ACL

ACL :ACCESS CONTROL LIST

ACL : ACCESS CONTROL LIST

ACL : Access Control List

Une ACL permet de vérifier le flux traversant un routeur.

Les ACL permettent de filtrer les accès entre les différents réseaux ou de filtrer les accès au routeur lui même.

ACL : ACCESS CONTROL LIST

Les paramètres contrôlés sont:

Adresse source ,Adresse destination,Protocole utilisé,Numéro de port

Les ACLs peuvent être appliquées sur le Traffic ***entrant*** ou ***sortant***.

Les actions :

interdit (DENY) , ***autorisé (PERMIT)***

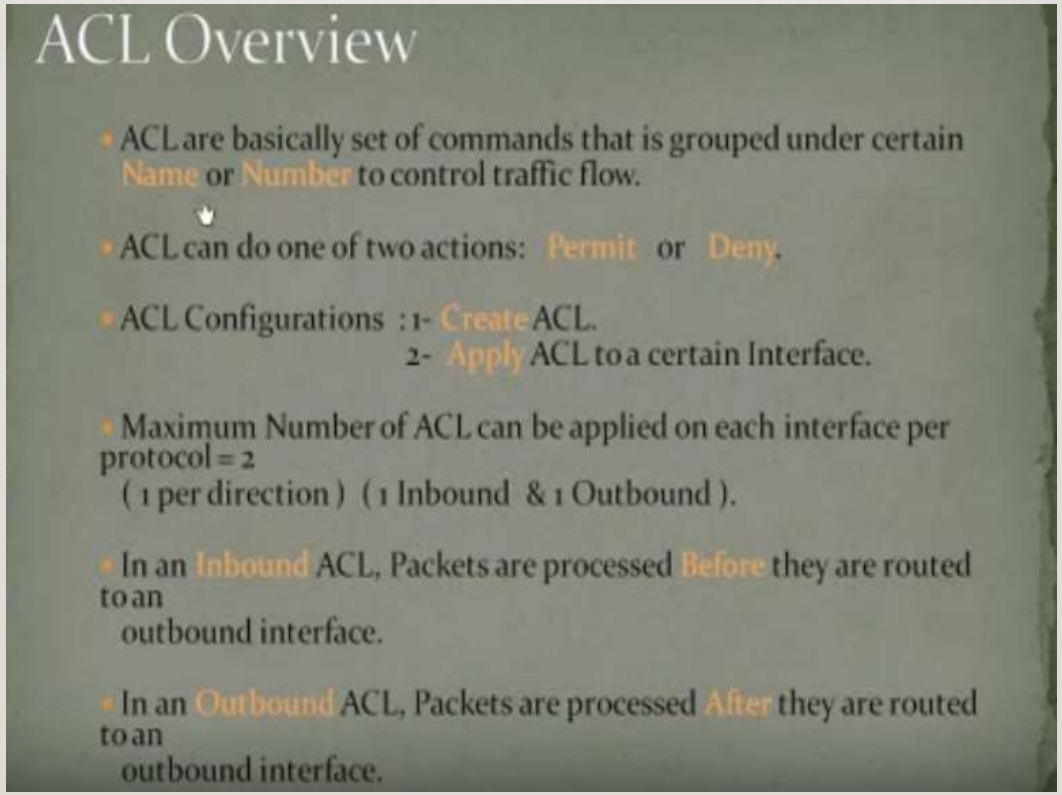
ACL

Les Acls sont prises en compte de façon séquentielle.

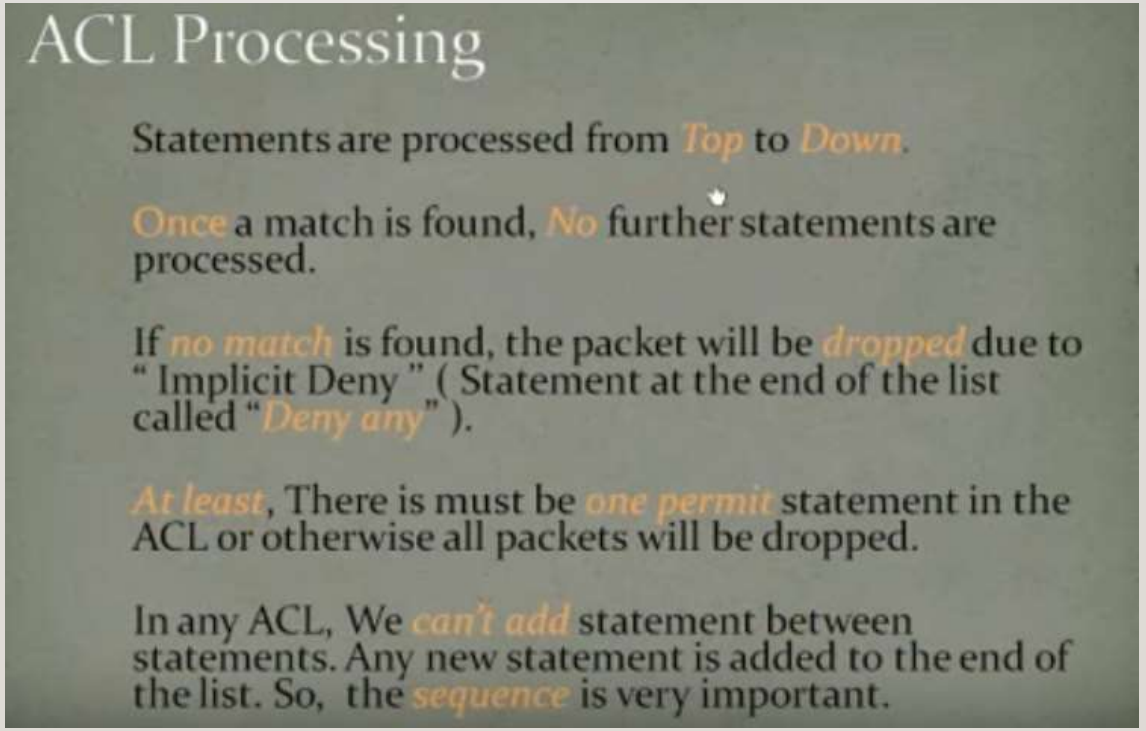
Il faut donc placer les instructions les plus précises en premier et l'instruction la plus générique en dernier.

Par défaut, tout le Traffic est interdit.

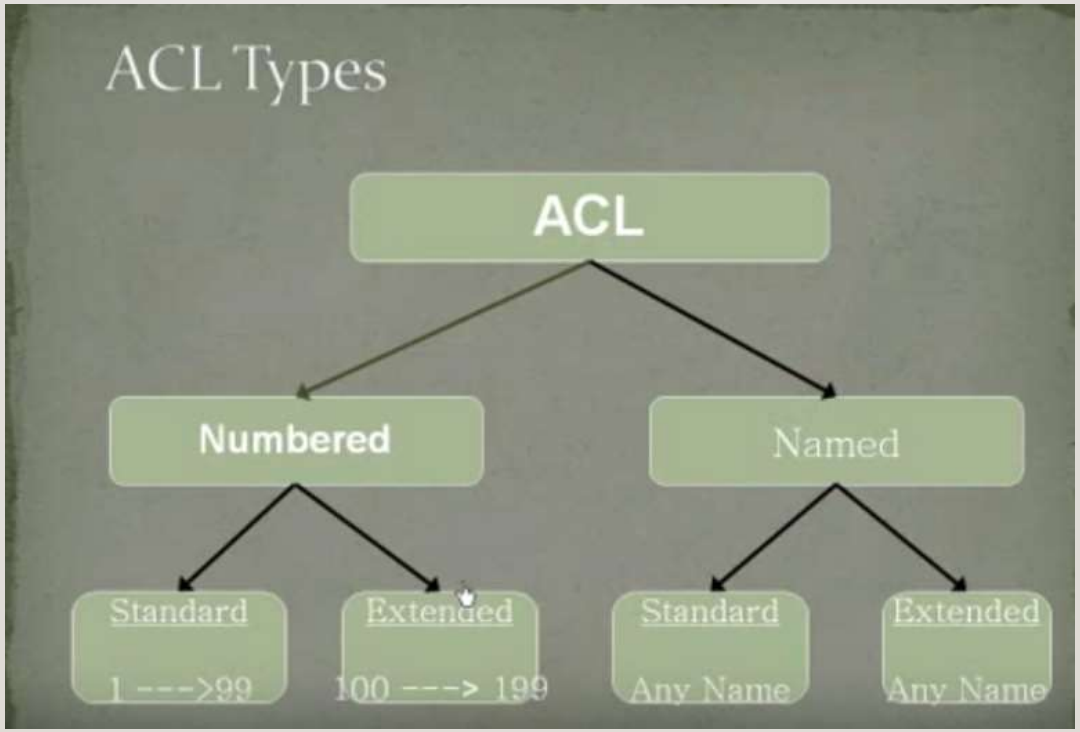
ACL


ACL Overview
• ACL are basically set of commands that is grouped under certain Name or Number to control traffic flow.
• ACL can do one of two actions: Permit or Deny.
• ACL Configurations : 1- Create ACL.
2- Apply ACL to a certain Interface.
• Maximum Number of ACL can be applied on each interface per protocol = 2
(1 per direction) (1 Inbound & 1 Outbound).
• In an Inbound ACL, Packets are processed Before they are routed to an
outbound interface.
• In an Outbound ACL, Packets are processed After they are routed to an
outbound interface.

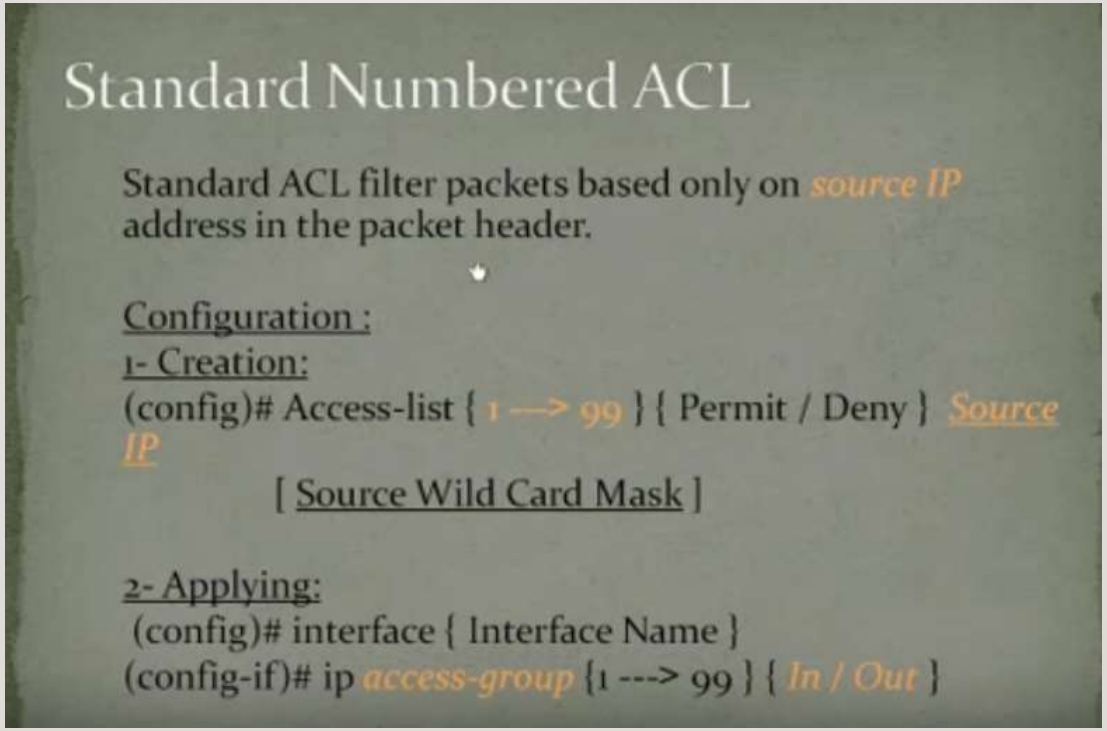
ACL


ACL Processing
Statements are processed from Top to Down.
Once a match is found, No further statements are processed.
If no match is found, the packet will be dropped due to " Implicit Deny " (Statement at the end of the list called "Deny any").
At least, There is must be one permit statement in the ACL or otherwise all packets will be dropped.
In any ACL, We can't add statement between statements. Any new statement is added to the end of the list. So, the sequence is very important.

TYPES ACL


ACL Types
ACL
Numbered
Named
Standard
1 --->99
Extended
100 ---> 199
Standard
Any Name
Extended
Any Name

ACL STANDARD



ACL STANDARD

Les ACL Standard (de 1 à 99 - 1300 à 1999)

L'ACL standard filtre uniquement sur les adresses ***IP sources.***

Elle est de la forme :
access-list numéro-de-la-liste {permit|deny} {host|source source-wildcard|any}

Le numéro de l'acl standard est compris entre 1 et 99 ou entre 1300 et 1999.

ACL STANDARD

Les ACL Standard (de 1 à 99 - 1300 à 1999)

Elles vérifient l'IP source uniquement.

Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Dans cet exemple nous créons une ACL (numéro 1) qui autorise le réseau 192.168.1.0.

Il faut saisir le ***Wildcard*** et non le masque de sous réseau.

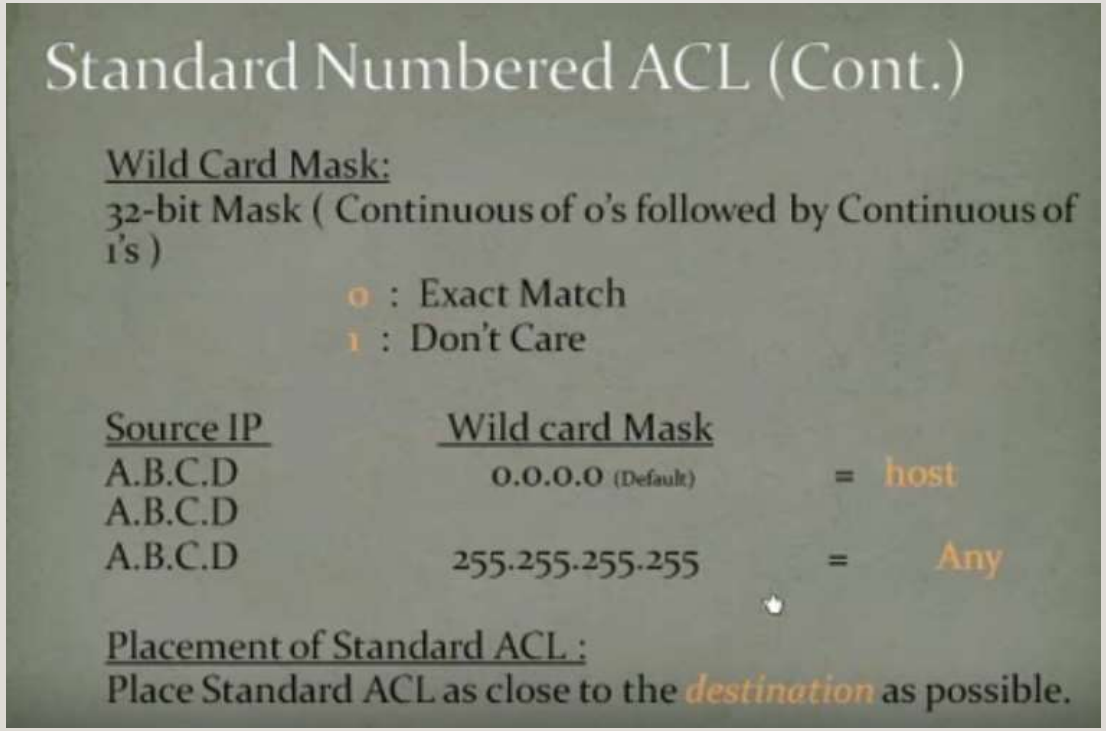
ACL STANDARD

Nous appliquons ensuite cette ACL à l'interface fa0/0 :

Router(config)#int fa0/0

Router(config-if)#ip access-group 1 out

ACL STANDARD



ACL ÉTENDUES

Les ACL étendues (de 100 à 199)

Elles vérifient ***l'IP source***, **l'IP de destination**, le **protocole**, les **ports** (pour les protocoles tcp et udp).

Elle est de la forme:

Router (config) # ***acces-list*** *choisir un numéro de* { 99 à 199 } *choisir l'action* { permit ou deny} *choisir le type de protocole* {TCP ou bien UDP} ***@de source + WildCard@source +@ de destination +WildCard de @destination + choisir entre {eq ; lt ;gt ;neq}+ numéro de port*** .

Extended Numbered ACL

It is much more flexible than Standard ACL.

Extended ACL can match on :

1- Source IP & Destination IP.

2- TCP/IP Protocols : (TCP , UDP , ICMP , IP)

3- Protocol Information : (Port Number , ICMP Message Type)

LES TYPES D'ACL

Exemples de ports utilisés fréquemment :

Nom	Protocole	Numéro port
FTP	TCP	20/21
SSH	TCP	22
Telnet	TCP	23
SMTP	TCP	25
DNS	TCP/UDP	53
TFTP	UDP	6

LES TYPES D'ACL

HTTP	TCP	80 443
POP3	TCP	110
IMAP	TCP	143

LES TYPES D'ACL

Opérateurs

égal	eq
non égal	neq
supérieur	gt
inférieur	lt

LES TYPES D'ACL

Exemples :

Le poste 192.168.0.1 a accès sans restriction au réseau 192.168.10.0/24

Router(config)#access-list 100 permit ip host 192.168.0.1 192.168.10.0 0.0.0.255

Les postes de 192.168.0.32 à 192.168.0.47 doivent avoir accès au serveur 192.168.1.200 en http

router(config)#access-list 100 permit tcp 192.168.0.32 0.0.0.15 host 192.168.1.200 eq 80

Les flux du réseau 192.168.0.0/24 doivent être bloqués vers le réseau 192.168.1.0/24

router(config)#access-list 100 deny ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255

LES TYPES D'ACL

Le réseau 192.168.0.0/24 peut accéder à tous les réseaux

router-dev(config)#access-list 100 permit ip 192.168.0.0 0.0.0.255 any

router-dev(config)#int fa0/0

router-dev(config-if)#ip access-group 100 in

LES TYPES D'ACL

Les ACL nommées

Elles sont définies par un nom plutôt que par un numéro, elles peuvent être standard ou étendues.

Router(config)#ip access-list extended test

Router(config-ext-nacl)#

LES TYPES D'ACL

ACL et connections Telnet et SSH

Autorisation de l'IP 192.168.1.1 uniquement :

router-dev(config)#access-list 2 permit host 192.168.1.1

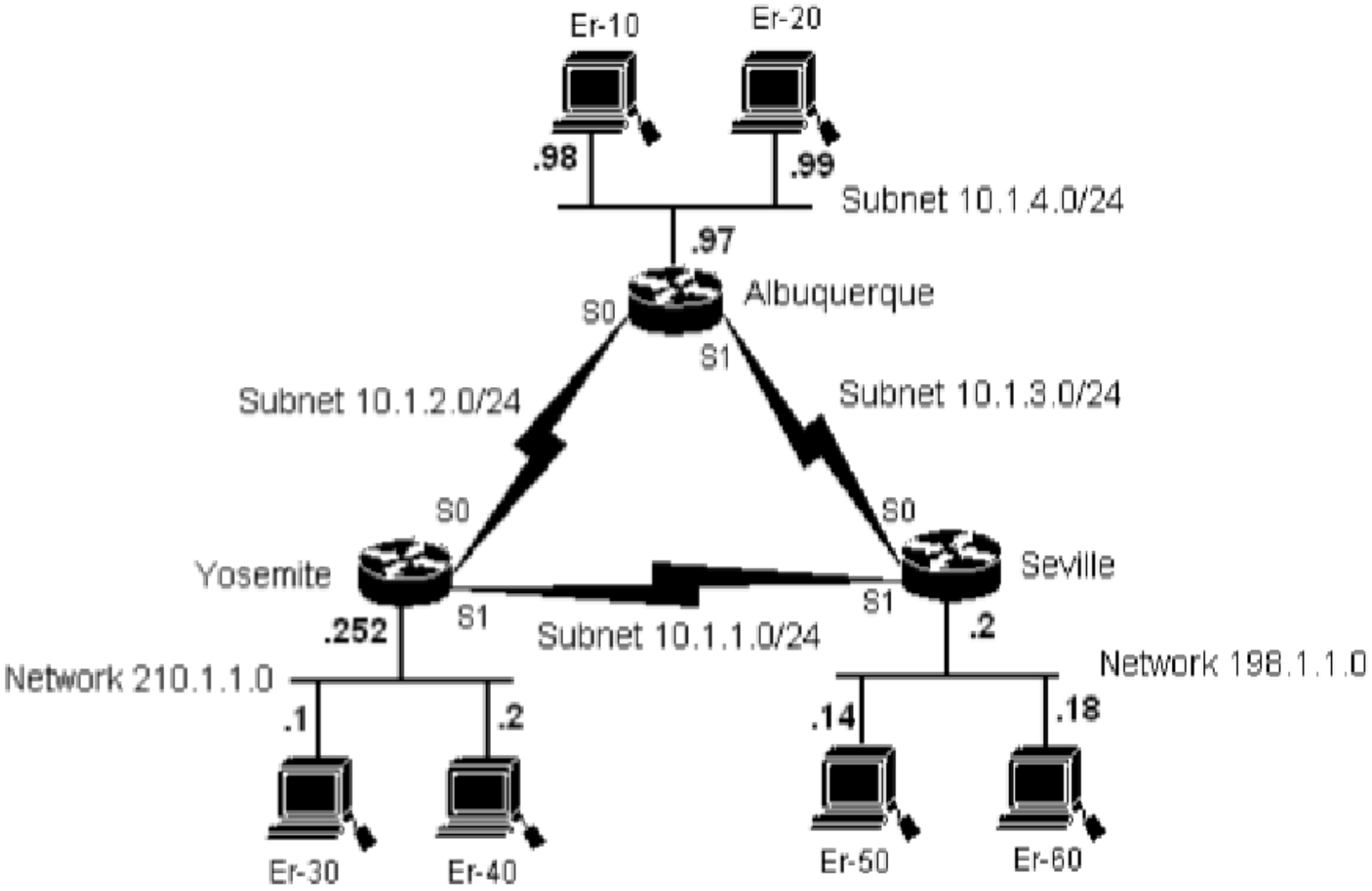
router-dev(config)#access-list 2 deny any

router-dev(config)#line vty 0 4

router-dev(config-line)#access-class 2 in

Comment appliquer les ACL?

On ***crée*** l'ACL puis ensuite on ***applique*** l'ACL à une interface en entrée ou en sortie (in ou out).
Si l'ACL doit être modifiée, il sera nécessaire de supprimer celle ci puis de la recréer entièrement.
Une façon pratique de faire est de conserver l'acl dans un fichier texte puis de faire un copier/coller.


Er-10
Er-20
.98
.99
Subnet 10.1.4.0/24
.97
Albuquerque
S0
S1
Subnet 10.1.2.0/24
Subnet 10.1.3.0/24
S0
S0
Yosemite
Seville
S1
S1
.252
.2
Subnet 10.1.1.0/24
Network 210.1.1.0
Network 198.1.1.0
.1
.2
.14
.18
Er-30
Er-40
Er-50
Er-60

SCÉNARIO 1

- Les critères de filtrage sont :
  - 1. ER-30 doit pouvoir accéder aux machines du sous-réseau de Séville.
  - 2. Toutes les autres machines du sous-réseau de Yosemite ne sont pas autorisées à accéder au sous-réseau de Séville.
  - 3. Tous les autres accès sont autorisés

SCÉNARIO 2

Les critères de filtrage sont :

1. Les machines du sous-réseau de Albuquerque ne sont pas autorisées à communiquer avec les machines du sous-réseau de Yosemite.
2. 2. Les machines ER-30 et ER-40 ne sont pas autorisées à accéder aux machines du sous réseau de Séville.
3. 3. Les autres accès entre les machines des sous-réseaux de Séville et Yosemite sont autorisés.