

CONFIGURACION BÁSICA DE UN ROUTER Y UN SWITCH

NOTA:

Todo en el modo de configuración global

- configure terminal

Nombre del Host

- Hostname nombre

Línea de consola

- line console 0
password cisco
login

Línea de consola

- line vty 0 4 (router) 0 15 (switch)
password cisco
login
end

Contraseña modo privilegiado

- enable password cisco

Contraseña secreta

- enable secret class

Passwords encriptados

- Service password-encryption (cifrado en MD5)

Banner

- Banner motd %"ACCESO RESTRINGIDO"%

CONFIGURACIÓN DE UN ROUTER

Desactivar la búsqueda DNS

- no ip domain-lookup

Configurar FastEthernet

- interface fastethernet 0/0
ip address 192.168.1.1 255.255.255.0
no shutdown

Configurar Serial

- interface serial 0/0/0
ip address 192.168.2.1 255.255.255.0
clock rate 64000 (en caso de ser DCE)
no shutdown

Configurar direccion loopback

- interface loopback 0
ip address 209.165.200.1 255.255.255.224
(no se levantan porque son virtuales)

Definir rutas estáticas

- ip route **192.168.1.0** 255.255.255.0 **192.168.2.1**
192.168.1.0 (Red que quiero conocer, donde quiero llegar (fastethernet))
192.168.2.1 (Siguiendo el salto, IP del serial del otro router por el cual debo pasar o la interfaz de salida de mi router, es decir en el que estoy **Serial 0/0**)

Definir ruta por defecto

- ip route 0.0.0.0 0.0.0.0 209.165.200.226 (todos los paquetes destinados a redes que **NO** se encuentren en la tabla de enrutamiento son enviados al router especificado, en este caso la serial)
-

DHCP

- dhcp excluded-address 192.168.1.1 (IP fa del router)
ip dhcp pool INTERNAL (nombre del pool)
network 192.168.1.0 255.255.255.0 (declarar la red completa)
domain-name abc-xyz-widgets.inc
default-router 192.168.1.1 (interfaz de salida)
 - Show ip dhcp binding (muestra asignación DHCP en el router)
-

RIP

- router rip
versión 2
network 192.168.1.0 (Redes directamente conectadas)
network 192.168.2.0
-

NAT

Primero ha que crear la lista de control de acceso, para indicar las direcciones que se quieren traducir

- Access-list 1 permit 192.168.1.0 0.0.0.25
Luego NAT
 - Ip nat inside source list 1 interface serial 0/0 overload
Por último aplicar NAT a las interfaces internas y externas
 - Interface serial 0/0
Ip nat outside
Exit
 - Interface fastethernet 0/0
Ip nat inside
Exit
 - Show ip nat translation (verifica la traducción NAT)
-

ACL

Siempre se ubican lo más cerca de destino

Las acl estándar solo pueden filtrar el tráfico de la dirección Ip de origen

Se configura IN: cuando es en mi propia LAN (fasth etehrnet). OUT cuando es externo, fuera de mi LAN, otro router, ISP(serial)

- Access-list 1 permit 192.168.200.10 (host conectado a otro router)
Access-list 1 permit 192.168.100.1 (router vecino, sino se agrega no recibe actualizaciones de él)
Access-list 1 deny any
(permite el acceso de un solo host a una red, deniega el resto)
Luego de crearla hay que asignarla a un puerto específico
- Interface serial 0/0/0
Ip access-group 1 in

- Show Access-list (verifica las acls creadas)
- Clear ip access-list counters (borra los contadores de Acl)

Acl extendida (Lab 8.3.4)

- Router 2
- access-list 101 permit ip host 192.168.1.10 host 192.168.5.10 (el host 1 tiene acceso al host 3)
- access-list 101 deny ip 192.168.1.0 0.0.0.255 host 192.168.5.10
- access-list 101 permit ip any any
- access-list 101 deny ip any any
- interface fa 0/0
- ip access-group 101 out
- Router 1
- access-list 101 permit ip host 192.168.5.10 host 192.168.15.1
- access-list 101 permit ip host 192.168.5.10 host 192.168.1.1
- access-list 101 deny ip any host 192.168.15.1
- access-list 101 deny ip any host 192.168.1.1
- access-list 101 permit ip any any
- access-list 101 deny ip any any
- interface fa 0/0
- ip access-group 101 in
- interface s 0/0/0
- ip access-group 101 in

Denegar Telnet a una porción de red

- access-list 101 deny tcp 172.16.2.0 0.0.0.255 any eq telnet (deniega el acceso a telnet a toda la red)

Configuración EIGRP

- router eigrp 100
- network 10.0.0.0 (Todas las redes conectadas al router, en este caso no se declara wildcard mask porque se declara la red completa, pero si es una porción de red si es necesario)
- network 192.168.125.4 0.0.0.3 (solo cuatro host iniciando en el 4, 5, 6 y 7)
- **NOTA:** el wildcard mask es la resta de la máscara de 32 bits menos la máscara de la red especificada.

$$\begin{array}{r} 255.255.255.255 \\ -255.255.255.252 \\ \hline 0.0.0.3 \end{array}$$
- Show ip protocols (muestra los elementos básicos del protocolo de enrutamiento)
- Show ip route (muestra la tabla de enrutamiento)
- Show interface (muestra la configuración de la interface especificada ya sea serial o fast-ethernet)

Modificar ancho de banda de las interfaces seriales

- Interface serial 0/0/0
- Bandwidth 64 (1024) (no es un cambio a nivel físico, sino a nivel lógico; independiente de la conexión que se tenga, debe mantenerse en los dos extremos. La idea es que el flujo de datos sea más eficiente)
- Show ip eigrp topology (visualiza la tabla de topología de eigrp)

Desactiva el resumen automático de EIGRP

- Router eigrp 1

- No auto-summary

Autenticación MD5

- key chain discchain
key 1
key-string san-fran
end
 - confi te
interface serial0/1/1
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 discchain
(repita para todos los routers en todas las interfaces necesarias).
-

OSPF

- router ospf 1
- network 172.16.1.16 0.0.0.15 area 0
- network 192.168.10.1 0.0.0.15 area 0

Para definir prioridad

- interface fa0/0
- ip ospf priority 25 (El número mas alto de la mas alta prioridad)
- end

CONFIGURACIÓN DE UN SWITCH

Configuración de la interfaz para la VLAN 1

- interface vlan 1 (solo la nativa tiene IP)
ip address 192.168.1.2 255.255.255.0
no shutdown
exit
- ip default-gateway 192.168.1.1
end

Creación de VLAN

- vlan 10 (así sucesivamente ejemplo: vlan 20, vlan 30)
name Faculty
exit

Asignar interfaces dentro de una Vlan, por ejemplo la Fa5 y Fa6

- interface fa0/5
switchport mode access
switchport access vlan 10
exit

- interface fa0/6
switchport mode access
switchport access vlan 10
- exit

Definir MAC estática en una interfaz del switch.

- mac-address-table static ooeo.2917.1884 vlan 1 interface fastethernet 0/4

Para verificar los resultados

- show mac-address-table

Permitir que el puerto del switch fastethernet 0/4 acepte solo un dispositivo (seguridad del puerto)

- interface fastethernet 0/4
switchport mode access
switchport port-security
switchport port-security mac-address sticky

Para verificar la seguridad del puerto

- show port-security

Para que establezca en 1 el conteo máximo de MAC de seguridad de puerto

- interface fastethernet 0/4
- switchport port-security maximum 1

En caso de que se produzca una violación de seguridad la interface debe desconectarse.

- Switchport port-security violation shutdown

Para deshabilitar los puertos que no se utilicen

- interface range fastethernet0/5 – 24
- shutdown
- interface range gigabitethernet0/1 – 2
- shutdown

Para establecer la prioridad de un switch sobre otro

- spanning-tree vlan 1 priority 4096
- exit

Configuración de un enlace troncal

Primero en el router

- interface fa0/0
no shutdown
interface fa0/0.1
encapsulation dot1q 1
ip address 172.168.1.1 255.255.255.0 (la ip de red la la vlan en el switch)
exit

- interface fa0/0,10
encapsulation dot1q 10
ip address 172.16.10.1 255.255.255.0
exit
- interface fa0/0,20
encapsulation dot1q 20
ip address 172.16.20.1 255.255.255.0
end

Luego se definen las vlan con un nombre cada una
Definir los puertos a las vlan

- interface fa0/5
switchport mode access
switchport access vlan 10
exit

Luego al puerto fa0/6 a la vlan 10 y así sucesivamente a los puertos y vlan que se requieran

Definir el enlace troncal entre el switch1 y el switch2

- Switch1(config) # int fa0/1
Switch1(config-if) # switchport mode trunk
Switch1(config-if) # exit

Definir el enlace troncal entre el switch1 y el Router

- Switch1(config) # int fa0/2
Switch1(config-if) # switchport mode trunk
Switch1(config-if) # end

Configurar el VTP en el Switch 1

- Switch1(config) # vtp domain Group1
- Switch1(config) # vtp mode server (en el switch1 como server y cliente en el switch 2)

Luego se repite todo igual en el Switch 2, el trunk fa(conectado al otro switch y el vtp mode client)