ACL

Las ACL estándar son guiones de configuración del router que controlan si un router acepta o rechaza paquetes según la dirección de origen.

R1(config)#**access-list 10 deny 192.168.10.0 0.0.0.255**

R1(config)#**access-list 10 permit any**

R1(config)#**interface fa0/1**

R1(config-if)#**ip access-group 10 out**

R3(config)#**ip access-list standard NO\_ACCESS**

R3(config-std-nacl)#**deny host 192.168.30.128**

R3(config-std-nacl)#**permit any**

R3(config)#**interface fa0/0**

R3(config-if)#**ip access-group NO\_ACCESS in**

Las ACL extendidas son guiones de configuración del router que controlan si un router acepta o rechaza paquetes según la dirección de origen o destino y protocolos o puertos. Las ACL extendidas proporcionan mayor flexibilidad y especificidad que las ACL estándar.

* Para la red 192.168.10.0/24, bloquee el acceso Telnet a todas las ubicaciones y el acceso TFTP al servidor Web/TFTP corporativo en 192.168.20.254. Se permite todo el acceso restante.

R1(config)#**access-list 110 deny tcp 192.168.10.0 0.0.0.255 any eq telnet**

R1(config)#**access-list 110 deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp**

R1(config)#**access-list 110 permit ip any any**

La primera sentencia bloquea el acceso de la 192.168.30.0/24 a todas las direcciones en la red 192.168.30.0/24.

R3(config)#**access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255**

* Los hosts externos pueden establecer una sesión de Web con el servidor Web interno únicamente en el puerto 80.
* Se permiten únicamente las sesiones TCP establecidas.
* Las respuestas de ping se permiten a través de R2

.

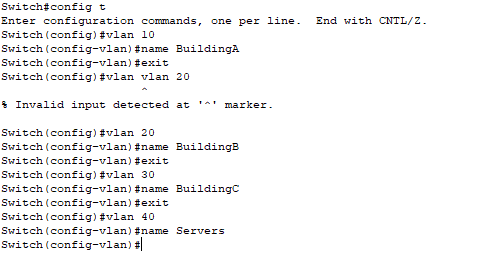
R2(config-ext-nacl)#**permit tcp any host 192.168.20.254 eq www**

R2(config-ext-nacl)#**permit tcp any any established**

R2(config-ext-nacl)#**permit icmp any any echo-reply**

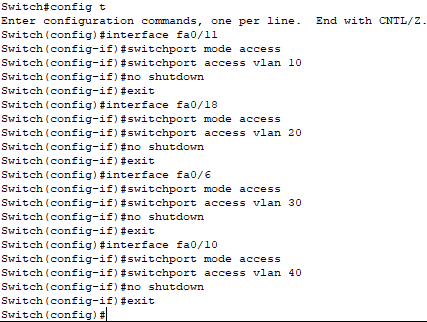
R2(config-ext-nacl)#**deny ip any any**

VLAN



Which command will only display the VLAN name, status, and associated ports on a switch?

**# show vlan brief**



Comandos

comando show cdp neighbors detail

VPN

R1(config)# license boot module c2900 technology-package securityk9

R1(config)# end

R1# copy running-config startup-config

R1# reload

Configurar acl

R1(config)# crypto isakmp policy 10

R1(config-isakmp)# encryption aes

R1(config-isakmp)# authentication pre-share

R1(config-isakmp)# group 2

R1(config-isakmp)# exit

R1(config)# crypto isakmp key escom address 10.2.2.2

R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac

R1(config)# crypto map VPN-MAP 10 ipsec-isakmp

R1(config-crypto-map)# description VPN connection to R3

R1(config-crypto-map)# set peer 10.2.2.2

R1(config-crypto-map)# set transform-set VPN-SET

R1(config-crypto-map)# match address 110

R1(config-crypto-map)# exit

R1(config)# interface S0/0/0

R1(config-if)# crypto map VPN-MAP

R1# show crypto ipsec sa

NAT

ip nat pool NAT1 209.165.76.196 209.165.76.199 netmask 255.255.255.252

ip nat inside source list 1 pool NAT1

ip classless

ip route 0.0.0.0 0.0.0.0 Serial0/0/0

ip route 172.16.0.0 255.255.0.0 Serial0/0/1

ip nat pool R2POOL 209.165.76.195 209.165.76.223 netmask 255.255.255.224

ip nat inside source list 101 pool R2POOL

ip classless

ip route 10.0.0.0 255.0.0.0 10.4.1.2

ip route 0.0.0.0 0.0.0.0 209.165.76.193