**Configuración inicial de SW:** (aquellos que tienen de hojas a las PCs y otros SW)

1. Conectar los cables correspondientes, con los otros dispositivos (PC y ROUT)
   1. SW a PC => Negro (directo)
   2. SW a ROU => Negro punteado (Cruzado)
2. Cambiar el nombre
3. Asignar una clave
4. Activar Telnet con clave
5. Asignar las IP correspondientes.
6. Crear las VLANS y asignarles un nombre
7. **Puertos conectados a PC**
   1. Asignar las VLANS que correspondan (depende de cada PC)
   2. Configurar los puertos como Mode Access
   3. Configurarlos en modo TRUNK
8. **Puertos conectados a SW**
   1. Configurarlos en modo TRUNK
9. **Puertos conectados a Routers**
   1. Configurarlos en modo TRUNK

**#En los SW, NO se asignan IP de las PC conectadas**

**Configuración inicial de ROUTER**

1. Cambiar el nombre
2. Asignar una clave
3. Activar Telnet con clave
4. **Puertos conectados SW**
   1. Crear tanta sub-interfaces como VLANS tenga en los switches
   2. Configurar cada sub-interfaces en modo de “encapsultation do1q Nro\_VLAN”
   3. Asignar a cada sub-interface la dirección IP + 1 (primer host de la red) de la sub-red con la correspondiente máscara (depende si es /24, /26, etc.)
   4. Con la interfaces que tenga sub-interfaces, solo debo levantarla (no shutdonw)
5. **Puertos conectados ROUTERS**
   1. Asignar IP
   2. Asignar modo de encapsulamiento (PPP)
   3. Asignar Clock rate (solo cuándo tengo el reloj)

**1 – Cambiar el “Host Name” y habilitar el telnet**

Enable

Config t

Hostname REMOTO

Enable secret utn

Line vty 0 1

Password cisco

Login

exit

**2- Habilitar las interfaces en los SW y RO**

Enable

Config t

Int f0/1

No shutdown

Exit

**Apagar interfaces**

Enable

Config t

interface range f0/1-10

shutdown

**3 – En los ROU asignar direcciones de IP Fast Ethernet (a un SW u otro ROU)**

Enable

Config t

Int f0/1

Ip address [IP] [Mascara]

No shutdwon

Exit

**4 – Asignar en los ROU las direcciones de IP Seriales (a otro ROU)**

Enable

Config t

Int se0/1/0

Encapsulation ppp

**Clock rate 14800**

Ip address 132.248.204.1 255.255.0.0

No shutdwon

Exit

*# Ese número de CLOCK si conecto 2 o mas routers*

**Comando generales**

Show running-config

Show interface

Show Ip route

telnet 192.168.1.100

**Crear las VLAS (aplica para el Switch)**

Enable

Config t

Vlan 10

Name GERENCIA

Exit

Vlan 20

Name VENTAS

Exit

Vlan 30

Name LOGISTICA

Exit

**SW- Asignar las VLANS a los puertos (cuándo quiero que una pc sea parte de una vlan)**

Enable

Config t

Interface FX/X

Switch port mode Access

Switch port Access vlan XX

**Verificar VLANs asignadas a los puertos:**

show vlan brief

**Para que se vean las vlans**

1. Voy a crear las VLANs 10 (101) y 20 (102) en SW1 => Una para cada PC. Los puertos se ponen en modo ACCESS
2. Voy a crear las VLANs 10 (201) y 20 (202) en SW2=> Una para cada PC. Los puertos se ponen en modo ACCESS
3. Si no creo las vlans en el switch superior, no se van a ver. Para que se puedan ver deben tener creadas (por lo menos) las VLANs, no hace falta asignar los puertos. En caso de asignarlos, los puertos deben estar en modo TRUNK (puertos que permite el pasaje de trama entre vlans)

**Puertos del SW en modo TRUNK (necesario si quiero que las vlans se vean, pero debe hacerse en el puerto que conecta el SW con el Router)**

Enable

Config t

Int fX/Y

Switchport mode trunk

End

Copy run start

**En Router – Configurar tantas sub-interfaces como vlans haya creado. Estas se deben crear en el puerto que está conectado con el SW.**

Enable

Int fa0/0. 1 *[2, 3, etc]*

IP address 192.168.0.1 255.255.255.0 *[IP de cada Gateway de red de cada VLAN]*

Encapsulation dot1q 10 *[Número de la vlan, podría ser 10 o 20]*

Not shutdown

**Configurar interfaces para MAC**

switch-100(config)#interface f0/1

switch-100(config-if)#switchport mode access

switch-100(config-if)#switchport port-security

switch-100(config-if)#switchport port-security maximum 1

switch-100(config-if)#switchport port-security mac-address 00D0.FF8B.2C7E

switch-100(config-if)# switchport port-security violation shutdown

**Bridging - Configurar Spanning-Tree (para diferente vlans al mismo tiempo). Comando a ejecutar en el switch que deseo que sea el root.**

