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- Les ACL utilitzen **màscares 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- La paraula **any** significa qualsevol IP de qualsevol xarxa.

13- Per fer proves, descarrega ara el fitxer acl.pkt.

14- Creació d'una ACL i una entrada de tipus **out** perquè faci un **deny**:
Router(config)# acces-list 10 deny 192.168.20.0 0.0.0.255
Router(config)# acces-list 10 permit any
Router(config)# int fa0/0
Router(config-if)# ip access-group 10 out

- La primera ordre crearà una llista ACL i una entrada de la llista identificada amb el número **10** de **denegació** a qualsevol paquet que tingui com origen una IP de la xarxa **192.168.20.0/24**

- La segona ordre crea una entrada que dóna **permís** de pas a qualsevol altre paquet que vingui de qualsevol altra IP de qualsevol altra xarxa.

- L'entrada **10** de la llista ACL s'associa amb la interfície **fa0/0** i és de tipus **out**. Per tant, els paquets que vinguin de la xarxa **192.168.20.0/24 no** poden **sortir** per **fa0/0**.

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

16- Si es vol visualitzar les ACL aplicades a una **fa0/0** i comprovar si són d'entrada o sortida s'ha d'executar:
Router#: show ip interface fa0/0

17- Per eliminar l'associació de l'entrada **10** de l'ACL amb la interfície **fa0/0** executa:
Router(config)# interface fa0/0
Router(config-if)# no ip access-group 10 out

18- Per eliminar completament l'entrada **10** de l'ACL executa:
Router(config)# no acces-list 10

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