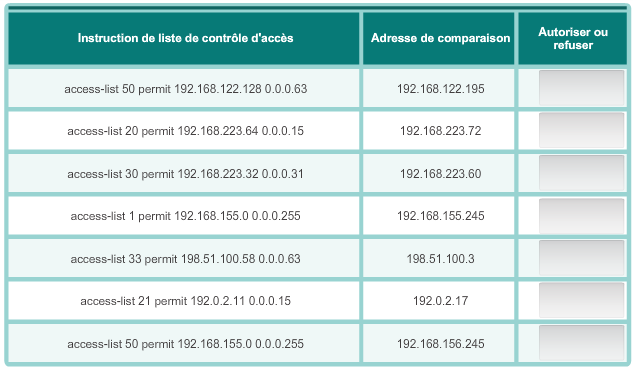
**Exercice 4 :**

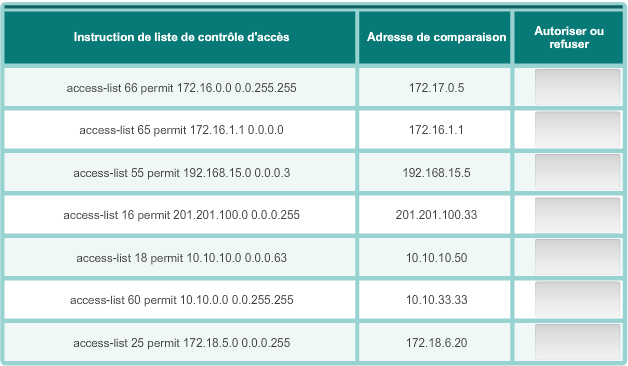
Calculer le masque générique si nous supposons que vous souhaitiez faire correspondre la plage des adresses de 192.168.16.0 à 192.168.31.0. 0.0.15.255

1. Mots-clés des bits de masque générique



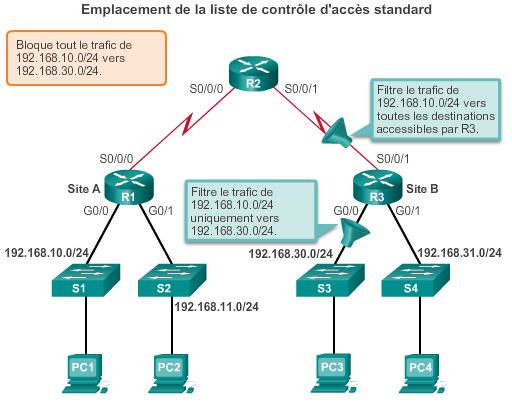
Exercice 1 **: 9.1.3.6**

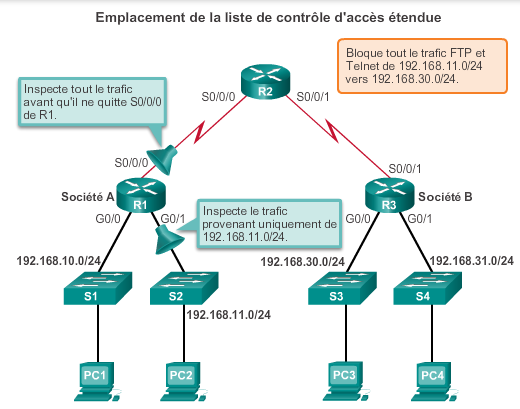
Exercice 2 : 9.1.3.7

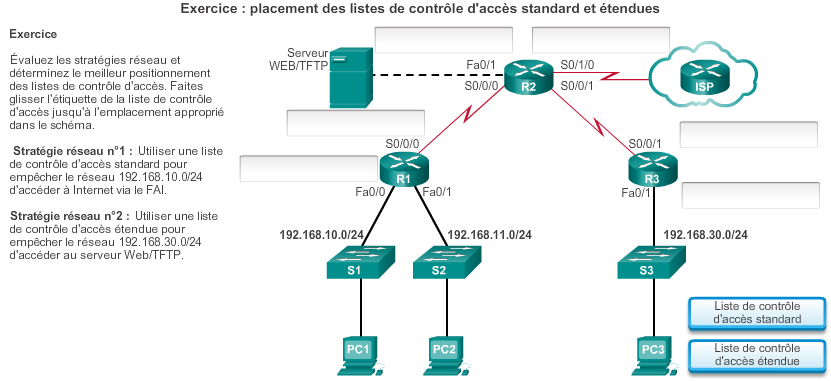
Exercice 3 :

