Conceptes bàsics sobre ACL Ampliades

1- Les **ACL ampliades** (*Access Control Lists ampliades*) són un tipus de llistes de control d'accés utilitzades principalment en xarxes (com en dispositius de Cisco) per filtrar el trànsit de manera molt més precisa que les ACL estàndard.

2- A diferència de les ACL estàndard, que només miren la IP d'origen, les ACL ampliades permeten filtrar segons diversos criteris:

- Adreça IP d'origen
- Adreça IP de destinació
- Protocol: TCP, UDP, ICMP, HTTP,….
- Ports: 80, 443, 22, etc...

3- Sintaxi general:

access-list [numero] [permit|deny] [protocol] [origen] [wildcard] [destínació] [wildcard] [port]

4- Exemple → **`access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 80`**

Aquest exemple, **permet** el trànsit que vagi dirigit al port **80/tcp** des de la xarxa **192.168.1.0** cap a **qualsevol xarxa destinació**.

5- El valors dels número identificador d'ACL ampliada vàlids són del **100** al **199**.

6- Valors típics dels paràmetres:

- Protocol: **ip**, **tcp**, **udp**, **icmp**.
- Ports: **eq**, **neq**, **gt**, **lt**, **range**. Amb **range** s'han d'indicar els valors **mínim** i **màxim**.
- origen I destínació: **any**, **host + adreça IP**, **xarxa + wildcard**

7- Ubicació prioritària: A prop de la font del trànsit per evitar càrrega innecessària a la xarxa.

8- Consideració important: Una ACL no s'aplica si la interfície està connectada a la xarxa origen del paquet.

9- Funcionament:

- S'avaluen de dalt a baix
- La primera coincidència s'aplica
- Si no hi ha coincidències, es denega el trànsit per defecte

10- Aplicacions:

- Seguretat de xarxa
- Control d'accés a serveis
- Filtrat de trànsit

11- De la mateixa manera que quan treballem amb ACL estàndard, les ACL ampliades:

- S'assignen a un interfície de xarxa.
- Cal indicar si són de tipus **in** o de tipus **out** per la interfície assignada.
- Cal indicar una opció per defecte.

12- Exemple complet d'una assignació d'ACL ampliada:

← creació de la llista →
```
Router00(config)#access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.10.0 0.0.0.255
Router00(config)#access-list 100 permit ip any any
```
← assignació de la llista a una interfície →
```
Router00(config)#int fa0/0
Router00(config-if)#ip access-group 100 in
Router00(config-if)#end
```
← comprovació de la configuració →
```
Router00#show access-list
Router00#show ip interface fastethernet0/0
```

L'assignació d'aquesta ACL **denega** l'accés a la **xarxa destinació 192.168.10.0/24** des de la **xarxa origen 192.168.1.0/24**. L'ACL s'assigna a **fa0/0** d'**entrada**. Es permet accedir des de **qualsevol** altra **adreça origen** a qualsevol altra **adreça destinació** com opció **per defecte**.

13- Exemple complet d'esborrament d'una ACL ampliada i la seva assignació a una interfície:

← esborrament de l'assignacióassignació de la llista a una interfície →
```
Router00(config)#int fa0/0
Router00(config-if)#noip access-group 100 in
Router00(config-if)#exit
```
← esborrament de la llista →
```
Router00(config)# no access-list 100
Router00(config)#exit
```
← comprovació de la configuració →
```
Router00#show access-list
Router00#show ip interface fastethernet0/0
```