Introducció a les ACLs (Llistes de control d'accés) de tipus estàndard

1- Una ACL és un filtre que col·locat al lloc adequat, controla el trànsit d'accés des de l'exterior a una xarxa o el trànsit de sortida des d'una xarxa cap a l'exterior.

2- El filtrat es pot fer en funció de l'adreça IP origen, IP destinació, Ports, protocols de nivell d'aplicació o adreces MAC. **En el cas de les ACL estàndard només s'utilitza l'adreça IP origen.**

3- Les ACLs s'apliquen a les interfícies de xarxa del router, no al router sencer.

4- Una ACL es composa d'un conjunt d'instruccions (que també es poden dir regles o entrades) que autoritzen o bloquen la sortida de / accés a de una xarxa.

5- Una entrada d'una llista d'ACL que **bloca** la sortida de / accés a una xarxa és una entrada de tipus **deny**. Una entrada d'una llista d'ACL que **permet** la sortida de / accés a una xarxa és una entrada de tipus **permit**.

6- En el moment de fer l'assignació d'una ACL a una interfície de xarxa, s'ha d'indicar si l'ACL serà de tipus **out** (sortida) o de tipus **in** (entrada).

7- Si una ACL és de tipus **out**, llavors l'ACL només s'aplica si el trànsit de dades ha arribat al router des d'una altra interfície i intenta sortir del router cap a una altra xarxa per la interfície a la qual s'ha assignat l'ACL. Els paquets entrants no són comparats amb l'ACL.

8- Si una ACL és de tipus **in**, llavors l'ACL només s'aplica si el trànsit de dades ha arribat al router des d'una altra xarxa i intenta entrar dins del router per la interfície a la qual s'ha assignat l'ACL. Els paquets sortints no són comparats amb l'ACL.

9- Una ACL necessita un número que l'identifiqui. Per ACLs estàndard ha de ser un número entre **1 i 99** o entre **1300 i 1999**.

10- Per indicar que l'entrada s'aplica a una xarxa s'haurà d'indicar la seva adreça de xarxa i una **màscara comodí** (o **wildcard mask** en anglès). Una màscara comodí és una màscara de xarxa normal però amb el bit invertits. Una màscara normal seria 255.255.255.0 i la màscara comodí seria 0.0.0.255. Així doncs, si volem crear una regla dins d'una ACL per totes els ordinadors de la xarxa 192.168.1.0/24 hauríem d'escriure 192.168.1.0 0.0.0.255.

11- Per indicar que l'entrada s'aplica a només una adreça IP en concret, la **màscara comodí** serà **0.0.0.0**. Així doncs, si volem crear una regla dins d'una ACL només per l'ordinador de la xarxa 192.168.1.10/24 hauríem d'escriure 192.168.1.0 0.0.0.0.

12- Per indicar "qualsevol xarxa" hem d'utilitzar la paraula clau **any**.

13- La llista ACL es crea sempre juntament amb la seva primera entrada.

14- Es poden afegir noves entrades a una ACL identificant-la amb el seu número identificador. Cada nova entrada queda sempre escrita darrera l'última entrada existent.

15- Per fer la configuració d'ACL sempre s'han de seguir els següents passos:

a) Creació de l'ACL amb la seva primera entrada

b) Afegir entrades a l'ACL

c) Assignar una ACL a una interfície. En el moment de fer l'assignació s'ha de dir si és de tipus **in** o **out**.

16- És important recordar novament que per realitzar el filtratge, el router utilitza l'ACL i l'adreça IP origen.

17- Les entrades es processen en seqüència. El router va comparant l'adreça IP origen amb les entrades. Si la primera entrada no concorda, llavors mira la segona, i així fins al final. Quan es troba una entrada que concorda llavor s'aplica el filtre associat. Si per exemple tenim la següent ACL:

```
deny    192.168.1.0   0.0.0.255
permit  192.168.2.0   0.0.0.255
```

Llavor, si arriba un paquet amb l'adreça IP origen 192.168.1.24, el paquet serà filtrat. Si arriba un paquet amb l'adreça IP origen 192.168.2.34 llavors, com que no concorda amb la primera entrada, es compararà amb la segona entrada. En aquest cas concorda i com que l'entrada és de tipus permit, llavors el paquet pot passar.

18- Si cap entrada no concorda llavors s'aplica la **denegació implícita** que és **deny any**, o sigui, per defecte es filtra qualsevol paquet que no concorda amb cap entrada de l'ACL. Si per exemple hem creat la següent ACL:

```
deny    192.168.1.0   0.0.0.255
permit  192.168.2.0   0.0.0.255
```

en realitat tenim aquesta ACL:

```
deny    192.168.1.0   0.0.0.255
permit  192.168.2.0   0.0.0.255
deny any
```

Si arriba un paquet amb l'adreça IP origen 192.168.4.3 llavors, com que no concorda amb cap entrada, per defecte se l'aplica l'última entrada i per tant serà filtrat, o sigui, no passarà.

19- Si volem permetre el pas de qualsevol paquet que no concordi amb les entrades anteriors llavors hauríem de crear una ACL així:

```
deny    192.168.1.0   0.0.0.255
deny    192.168.20.0   0.0.0.255
permit any
```

20- Ordre per crear una ACL:

Router(config)# access-list número_acl deny/permit adreça_ip mascara_comodí

Exemple:

Router(config)# acces-list 15 deny 192.168.20.0 0.0.0.255

Afegeix una entrada a la llista ACL número 15 denegat l'accés a qualsevol paquet que tingui com adreça IP origen una adreça qualsevol de la subxarxa 192.168.20.0/24, o sigui, qualsevol ordinador entre les adreces 192.1681.1 i 192.168.1.254.

21- Ordre per assignar una ACL a una interfície de xarxa i indicar si és de tipus in o out:
Router(config)# interface nom_interfície
Router(config-if)# ip access-group número_acl in/out
Exemple:
Router(config)# interface fastethernet0/0
Router(config-if)# ip access-group 15 out
Associa l'ACL 15 a la interficie fastethernet0/0. Només s'aplica si el trànsit de dades és de sortida, o sigui, des dins del router cap a fora.

22- Si es vol visualitzar les ACL creades s'ha d'executar:
Router#: show access-list

23- Si es vol visualitzar les ACL aplicades a una interfície i si són d'entrada o sortida s'ha d'executar:
Router#: show ip interface nom_interfíce
Per exemple:
Router#: show ip interface fastethernet0/0

24- Per esborrar una ACL associada a una interfície s'ha d'executar:
Router(config)#: interface nom_interfície
Router(config-if)#: no ip access-group número_acl in/out
Exemple:
Router(config)# interface fastethernet0/0
Router(config-if)# no ip access-group 15 out
Esborra l'ACL 15 de tipus out de la interficie fastethernet0/0.

DOCUMENTACIÓ
1- CISCO: Configuring IP Access Lists --> Standard ACLs
2- https://www.youtube.com/watch?v=SfrDdkZZCzM