1. Directives concernant le placement des listes de contrôle d'accès

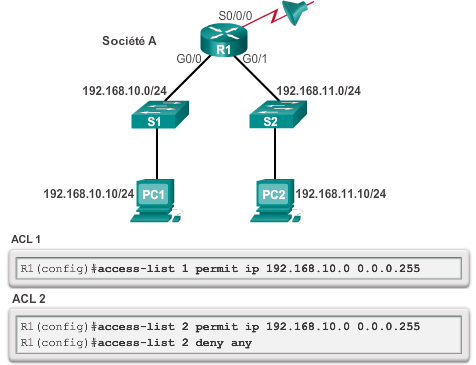
Chaque liste de contrôle d'accès doit être placée là où elle aura le plus grand impact sur les performances. Les règles de base sont les suivantes :

* 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. De cette manière, le trafic indésirable est refusé près du réseau source et ne traverse pas l'infrastructure réseau.
* 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. Le fait de placer une liste de contrôle d'accès standard à la source du trafic empêche efficacement ce trafic d'accéder à tous les autres réseaux via l'interface à laquelle la liste est appliquée.



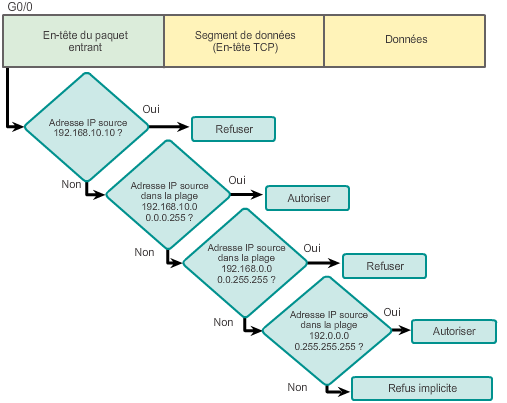
Exercice :

1. LISTES DE CONTROLE D'ACCES IPV4 STANDARD
2. Configuration des listes de contrôle d'accès IPv4 standard
3. Principe

Lorsque le trafic entre dans le routeur, il est comparé à toutes les entrées de contrôle d'accès dans l'ordre dans lequel ces entrées apparaissent dans la liste de contrôle d'accès. Le routeur continue à traiter les ACE jusqu'à ce qu'il trouve une correspondance. Le routeur traite le paquet en fonction de la première correspondance trouvée et aucune autre ACE ne sera inspectée.

Si aucune correspondance n'est trouvée, lorsque le routeur atteint la fin de la liste, le trafic est refusé. Ceci est dû au fait que, par défaut, il existe un refus implicite à la fin de toutes les listes de contrôle d'accès pour le trafic qui ne correspond à aucune entrée configurée.

1. Exemple



**access-list 2 deny 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**

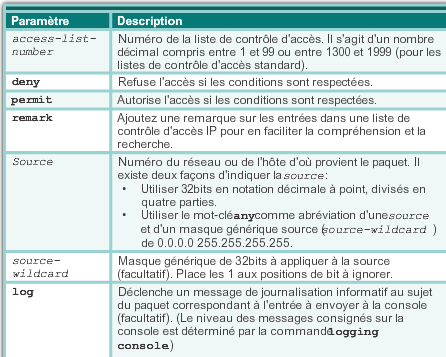
**access-list 2 permit 192.0.0.0 0.255.255.255**

1. Configuration des listes de contrôle d’accès standard IPV4

Pour utiliser des listes de contrôle d'accès standard numérotées sur un routeur Cisco, vous devez d'abord créer la liste de contrôle d'accès standard, puis l'activer sur une interface.

