ACL Quick Guide

Example:

R1#access-list 100 deny tcp 10.10.30.0 0.0.0.255 gt 49151 10.10.20.1 0.0.0.0 eq 23

Example:

R1#access-list 1 deny 10.10.10.10 0.0.0.0 – Decline the specific host

R1#access-list 1 permit 10.10.10.0 0.0.0.255 – Allow all other hosts on 10.10.10.0 network

***Note:** We use 0.0.0.0 for specific host such as 10.10.10.10 or we can use 0.0.0.255 to specify a range of IP addresses such as 10.10.10.0

Quick commands:

R1#ip access-list?

R1#show access-list 100

Named ACL Example:

R1#ip access-list standard Flackbox-demo

R1#deny 10.10.10.10 0.0.0.0

R1#permit 10.10.10.0 0.0.0.255

Example:

R1#access-list 100 deny tcp 10.10.10.10 0.0.0.255 10.10.50.0 0.0.0.255 eq 80

***Note:** Wildcards save you typing out the wildcard mask

These examples mean the same thing:

R1#access-list 100 permit tcp 10.10.10.10 0.0.0.0 **is the same as**

R1#access-list 100 permit tcp host 10.10.10.10

R1#access-list 100 permit tcp 0.0.0.0 255.255.255.255 **is the same as**

R1#access-list 100 permit tcp any

Injecting ACES in existing ACL:

R1#ip access-list extended 100

R1#15 deny tcp host 10.10.10.11 host 10.10.50.10 eq telnet

Standard ACL example:

R1#access-list 1 deny 10.0.2.0 0.0.0.255

R1#access-list 1 permit 10.0.1.0 0.0.0.255

R1#int f0/0

R1#ip access-group 1 out (apply ACL 1 on outbound interface)

Extended ACL example:

R1#access-list 100 permit tcp host 10.0.1.10 host 10.0.0.2 eq telnet

R1#access-list 100 deny tcp 10.0.1.0 0.0.0.255 host 10.0.0.2 eq telnet

R1#access-list 100 permit ip any any

R1#ip access-group 100 in