-Núcleo

Núcleo de la red

-Distribución

Politicas de red

Politicas de seguridad

Firewall

-Acceso

Donde se conectan los usuarios

-ip default-gateway 192.168.1.1

Establece la puerta de enlace

-Interface range fastethernet 0/1-10

Modo de configuracion para rango de puertos

-speed 100/1000/auto

Establece la velocidaddelpuerto

-duplex full/half/auto

Establece el modo duplex

-mdix auto

Configura el modo mdix

-erase startup-config

Borra configuración de respaldo

-init\_flash

-load\_helper

-dir flash:

-rename flash:config.textflash:config.old

Procedimientopararesetear password. Switch catalyst

-show mac-address-table

Muestra table CAM

-switchport mode Access

Establece el modo de acceso para los puertos

-switchport port-security

Configurarseguridad

-switchport port-security maximum 1

Establecelimite de 1 direccion MAC

-switchport port-security mac-address sticky

Establece la primera dereccion MAC que se conecte como valida

-switchport port-security mac-address 0000.0000.0000

Establece la MAC valida

-switchport port-security violation shutdown

Se apaga la interfaz si se conecta una MAC diferente

-switchport mode access

Establece modo de acceso para usuarios

-switchport acces vlan 5

Configura la interfaz dentro de la vlan 5

-switchport mode trunk

Establece modo troncal

-switchport trunk native vlan 99

Configura la interfaz dentro de la vlan nativa 99

-switchport trunk allowed vlan 10

Configura el puerto troncal para transportar tramas de una o mas vlans

-router rip

-version 2

-network 10.0.0.0

-network 192.168.1.0

Establecer el protocol de enrutamiento rip para 10.0.0.0 192.168.1.0

-terminal length

Parametro para limitar las lines del comando show, con 0 muestra el comando completo

-show history

Historial de comandos

-interface f0/0.10

Crea una interface virtual

-encapsulation dot1q 10

Establece encapsulación 802.1q para la vlan 10 y establece lavlan 10 para la interfaz f0/0.10

-Ipv6 ospf 10 area 0

Configura el protocolo ospf v3 dentro de una interfaz dada

-ipdhcpexcluded-address 10.0.10.1 10.0.10.15

Excluye 15 direcciones de la asignación de dhcp

-ipdhcp pool diez

Crea un pool de direcciones con nombre diez

-network 10.0.10.0 255.255.255.0

Configura la red 10.0.10.0

-default-router 10.0.10.1

Establece el servidor de dhcp

-dns-server 10.0.15.10

Establece el servidor dns

-iphelper-address 192.168.1.2

Desvia broadcast a la dirección 192.168.1.2

-ipv6 rip rip-as enable

Habilita el protocolo rip ipv6 en la interfaz

-show ipv6 protocols

Muestra los protocolos ipv6

-show ipv6 route

Muestra las rutas ipv6

-router ospf 10

Modo de configuración para el protocolo ospf. Proceso 10.

-router-id 1.1.1.1

Establece el router id a 1.1.1.1. el mayor será DR.

-network 10.1.2.0 0.0.0.255 area 0

Configura la red en el área 0

-show ip ospf interface

Muestra datos de ospf para las interfaces

-domain-name Server.com

Configura el nombre de dominio Server.com

-ipv6 nd other-config-flag

-ipv6 dhcp Server version6a

**ACL**

**Estandar**

-access-list 1 deny 10.0.10.0 0.0.0.255

-access-list 1 permit any

Deniega el trafico de la red 10.0.10.0

-interaface f0/0

-ip access-group 1 out

Configura la acces list 1 en la interfaz

-no ip access-group 1 out

-no access-list 1

**Extendida**

-access-list 100 permit tcp 10.0.30.0 0.0.0.255 host 10.0.20.100 eq 80

Permite trafico de 10.0.30.0 al host 10.0.20.100 por el Puerto 80

-access-list 100 deny ip 10.0.30.0 0.0.0.255 10.0.20.0 0.0.0.255

Deniega trafico ip hacia 10.0.20.0

-access-list 100 permit ip any any

Permite trafico ip desde cualquier origin a cualquier destino

-interface f0/0

-ip access-group 100 in

Configura la access list 100 en la interfaz con direccion de entrada

-access-list 100 permit icmp 10.0.20.0 0.0.0.255 any echo

Permite icmp desde 10.0.20.0 a cualquier destino

-access-list 100 permit icmp 10.0.20.0 0.0.0.255 any echo reply

Permite respuesta icmp desde 10.0.20.0 a cualquier destino

**Nombrada**

-ip access-list extended noentre

-permit tcp 172.16.10.0 0.0.0.255 host 192.168.1.50 eq 80

-permit tcp 172.16.20.0 0.0.0.255 host 192.168.1.50 eq 80

-deny icmp 172.16.0.0 0.0.255.255 192.168.1.0 0.0.0.255 echo

-permit ip 172.16.0.0 0.0.255.255 192.168.1.0 0.0.0.255

-ip access-group noentre out

-access-list 1 permit 172.16.10.0 0.0.0.255

-access-list 1 deny 172.16.20.0 0.0.0.255

-line vty 0 4

-password cisco

-login

-access class 1 in

**NAT**

**Estatica**

-ip nat inside source static 172.16.12.10 199.9.9.9

Configura NAT estatico

-interface f0/0

-ip nat inside

Establece NAT interno en la interfaz

-ip nat outside

Establece NAT externo en la interfaz del isp

-show ip nat translation

Muestra la tabla de NAT

**Dinamica**

-access-list 1 permit 172.16.12.0 0.0.0.255

-access-list 1 permit 172.16.18.0 0.0.0.255

-ip nat pool jueves 200.0.0.1 200.0.0.4 netmask 255.255.255.248

Crea el pool NAT

-ip nat inside source list 1 pool jueves

-clear ip nat translation \*

Borra la tabla NAT

**Con sobrecarga**

-access-list 1 permit 172.16.12.0 0.0.0.255

-access-list 1 permit 172.16.18.0 0.0.0.255

-ip nat inside source list 1 interface s3/0 overload

-interface f0/0

-ip nat inside

-ip nat outside