Syntaxe :

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



Exemples :

Autoriser une seule adresse IP (un seul hote) :

* R1(config)# access-list 10 permit host 192.168.10.10

Autoriser une plage d’adresse IP :

* R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255

Autoriser n’importe quelle adresse

* R1(config)# access-list 10 permit any

Ajouter un commentaire a une ACL

* R1(config)# access-list 10 remak cette access-list permet d’autoriser le LAN 192.168.0.0
* R1(config)# access-list 10 permit 192.168.0.0 0.0.255.255

Afficher les ACL

* R1(config)# show access-lists

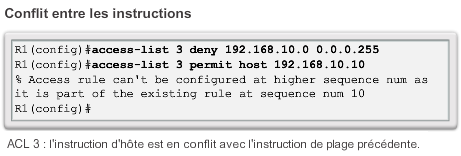
Supprimer une ACL

* R1(config)# no access-list <numero>

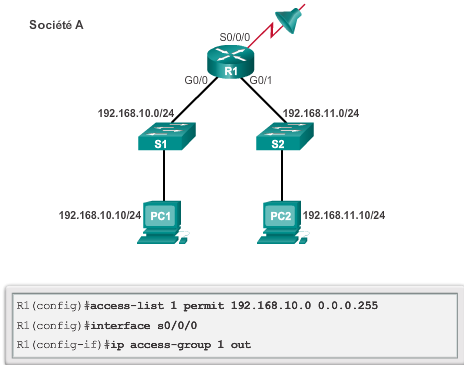
1. Logique interne

Les ACE sont traitées de manière séquentielle. Par conséquent, l'ordre dans lequel elles sont saisies est important.

EXEMPLES :



1. Application des ACL aux interfaces de routeur

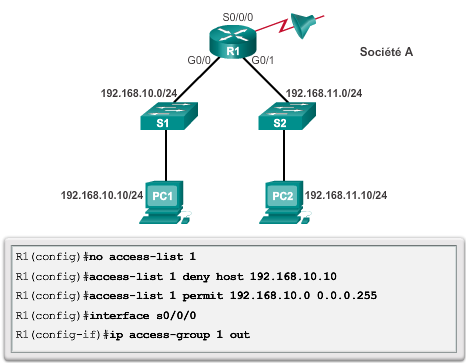
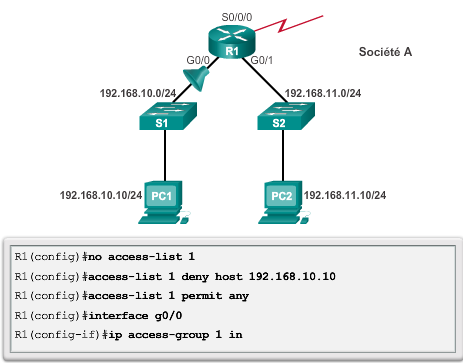
Une fois qu'une liste de contrôle d'accès standard est configurée, elle est associée à une interface à l'aide de la commande ip access-group en mode de configuration d'interface :

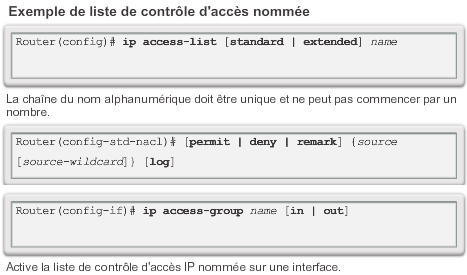
Syntaxe :

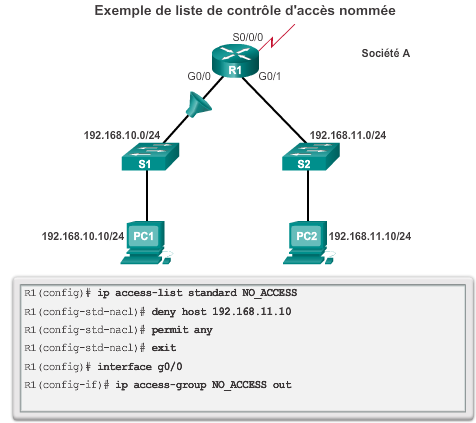
Router(config-if)# ip access-group { access-list-number | access-list-name } { in | out }

1. Exercices

Quelle est la différence entre les deux listes de contrôle d’accès.