*Switch1(config)# spanning-tree vlan* 1,10,20 root

**Configurar LACP**

***Se hace en los switch de principal, el que se conecta al router***

*Switch1(config)# port-channel load-balance* dst-mac

***Se hace en los*** *switchs* ***del 2do nivel***

*Switch1(config)# port-channel load-balance* src-mac

**Ahora, creo un grupo para cada ramificación que tiene el switch principal. Recordar repetir la configuración en los switchs de las ramificaciones, pero en este caso solamente tendrá 1 grupo que será el asignado por el pricipal**

-

*Switch1(config)# interface gigabitethernet* **1/1**

*Switch1(config-if)# switchport mode* **trunk**

*Switch1(config-if)# channel-protocol* **LACP**

*Switch1(config-if)# channel-group* **1 o 2** *mode active*

*Switch1(config-if)# exit*

**Configuración de equipos**

1. Asignar la IP estática
2. Asingar la mascara de sub red
3. Asignar el default Gateway, que debe ser la IP del Router (NO del SW)
4. Probar Telnet: Telnet 192.168.1.33 (pruebo conectar remotamente al router/switch para administrarlo)
5. Probar telnet anidado: Telnet 192.168.1.33 y cuándo me dé la conexión OK (me daré cuenta cuándo me cambie el nombre en la línea de comando) pues vuelvo a ejecutar Telnet 192.168.2.33

**Configuración del enrutamiento dinámico**

**Opción 1**

1) Desde el modo de configuración global ingrese:

remotox(config)# ***router rip***

remotox(config-router)# ***version 2***

remotox(config-router)# ***network w.x.y.z* (1)**

remotox(config-router)# ***exit***

*(1) w.x.y.z es la dirección de red correspondiente a las IP de las interfaces asociadas el router. Debo ingresarlas a todas y cada una de ellas.*

*# Lo que estoy haciendo acá es que los routers conozcan a sus routers vecinos cuales son las redes que tienen / conocen. Esto permitiría la comunicación entre redes (ahora tengo IP entre las redes que no se veían, por ejemplo desde la PC2 a PC3). El principal problema es que si agrego una nueva red, deberá hacerla conocida en todos los vecinos.*

2) Desactive en las LAN remotas el tráfico generado por RIP para evitar las publicaciones **RIP** en dichas redes

remotox(config-router)#***passive-interface fastEthernet 0/0***

*Con este comando a la interfaz marcada no se le envían las actualizaciones del RIP desde el Router. Se utiliza cuando en la interfaz marcada no hay otro Router conectados (hay una pc o un Switch).*

**Opción 2**

3) remotox(config)# i***p route 192.168.1.0 255.255.252.0 fastEthernet 0/0***

La idea es agregar una red que engoble a todas las otras redes conectadas al router, para ello tengo que:

1. Identificar las redes y ordenarlas de mayor a menor
2. Convertirlas a Binario
3. Sumarizar las redes (ADN) => Solo pongo 1 cuándo todos son 1, el resto 0
4. El resultado el la red genérica que tengo que agregar

**Configurar enrutamiento dinámico – EIGRP**

Routers:

Enable

Config t

Router eigrp 1

Network 192.168.10.0 [IP\_Ethernet de los swithch (s)] 0.0.0.255 [White cap]

Network 10.0.0.2 [IP\_SERIAL de los Router (s)] 0.0.0.255 [White cap]

Passive interface Fa0/0 => LAN

No auto-summary

**Configurando el ancho de banda del EIGRP**

Router(config-if)# ip bandwidth-percent eigrp *percent*

**Configurar encriptación de tunel VPN**

**Extremo B**

config t

crypto isakmp policy 10

encr AES

authentication pre-share

group 5 (Diffie-Hellman grupo 5 – clave de 1536 bits)

lifetime 3600 (tiempo de vida en segundos)

exit

**Definición de una clave simétrica con el otro extremo del túnel:**

Router2(config)#crypto isakmp key cisco address 10.1.0.1

Router2(config)#crypto isakmp key cisco address 10.4.0.1

**Configuración de IPSec modo túnel**

Router2(config)#crypto ipsec transform-set SETRouter2 esp-aes 256 esp-sha-hmac

**Configurar el mapa que determina la IP del extremo remoto del túnel y el tráfico de interés que será encapsulado.**

crypto map mymap 10 ipsec-isakmp

set peer 10.1.0.1

set security-association lifetime seconds 1800

set transform-set SETRouter2

match address 101

**Spanning-tree**

spanning-tree mode pvst

**Activar el tunel**

interface Serial0/0/0

ip address 10.2.0.2 255.255.255.0

crypto map mymap 10

**ACL – Access- lists . Lista permitida de acceso. Las uso cuándo quiero que solamente ciertos equipos puedan acceder a una web segura (un server por ejemplo)**