1. Configuration des listes de contrôle d’accès nommées

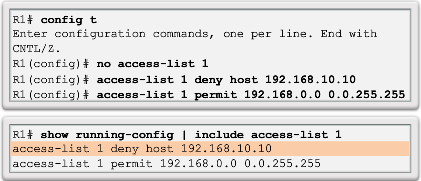


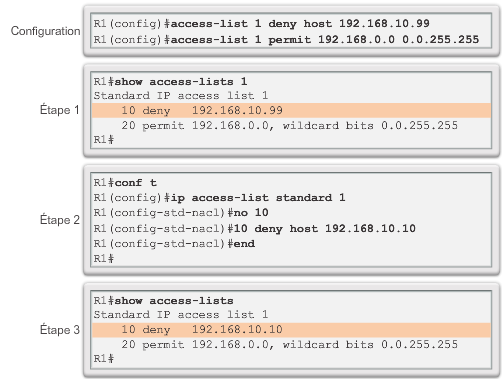
Exercice : 9.2.1.9

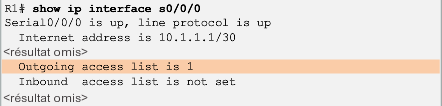
TP : 9.2.1.10

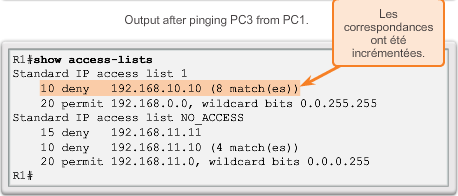
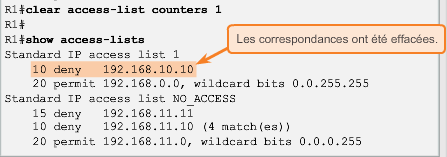
TP : 9.2.1.11

1. Modification des listes de contrôle d'accès IPv4
2. Méthode 1 : supprimer et créer



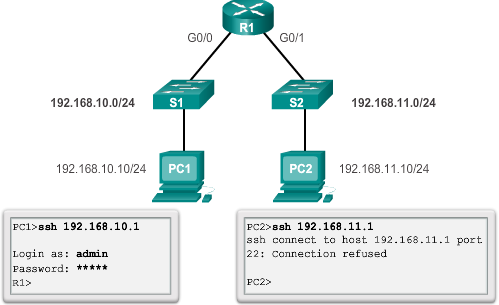
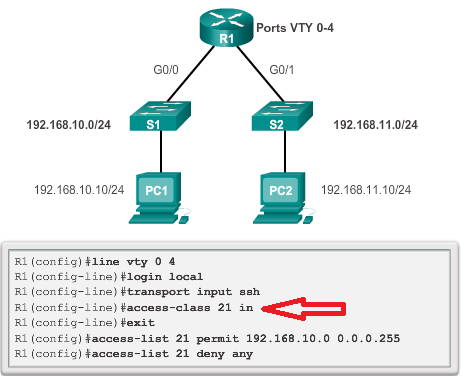
1. Méthode 2 : à l’aide de numéro d’ordre
2. Méthode 3 : Ajouter des lignes
3. Vérification des listes de contrôle d’accès



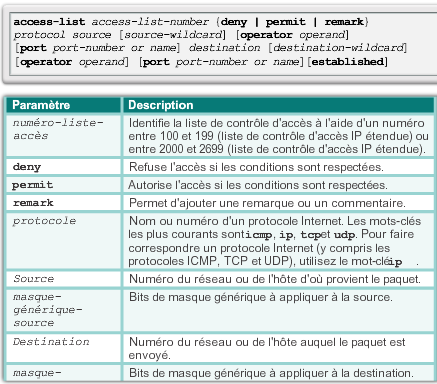
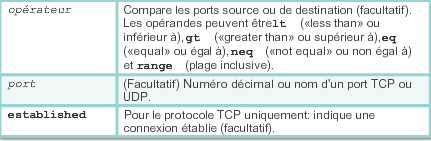
1.  Statistiques des listes de contrôle d’accès

TP : 9.2.2.7

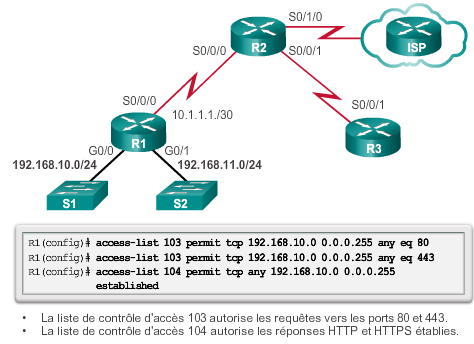
1. Sécurisation des ports VTY à l'aide d'une liste de contrôle d'accès IPv4 standard
2. Sécuriser un port VTY avec des ACL standard



TP : 9.2.3.3 / 9.2.3.4

1. LISTES DE CONTROLE D'ACCES IPV4 ETENDUES
2. Configuration des listes de contrôle d’accès étendues

Exemple :



1. Application des ACL étendues aux interfaces



EXERCICE 1  :

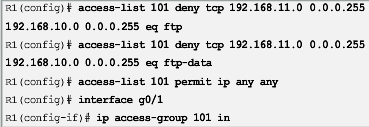
Créer une liste de contrôle d’accès étendue permettant de :

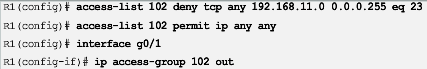
* Refuser le trafic FTP provenant de réseau 192.168.11.0 vers le réseau 192.168.10.0.
* Refuser le trafic FTP-data provenant de réseau 192.168.11.0 vers le réseau 192.168.10.0.
* Autoriser tous autres types de trafic
* Appliquer ACL a une interface.

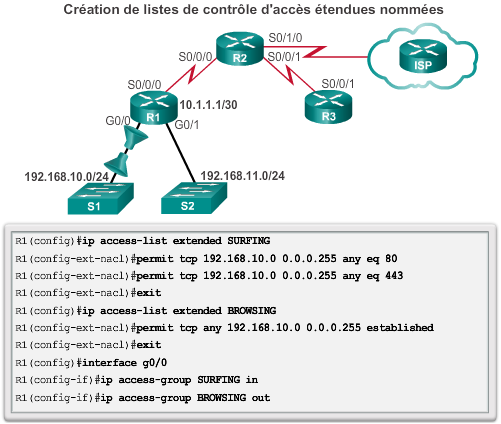
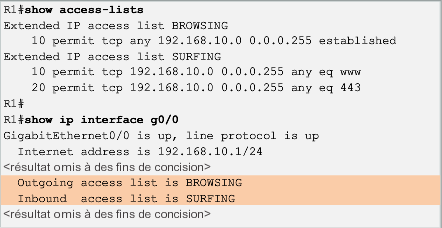
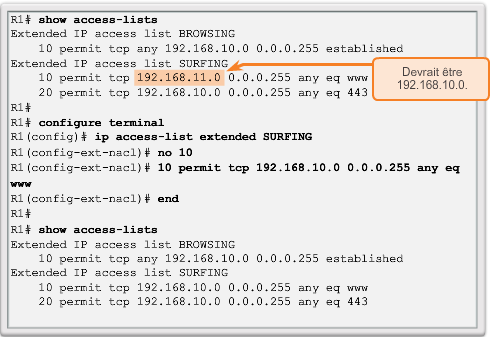
EXERCICE 2  :

Créer une liste de contrôle d’accès étendue permettant de :

* Refuser le trafic Telnet provenant de n'importe quelle source vers le réseau local 192.168.11.0/24
* Autoriser tout autre trafic IP.

Solution 1 :

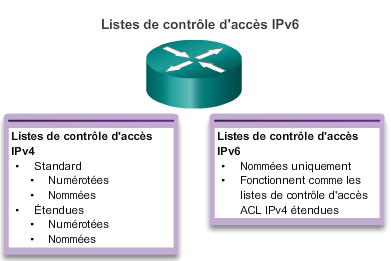
Solution 2 :

1. Création d’une liste de contrôle d’accès étendue nommée
2. Vérification d’une liste de contrôle d’accès étendue
3. Modification d’une liste de contrôle d’accès étendue

Exercices : 9.3.2.7 / 9.3.2.8 / 9.3.2.9

TP : 9.3.2.10 / 9.3.2.11 / 9.3.2.12 / 9.3.2.13

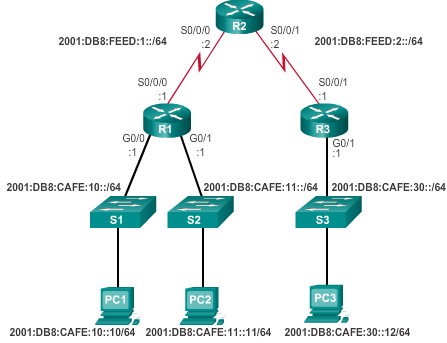
1. LISTES DE CONTROLE D'ACCES IPV6
2. Types des listes de contrôle d’accès IPV6

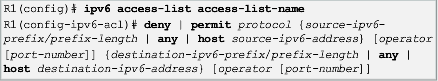
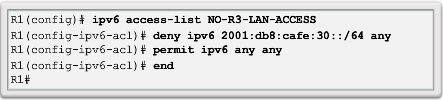


1. Comparaison ACL IPV4 et ACL IPV6

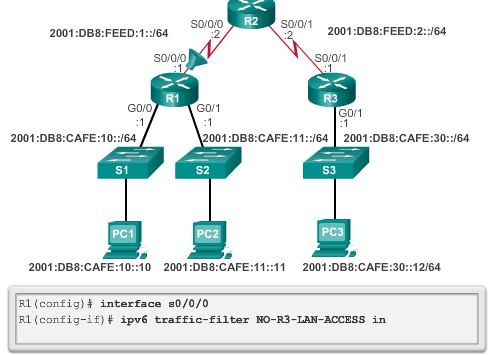
|  |  |  |
| --- | --- | --- |
|  | AcL IPV4 | ACL IP V6 |
| Application de l’ACL sur une interface de routeur | Ip access-group | ipv6 traffic-filter |
| WildCardMask | Oui | Non, il utilise la longueur de préfixe pour indiquer la correspondance. |

1. Topologie du travail



1. Configuration des listes de contrôle d'accès IPv6
2. Configuration
3. Exemples

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



Remarques :

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

**no ipv6 access-list.**

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

1. Exercices

Exercice 1 :

* Configurer avec une liste d'accès IPv6 **No-FTP-to-L1** pour refuser le trafic FTP vers 2001:DB8:CAFE:11::/64. Les ports utilisés pour les données FTP (port 20) et le contrôle FTP (port 21) doivent être bloqués.
* Sur quelle interface vous-allez appliquer la liste ?
* Appliquer l’ACL a l’interface G0/0 de R1. Quels sont les réseaux qui seront bloqués ?

Exercice 2 :

Créer une liste de contrôle d’accès IPV6 permettant de :

* d'autoriser l'accès de n'importe quel périphérique au serveur Web à l'adresse 2001:DB8:CAFE:10::10.
* Tous les autres périphériques se voient refuser l'accès au réseau 2001:DB8:CAFE:10::/64.
* PC3 sur 2001:DB8:CAFE:30::12 est autorisé à accéder via Telnet à PC2 portant l'adresse IPv6 2001:DB8:CAFE:11::11
* Tous les autres périphériques se voient refuser l'accès Telnet à PC2.
* Le reste du trafic IPv6 est autorisé vers toutes les autres destinations.
* Appliquée à l'interface G0/0 de R3 dans la direction entrante.

Réponses : voir 9.5.2.4

1. Vérification des listes de contrôle d’accès

* **Show running-config**
* **Show access-lists**
* **Show ipv6 interface <nom>**

TP : 9.5.2.6

9.5.2.7

1. Résumé : liste des ports les plus utilisés