* **Equipo A se quiere conectar al server B**
* **El server B debe tener activado el HTTP y HTTPS**

access-list 101 permit ip 10.4.0.0 0.0.255.255 10.10.0.0 0.0.255.255  **=> Lado B**

access-list 101 permit ip 10.10.0.0 0.0.255.255 10.4.0.0 0.0.255.255  **=> Lado A**

**ACTIVAR TUNEL**

**Router 1**

**fa0/0 => 10.10.0.1 => 255.255.255.252**

**Se0/0 => 10.1.0.1 => 255.255.255.252**

**Router 3 \_ Origen**

**Fa0/0.88 => 192.168.1.129 255.255.255.192**

**Se0/1/0 => 50.3.0.1 255.255.255.192**

**Router 5\_Detino**

**Fa0/1 => 192.168.111.1 255.255.255.0**

**Se0/1/0 => 50.4.0.2 255.255.255.192**

**Access list:**

***Router3#show access-lists***

***Extended IP access list 110***

***10 permit tcp 192.168.1.1 0.0.0.192 192.168.111.1 0.0.0.255***

***20 permit ip 192.168.1.1 0.0.0.192 192.168.111. 1 0.0.0.255***

**Router 2**

**fa0/0 => 10.4.0.1 => 255.255.255.252**

**Se0/0 => 10.2.0.2 => 255.255.255.252**

**En router ORIGEN**

Router#show access-lists

Extended IP access list 100

10 permit tcp 10.10.0.0 0.0.255.255 10.4.0.0 0.0.255.255

20 deny tcp 10.20.0.0 0.0.255.255 10.4.0.0 0.0.255.255

30 deny tcp 10.50.0.0 0.0.255.255 10.4.0.0 0.0.255.255

40 permit ip 10.10.0.0 0.0.0.255 10.4.0.0 0.0.0.255

Extended IP access list 110

10 permit ip 10.10.0.0 0.0.0.255 10.4.0.0 0.0.0.255

Router#config t

Router(config)#crypto isakmp policy 10

Router(config-isakmp)#encryption aes

Router(config-isakmp)#authentication pre-share

Router(config-isakmp)#group 2

Router(config-isakmp)#exit

Router(config)#crypto isakmp key cisco address 10.2.0.2=> *Salida S0/0 Destino 50.4.0.2*

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

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

Router(config-crypto-map)#description VPN connection to R2

Router(config-crypto-map)#set peer 10.2.0.2

Router(config-cryp to-map)#set transform-set VPN-SET

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

Router(config-crypto-map)#exit

Router(config)#interface s0/0/1

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

\*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON

**En router DESTINO**

Router2(config)#access-list 100 permit tcp 10.4.0.0 0.0.0.255 10.10.0.0 0.0.0.255

Router2(config)#exit

Router2#show access-lists

Extended IP access list 101

10 permit ip 10.4.0.0 0.0.0.255 10.0.0.0 0.0.0.255

20 permit ip 10.4.0.0 0.0.255.255 10.10.0.0 0.0.255.255

Extended IP access list 100

10 permit tcp 10.4.0.0 0.0.0.255 10.10.0.0 0.0.0.255

20 permit ip 10.4.0.0 0.0.0.25 5 10.10.0.0 0.0.0.255

Extended IP access list 110

10 permit ip 10.4.0.0 0.0.0.255 10.10.0.0 0.0.0.255

Router2#config t

Router2(config)#crypto isakmp policy 10

Router2(config-isakmp)#encryption aes

Router2(config-isakmp)#authentication pre-share

Router2(config-isakmp)#group 2

Router2(config-isakmp)#exit

Router2(config)#crypto isakmp key cisco address 10.1.0.1 50.3.0.1

A pre-shared key for address mask 10.1.0.1 255.255.255.255 already exists!

Router2(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac

Router2(config)#crypto map VPN-MAP 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

Router2(config-crypto-map)#description VPN connection to R1

Router2(config-crypto-map)#set peer 10.1.0.1

Router2(config-crypto-map)#set transform-set VPN-SET

Router2(config-crypto-map)#match address 110

Router2(config-crypto-map)#exit

Router2(config)#interface s0/0/0

Router2(config-if)#crypto map VPN-MAP

\*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON