- enable (comando que te permite cambiar al modo privilegiado)
- show running-config (comando para ver la configuración del router)
- configure terminal (pasas al modo de configuración global)
- hostname (cambiar el nombre del host)

contraseña para el modo privilegiado

- enable password (class)
- enable secret (class)

contraseña consola

- line console 0
- password (cisco)
- login

contraseña a las líneas virtuales

- line vty (depende si es route o switch) (si es route se pone de 0 4 y si es switch de 0 15)
- password (cisco)
- login

interfaces

- interface (nombre de la interfaz: s0/0/0, s0/0/1, g0/0 o g0/1 si es switch es vlan1)
- ip address (ip y mascara)
- no shutdown (levantar la red)
- description (descripción de la red)
- clock rate 64000 (solo se le pone al router que tenga la interfaz s0/0/0)

enrutamiento con rip (dinamico)

- route rip
- versión (solo si se requiere la versión 2)
- network (ID)
- no auto-summary
- Passive-interface (poner pasivas las interfaces en este caso serían las g0/0, g0/1 o Loopback)
- No route rip (en caso de querer eliminar rip)

enrutamiento con rip (estático)

- ip route (ID, Mascara, ip por donde va a salir)
- no ip route (ID, mascara, ip por donde va a salir) (comando por si te equivocas)

- no ip domain lookup (desactivar búsqueda del DNS)
- service password-encryption (poner todas las contraseñas encriptadas)
- banner motd #mensaje# (mensaje del dia)
- show ip route (ver las tablas de enrutamiento)
- show interfaces (para ver las direcciones mac en este caso sería con g0/0 o g0/1)
- netstat -r (tablas de enrutamiento en pc)
- show ip arp (comando para ver las tablas ARP)
- arp-a (comando para ver las tablas ARP en pc)
- show cdp neighbors (para ver a los vecinos)
- cdp run/enable (para activar cdp neighbors)
- no cdp run (desactivar cdp)
- show protocols (para ver si las interfaces están activas)
- show ip protocols (verificar el protocolo)
- show ip interface brief (para ver si las interfaces están activadas o desactivadas y ver sus estados)
- telnet (dirección ip) (para hacer conexiones remotas)
- tracert (dirección ip) (para ver las rutas)
- trace (dirección ip) (comando desde el route)

SSH

- ip domain-name(dominio)
- ip ssh versión 2
- crypto key generate rsa (1024)
- username (usuario) secret (contraseña)
- line vty 0 4 o 0 15 (depende si es router o switch)
- transport input ssh
- login local
- ssh -l (usario) (ip) **Comando para la computadora**
- show ssh
- show ip ssh

VLAN

Crear VLAN en el switch

- Vlan (ID de la vlan)
- Name (nombre)

Configura puerto de accesos VLAN (solo en los switches que tengan pc conectadas)

- Interface (la interfaz)
- switchport mode access
- switchport Access vlan (el ID de la vlan que corresponde)

Configuracion de enlaces troncales de la VLAN (Solo a los enlaces que se conectan entre switch, incluyendo la g0/0 o g0/1)

- interface (la interfaz)
- switchport mode trunk
- switchport trunk native vlan (ID de la vlan nativa)
- switchport trunk allowed vlan (ID de todas las vlan hasta de la nativa)

show vlan brief

show interface trunk

Hacer subinterfaces

- interface (la gigabit.vlan, ejemplo=g0/0.10)
- encapsulation dot1q (vlan)
- ip address (ip+mascara)
- no shutdown
- description (Descripción)
- Entrar a interfaz de la gigabit y darle (no shutdown)

Crear VLAN en el switch

- interface vlan (ID de la vlan)
- ip address (ip+mascara)
- no shutdown

ip default-gateway (ip) (**en modo de configuración)**

ISP (Proveedor de internet)

- Configurar la interfaz en los dos router el ISP y que esta conectado a el.
- Después Ip route 0.0.0.0 0.0.0.0 (ip por donde va a salir) (esto se le hace a los dos router al ISP y al que esta conectado a el)
- Si hacemos enrutamiento estático se deja asi como ya habíamos mencionado, pero para enrutamiento dinámico se le configura lo siguiente (solo en el otro router no en el ISP):
- Router rip
- Versión 2
- Default-information originate

ISP IPV6

- Ipv6 route ::/0 (ip por donde va a salir) (esto se le hace a los dos router al ISP y al que está conectado a él)

Configuración de un Switch de capa 3

se configura igual como un router

ip routing (se levanta de capa 2 a capa 3)

- no switchport (para enrutar cuando se conecta a un router)
- ip address
- no shutdown

Árbol de expansión

show spanning-tree vlan 1 (para saber que switch hará la función de árbol de expansión)

Antes de poner los comandos de seguridad del switch tenemos que poner

- switchport mode access (dentro de la interfaz)

Seguridad en los Switch

- interface (pondré la fastEthetnet que le pondremos seguridad)
- switchport port-security

Limitaciones de direcciones MAC

- interface (pondré la fastEthetnet que le pondremos seguridad)
- switchport port-security mac-address (dirección MAC de queremos delimitar)

Configurar como se debe responder el switch cuando se produce una violación de seguridad en un puerto que tiene habilitado la seguridad

- interface (pondré la fastEthetnet que le pondremos seguridad)
- switchport port-security violation shutdown

DHCP

Crear POOL

- ip dhcp excluded-address (ip las cuales vamos a excluir, se recomienda la .1 y .la .9)
- ip dhcp excluded-address (la última dirección la .254)
- ip dhcp pool LAN-POOL- (número de pool)
- network (id de la red junto con su mascara)
- default-router (en este caso sería la .1)
- dns-server (pondremos la dirección que le asignamos al servidor) (opcional si es que contamos con un servidor)
- domain-name (nombre del dominio) (opcional si contamos con un dominio)
- exit

show running-config | section dhcp
show ip dhcp binding

ipconfig /release (borra dirección ip en PC)
ipconfig /renew (te pone otra vez la dirección ip en PC)

ip helper-address (para hacer agente de retransmisión)

- interface (g0/0/0, g0/0 dependiendo por donde va a entrar)
- ip helper-address (ip del servidor)
- exit

IPV6

ipv6 unicast-routing (Para configurar direcciones ipv6 en el router, se pone antes de configurar ipv6)

OSPF

- Router ospf (poner un numero entre el 1 y el 65.535)
- Network (ID de las redes que estan conectada directamente, wildcard, área (numero))

Configurarlo por interfaz

- Interface (g0/0, g0/1)
- ip ospf (poner un numero entre el 1 y el 65.535) y área (numero)

Para la dirección de Loopback

- interface loopback (número de loopback)
- ip address (ip y mascara)

Poner router ID (DR)

- router ospf (poner un numero entre el 1 y el 65.535)
- router-id (ip)

Poner pasivas las interfaces

- router ospf (poner un numero entre el 1 y el 65.535)
- passive-interface (puede ser g0/0, g0/1 o looback 0)

Comando por si cambiamos de router ID o nos equivocamos para que vuelva a calcular

- clear ip ospf process (se pone en modo privilegiado)

show ip protocols
show ip ospf
show ip route ospf
show ip ospf interface (g0/0, g0/1) (para ver cuales los routers Cisco eligen DR y BDR en las interfaces Ethernet)

Tabla de Topología

- show ip ospf database

Tabla de vecinos

- show ip ospf neighbor

Lista de Control de Acceso

Numeradas

Estándar

- access-list (número va del 1 al 99) (deny,permit,remark) host (ip)

Extendida

- access-list (número va de 100 al 199), (deny,permit,remark), (protocolo) host (ip) host (ip) eq (número de puerto o nombre)

Nota: en vez de poner “host” Podemos poner la id de la red junto con su mascara de wildcard por ejemplo:

access-list 101 deny tcp 83.2.0.0 0.0.255.255 any eq 443
access-list 101 permit ip any any

Ejemplo:
access-list 102 permit tcp host 50.0.144.10 host 50.0.128.10 eq 80

access-list 100 remark HOLA
access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp

Nombradas

- Ip access-list (standard o extended) (nombre en mayúsculas)
- (permit o deny) (protocolo) (ip) (mascara de wilcard) host (ip)

Ejemplo:
ip access-list extended HTTP_ONLY
permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
deny tcp host 172.31.1.101 host 64.101.255.254 eq 80

Poner la lista de control de acceso en una interfaz de salida o entrada

- Ip access-group (número o nombre) (in/out)

Deny: negar
Permit: permitir
Remark: Comentario
Any: Cualquiera (ejemplo: permit ip any any)
eq: podemos poner el número de puerto o el nombre

in: entrada
out: salida

Verificar lista de control de acceso

- Show ip interface (g0/0 o serial)
- Show access-lists

Estándar: siempre se coloca más cerca del destino
Extendido: Se coloca más cerca del origen

Poner la ACL en la linea vty

- Crear un usuario con su contraseña (username (nombre) secret (contraseña))
- Crea la lista de acceso ya sea numera o nombrada
- Line vty 0 4
- login local
- transport input (telnet o ssh)
- access-class (nombre de la ACL o número) (in / out)

Ejemplo:

```
username ADMIN secret class
ip access-list standard ADMIN-HOST
remark This ACL secures incoming vty lines
permit 192.168.10.10
deny any
exit

line vty 0 4
login local
transport input telnet
access-class ADMIN-HOST in
end

line vty 0 4
login local
transport input ssh
access-class ADMIN-HOST in
end
```

NAT

NAT Estático

- ip nat inside source static (direccion ip privada) (direccion ip publica)
- interface (g0/0 o serial de entrada)
- ip address (ip privada) (mascara)
- ip nat inside (entrada)
- exit
- interface (g0/0 o serial de salida)
- ip address (ip publica) (mascara)
- ip nat outside (salida)

Ejemplo:
ip nat inside source static 192.168.10.254 209.165.201.5

interface serial 0/1/0
ip address 192.168.1.2 255.255.255.252
ip nat inside
exit

interface serial 0/1/1
ip address 209.165.200.1 255.255.255.252
ip nat outside

Comandos para verificar NAT estático

- show ip nat translations
- show ip nat statistics

NAT Dinamico

- ip nat pool (nombre del pool) (poner la direccion que se utilizara para traducir por lo general siempre es la primera y la última) netmask (poner la masacara y para ello necesitaremos sumarisar indica qué bits de dirección pertenecen a la red y qué bits pertenecen al host para ese rango de direcciones)
- access-list (numero) (permit/deny) (id de la red) (mascara de wilcard)
- interface (g0/0 o serial)
- ip nat inside source list (numero de la lista creada) pool (nombre del pool creado)
- interface (g0/0 o serial de entrada)

- ip nat inside
- interface (g0/0 o serial de salida)
- ip nat outside

Ejemplo:
Ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224

access-list 1 permit 192.168.0.0 0.0.255.255

ip nat inside source list 1 pool NAT-POOL1

interface serial 0/1/0
ip nat inside

interface serial 0/1/1
ip nat outside

Comandos para verificar NAT dinamico

- show ip nat translations
- show ip nat translation verbose
- clear ip nat translation (Para borrar las entradas dinámicas antes de que expire el tiempo de espera, se configura en modo privilegiado)
- show ip nat translation
- show ip nat statistics

PAT
Para la configuracion de PAT solo agregamos “overload” al final

- **Crear una ACL**
- ip nat inside source list (numero de la ACL) interface (serial por donde sale a la otra red) overload
- interface (serial de entrada)
- ip nat inside
- interface (serial de salida)
- ip nat outside

Ejemplo:

NAT estático:

```
ip nat inside source list 1 interface serial 0/1/1 overload
access-list 1 permit 192.168.0.0 0.0.255.255

interface serial0/1/0
ip nat inside
exit

interface Serial0/1/1
ip nat outside
```

NAT dinámico:

```
ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask
255.255.255.224

access-list 1 permit 192.168.0.0 0.0.255.255

ip nat inside source list 1 pool NAT-POOL2 overload

interface serial0/1/0

ip nat inside
exit

interface serial0/1/1
ip nat outside
end
```

EIGRP

- router eigrp (número de proceso)
- network (id) (mascara de wildcard)

Poner pasivas las interfaces

- router eigrp (número de proceso)
- passive-interface (puede ser g0/0, g0/1)

Poner router ID

- router eigrp (número de proceso)
- eigrp router-id (id)

Comandos para verificar

- show ip eigrp neigbors
- show ip procols

Ejemplo:

Router eigrp 10
eigrp router-id 1.1.1.1
network 10.0.0.0 0.255.255.255
network 20.0.0.0 0.255.255.255
passive-interface g0/0

VPN

Tunnel GRE

Hacer ruta predeterminada en el router que conecta al ISP

- ip route 0.0.0.0 0.0.0.0 (ip por donde va a salir)

configurar interfaz del túnel GRE

- interface tunnel 0
- ip address (ip + mascara)
- tunnel source (poner la serial por donde sale s0/0/0, s0/0/1)
- tunnel destination (ip del destino) (en ocaciones puede ser la serial del otro router al cual también esta conectado al isp)

Comandos para verificar

- show ip interface tunnel 0

VPN de manera remota

Configuración el router

- ip local pool poolVPN (rango de direcciones)

- aaa new-model
- aaa authentication login UsuariosVPN local
- aaa authorization network GrupoVPN local

- username (usuario) secret (contraseña)

- crypto isakmp policy 5
- encryption aes 256
- hash sha
- authentication pre-sha
- group 5

- crypto isakmp client configuration group GrupoVPN
- key VPN
- pool poolVPN

- crypto ipsec transform-set setVPN esp-aes esp-sha-hmac

- crypto dynamic-map DinamicoVPN 5
- set transform-set setVPN
- reverse-route

- crypto map MapaEstatico client configuration address respond

- crypto map MapaEstatico client authentication list UsuariosVPN

- crypto map MapaEstatico isakmp authorization list GrupoVPN

- crypto map MapaEstatico isakmp authorization list GrupoVPN

- Accede a la interfaz de salida del router y ponemos lo siguiente:
- crypto map MapaEstatico

CDP

Comandos de verificación

- show cdp (ver estado de cdp)
- show cdp neighbors (descubrir a los vecinos)
- show cdp interface
- show cdp neighbors detail (descubrir de forma más detalla del dispositivo)

Habilitar o deshabilitar LLDP

- no cdp run (deshabilitar cdp en todo el dispositivo)
- cdp run (habilitar cdp en el dispositivo)

Habilitar o deshabilitar cdp en las interfaces

- interface (g0/0, s0/0/0 etc.)
- cdp enable (habilitar cdp en la interfaz)
- no cd penable (deshabilitar cdp en la interfaz)

LLDP

Comandos de verificación

- show lldp (ver estado de LLDP)
- show lldp neighbors (descubrir a los vecinos)
- show lldp neigbors detail (descubrir de forma más detalla del dispositivo)

Habilitar o deshabilitar LLDP

- no lldp run (deshabilitar LLDP en todo el dispositivo)
- lldp run (habilitar LLDP en todo el dispositivo)

Habilitar o deshabilitar LLDP en las interfaces

- interface (g0/0, s0/0/0 etc.)
- lldp transmit (transmite)
- lldp receive (recibe)

Recuperación de contraseña

Paso 1

- Ingresar al modo ROMMON, para ello apagaremos el router y lo volveremos a prender, una ves este prendiendo presionamos la combinación de teclas (Ctrl+Pausa) repetitivamente hasta que que el router entre al modo ROMMON

```
Readonly ROMMON initialized

monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

Paso 2

- Cambiar el registro de configuración para ello usaremos el comando:
- confreg 0x2142
- reset

```
rommon 1 > confreg 0x2142
rommon 2 > reset

System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
(output omitted)
```

Paso 3

- Copiar el startup-config en la running-config, Cuando el dispositivo haya terminado la recarga, copie la configuración de arranque a la configuración en ejecución mediante el uso del comando:
- copy startup-config running-config

```
Router# copy startup-config running-config
Destination filename [running-config]?

1450 bytes copied in 0.156 secs (9295 bytes/sec)
R1#
```

Paso 4

- Cambiar la contraseña, usando los comandos:
- Configure terminal
- enable secret (contraseña)

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# enable secret cisco
```

Paso 5

- Guardar el running-config como el nuevo startup-config, Una vez configuradas las nuevas contraseñas, vuelva a cambiar el registro de configuración a 0x2102 con el comando:
- config-register 0x2102 (el comando se ejecuta desde el modo de configuracion global)
- copy running-config startup-config (el comando se ejecuta en el modo privilegiado)

```
R1(config)# config-register 0x2102
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Paso 6

- Recargar el dispositivo, Vuelva a cargar el dispositivo, como se muestra en el ejemplo. El dispositivo ahora utiliza las contraseñas para autenticación recién configuradas, con el comando:
- reload

```
R1# reload
```

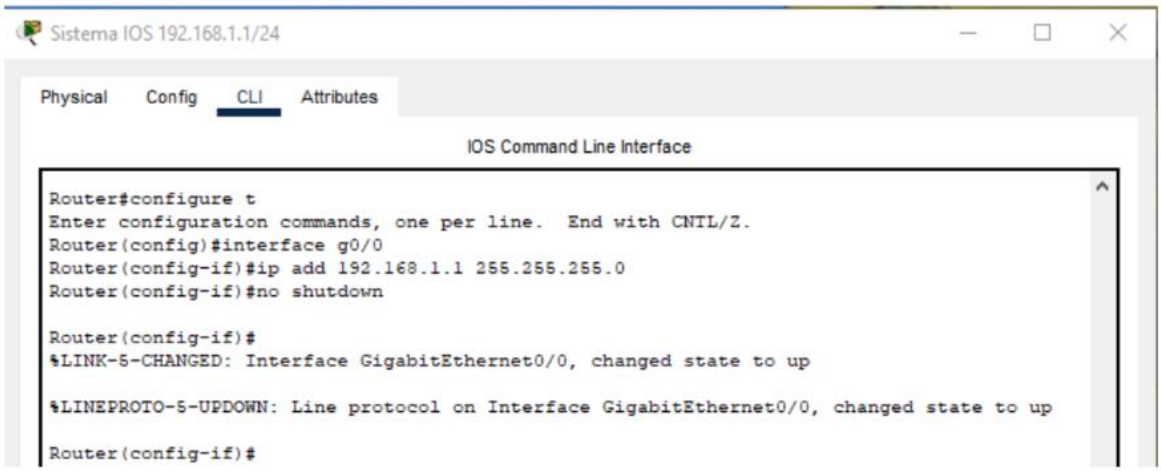
Recuperación de ISO en router Cisco

Paso 1

Conectar el cable de consola de PC a router

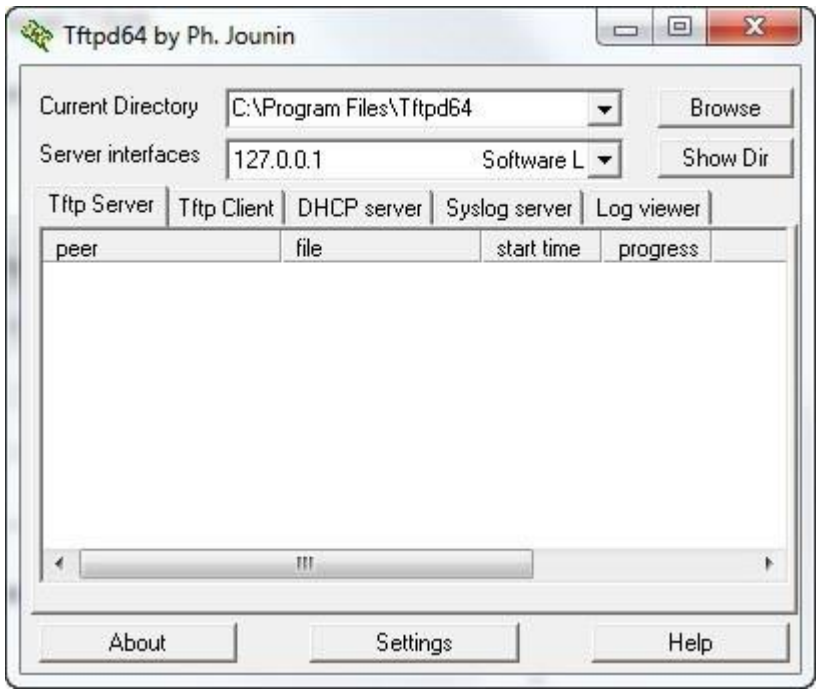
Paso 2

Configurar una dirección IP en el router que tiene el ISO



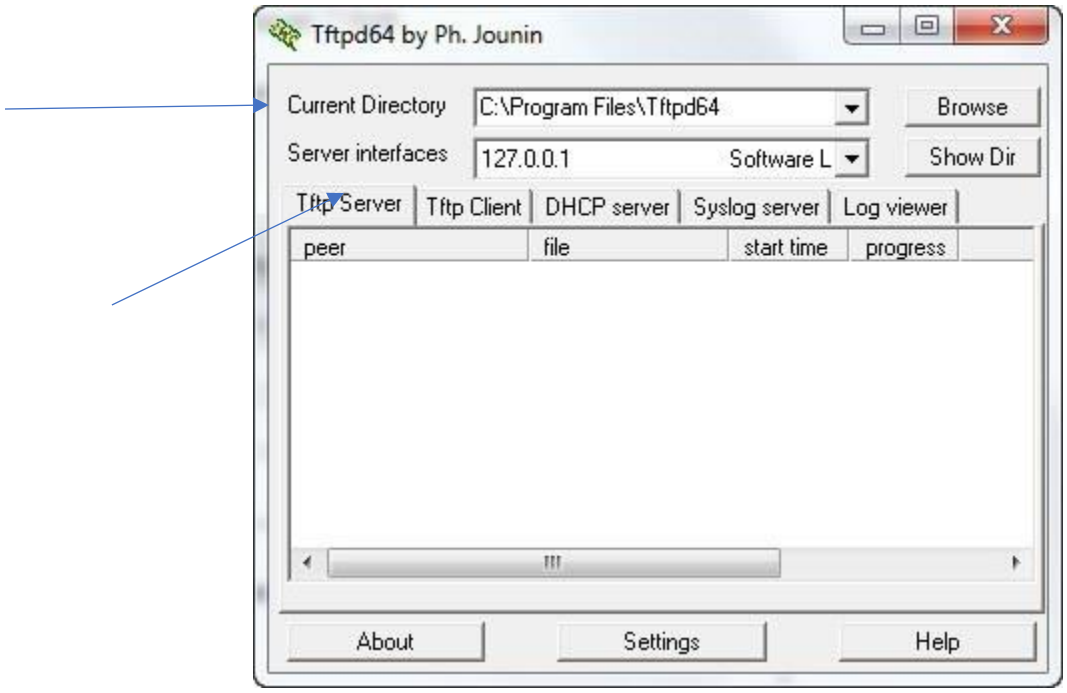
Paso 3

Descargar el programa Tftpd64 by ph. Jounin (en la PC que está configurando el router con el ISO)



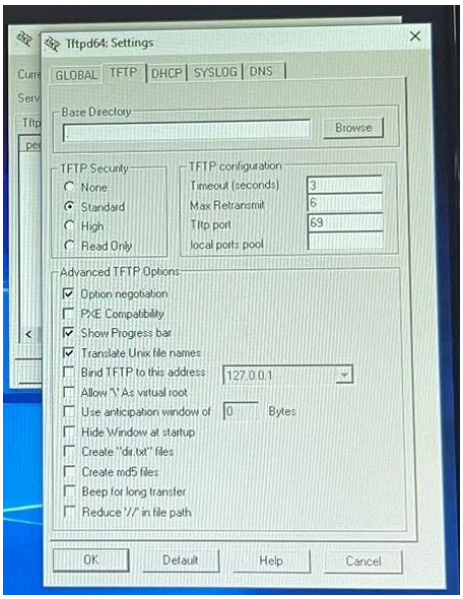
Paso 4

Una vez este descargado configuramos la parte de “current directory” que es en donde se va a guardar el archivo ISO y configuraremos el apartado de “Server interfaces” que ahí ira la dirección IP distinta a la que le configuramos al gigabit



Paso 5

Damos en el apartado “TFTP” y vemos que la configuración este bien como se ve en la ilustración



Paso 6

Ahora haremos una prueba de conectividad con la dirección IP que le pusimos al programa

```
Router#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Paso 6

Localizar en el directorio de la memoria flash el nombre del archivo del sistema operativo con terminación .bin, usando el siguiente comando

- DIR FLASH (modo privilegiado)
- Localizar y copiar el nombre del archivo con terminación .bin, ya que lo ocuparemos para mandar la copia al servidor TFTP

```
Router#DIR FLASH
Directory of flash0:/

    3  -rw-    33591768          <no date>  c1900-universalk9-mz.SPA.151-4.M4.bin
    2  -rw-       28282          <no date>  sigdef-category.xml
    1  -rw-      227537          <no date>  sigdef-default.xml

255744000 bytes total (221896413 bytes free)
```

Paso 7

Copiar la imagen del sistema operativo del router hacía el servidor TFTP para ellos ingresaremos los siguientes comandos en el modo privilegiado

- COPY FLASH: TFTP:
- Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin (Pegamos el nombre del archivo.BIN que copiamos anteriormente)
- Address or name of remote host []? (Ingresamos la dirección IP del servidor TFTP en este caso sería a la que le pusimos al programa)
- Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]? (Confirmamos con la Tecla ENTER)

```
Router>ena
Router#COPY FLASH: TFTP:
Source filename []? c1900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 192.168.1.10
Destination filename [c1900-universalk9-mz.SPA.151-4.M4.bin]?

Writing c1900-universalk9-mz.SPA.
151-4.M4.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 0.435 secs (8108038 bytes/sec)
Router#
```

Para visualizar el archivo copiado, iremos en donde le asignamos guardarlo y veremos que ahí estará

Si deseamos borrar el ISO del un router ingresamos los siguientes comandos

- delete c1900-universalk9-mz.SPA.151-4.M4.bin (modo privilegiado)
- Delete filename [c1900-universalk9-mz.SPA.151-4.M4.bin]? (ENTER)
- Delete flash:/c1900-universalk9-mz.SPA.151-4.M4.bin? [confirm] (ENTER)
- Reload

```
Router>ena
Router#delete c1900-universalk9-mz.SPA.151-4.M4.bin
Delete filename [c1900-universalk9-mz.SPA.151-4.M4.bin]?
Delete flash:/c1900-universalk9-mz.SPA.151-4.M4.bin? [confirm]

Router#reload
```

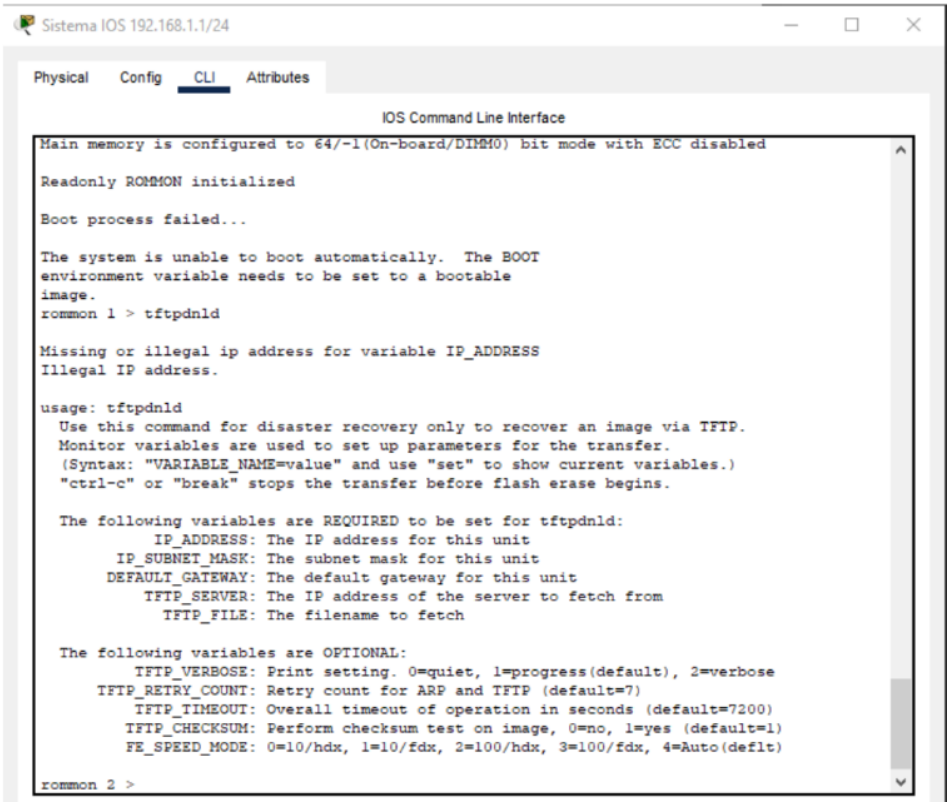
Paso 8

Una vez hecho todo lo anterior, ahora conectaremos el router que no tiene el ISO y lo conectamos por el cable de consola a la PC

Paso 9

Una ves inicie veremos que esta en modo rommon 1 y haremos los siguiente:

- Rommon 1 > tftpdnld (Muestra 10 variables que podemos utilizar, en este caso vamos a ocupar las requeridas ya que las otras 5 son opcionales)



- Crear las siguientes variables de ambiente de manera secuencial:

Rommon 2 > IP_ADDRESS= (IP de la gigat que configuramos anteriormente)

Rommon 3 > IP_SUBNET_MASK= (Mascara)

Rommon 4 > DEFAULT_GATEWAY= (IP del servidor TFTP en este caso la que le pusimos al programa)

Rommon 5 > TFTP_SERVER= (IP del servidor TFTP en este caso la que le pusimos al programa)

Rommon 6 > TFTP_FILE= (pondremos el nombre el archivo que se nos guardo al momento de descargar la ISO)

```
rommon 2 > IP_ADDRESS=192.168.1.1
rommon 3 > IP_SUBNET_MASK=255.255.255.0
rommon 4 > DEFAULT_GATEWAY=192.168.1.10
rommon 5 > TFTP_SERVER=192.168.1.10
rommon 6 > TFTP_FILE=c1900-universalk9-mz.SPA.151-4.M4.bin
```

- Visualizar las variables con sus valores asignados con el comando:

  Rommon 7 > SET

```
rommon 7 > SET
DEFAULT_GATEWAY=192.168.1.10
IP_ADDRESS=192.168.1.1
IP_SUBNET_MASK=255.255.255.0
PS1=rommon ! >
TFTP_FILE=c1900-universalk9-mz.SPA.151-4.M4.bin
TFTP_SERVER=192.168.1.10
rommon 8 >
```

- Y descargar el archivo del sistema operativo con el comando:

  Rommon 8 > tftpdnld

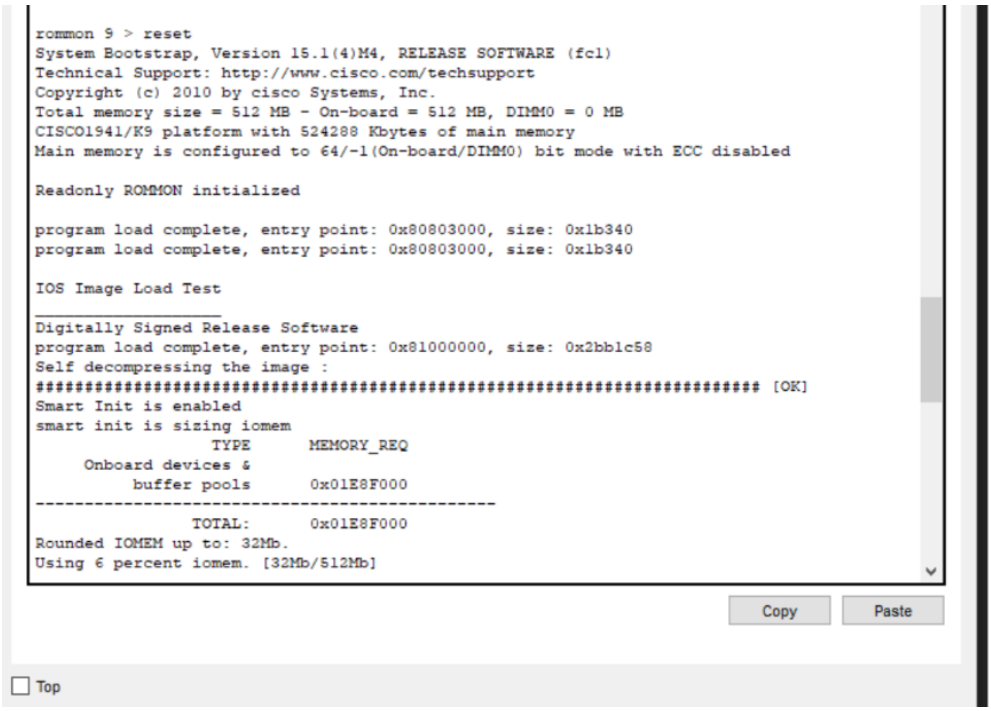
  Confirmar con la tecla y, dar enter y comenzará el proceso de transferencia del archivo program flash location 0x62000000

```
rommon 8 > tftpdnld

          IP_ADDRESS: 192.168.1.1
      IP_SUBNET_MASK: 255.255.255.0
     DEFAULT_GATEWAY: 192.168.1.10
         TFTP_SERVER: 192.168.1.10
           TFTP_FILE: c1900-universalk9-mz.SPA.151-4.M4.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!

Do you wish to continue? y/n:  [n]:  y
```

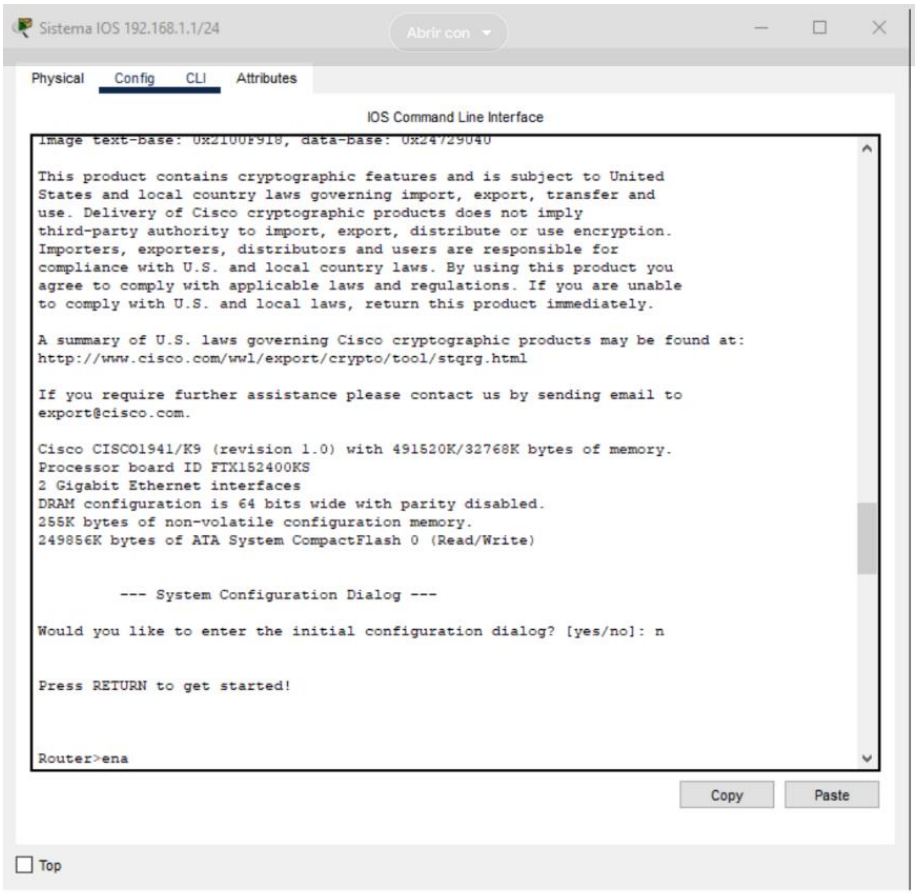
Nota: En caso de que la conexión sea fallida, volver a crear las variables en el orden especificado

- Ya que el proceso de transferencia fue exitoso, se debe reiniciar el dispositivo con el comando reset para cargar el sistema de forma

  normal.rommon 10 > reset



Y listo el proceso ha terminado



Seguridad en el router

Exija que se utilice un mínimo de 10 caracteres para todas las contraseñas

- **security passwords min-length 10**

Habilitar conexiones SSH

Asigne un nombre de dominio

Crear una entrada de base de datos de usuarios local para que se utilice al conectarse al router a través de SSH. La contraseña debe cumplir con los estándares de contraseña segura, y el usuario debe tener acceso de nivel de administrador.

- **username** (nombre del usuario) **privilege 15 secret** (contraseña)

Configure la entrada de transporte para las líneas vty de modo que acepten conexiones SSH y generar las claves RSA

Los siguientes comandos harán que se cierre la sesión de la línea después de cinco minutos de inactividad (los minutos pueden ser modificados).

- **line console 0**
- **exec-timeout 5 0**

- **line vty 0 4**
- **exec-timeout 5 0**

El comando siguiente impide los intentos de inicio de sesión por fuerza bruta

login block-for (intento de inicio de sesión se coloca por segundos) **attempts** (cuantas veces puede fallar al iniciar sesión) **within** (y en cuanto segundos se fallarán esos intentos de inicio de sesión)

Ejemplo: R1(config)# login block-for 30 attempts 2 within 120

show login (login para ver el estado de inicio de sesión)

Nota: Para el switch se hace exactamente lo mismo

Niveles de privilegios

Primero tenemos que recordar que podemos crear desde el nivel 1 hasta el 15.

El nivel 15 es el que tiene acceso a todo y el 1 no cuenta con todos los accesos. Es necesario solo crear el usuario junto con la contraseña para el usuario nivel 15 sin crear el nivel ya que vienen creado por defecto.

Antes de crear los niveles y usarios tenemos que configurar las líneas de consola y las líneas virtuales de la siguiente manera:

- line console 0
- login local

- line vty 0 4
- login local

Para crear y asignarle privilegios a un nivel utilizaremos el siguiente comando:

- **Privilege exec leven** (el numero del nivel) (y el privilegio que le queremos dar)

También podemos usar el “configure” y “interface” lo que indicamos que dentro de ese modo de configuración podemos asignarles los privilegios que se utilicen según el modo de configuración que le asignemos.

- **Privilege configure level** (el número del nivel) (y el privilegio que le queremos dar)
- **Privilege interface level** (el número del nivel) (y el privilegio que le queremos dar)

Podemos usar el comando “all” para que dentro del modo de configuración asignado podamos usar todos los privilegios que pertenecen a ese modo.

- **Privilege configure all level** (el número del nivel) (y el privilegio que le queremos dar)
- **Privilege interface all level** (el número del nivel) (y el privilegio que le queremos dar)

Por ejemplo:

```
R1(config)#privilege exec level 5 traceroute
R1(config)#privilege exec level 5 ssh -l
R1(config)#privilege exec level 5 telnet
R1(config)#privilege exec level 5 ping
R1(config)#
R1(config)#privilege exec level 10 configure terminal
R1(config)#privilege configure level 10 access-list
R1(config)#privilege configure all level 10 ip access-list
R1(config)#privilege configure all level 10 interface
R1(config)#privilege interface level 10 shutdown
R1(config)#privilege interface level 10 speed
R1(config)#
R1(config)#privilege configure all level 11 route
R1(config)#no privilege configure all level 11 route
R1(config)#privilege configure all level 11 router
R1(config)#privilege interface level 11 ip
R1(config)#privilege configure all level 11 crypto
```

Un ves creados los niveles de privilegios ahora crearemos un usuario y le asignaremos dicho nivel según corresponda, junto con una contraseña, usando el siguiente comando:

- **username** (nombre del usuario) **secret** (contraseña)
- **username** (nombre del usuario) **privilege** (número del nivel)

por ejemplo:

```
R1(config)#
R1(config)#username n5 secret cisco5
R1(config)#username n5 privilege 5
R1(config)#username n10 secret cisco10
R1(config)#username n10 privilege 10
R1(config)#username n11 secret cisco11
R1(config)#username n11 privilege 11
R1(config)#
```

Comandos extra:

Para asignar una contraseña a un nivel usaremos el siguiente comando:

- enable secret level (número del nivel) (contraseña)

Ejemplo: R1(config)#enable secret level 5 cisco5

Para acceder a un nivel pondremos el comando:

- enable (número del nivel)

Ejemplo: R1> enable 5

Con el siguiente comando podemos ver en qué nivel de privilegio nos encontramos:

- show privilege

Vistas

Primero habilitaremos la AAA dentro del router

- aaa new-model

Configuraremos una contraseña del modo EXEC privilegiada para acceder a la vista raíz

- enable secret (contraseña)

Para habilitar la vista raíz

- enable view (también usando el comando podemos acceder al directorio raíz)

Para crear un usuario usaremos el siguiente comando

- parser view (nombre del usuario)

ejemplo:

```
R1# configure terminal

R1(config)# parser view admin1
```

Una vez creado el usuario le asignaremos una contraseña

- secret (contraseña)

ejemplo:

```
R1(config-view)# secret admin1pass

R1(config-view)#
```

Empezaremos agregar todos los comandos que le vamos a proporcional al usuario

- commands exec include (el comando)

ejemplo:

```
R1(config-view)# commands exec include show version
```

También podemos usar “all” para asignarle todos los comandos que usen tal palabra

- commands exec include all (el comando)

ejemplo:

```
R1(config-view)# commands exec include all show
```

comandos para verificar la vista:

- enable view (usuario)
- show parser view

Syslog

Para configurar Syslog primero tenemos que asignarle una dirección ip a un servidor y habilitarle “Syslog”

Paso a paso de como configurar “syslog” dentro del router

- logging (dirección ip del servidor)
- logging trap debugging (lo que hace este comando es que cuando mande la alerta al servidor te aparezca de forma detallada la alerta)
- service timestamps log datetime msec (Agrega la fecha, hora y milisegundos a los mensajes de registros)

ejemplo:

```
STEAM(config)#logging 83.4.0.4
STEAM(config)#logging trap debugging
STEAM(config)#service timestamps log datetime msec
STEAM(config)#
```

Copy Paste

SNMP

Paso a paso de como configurar “SNMP” dentro del router

Configuraremos una comunidad

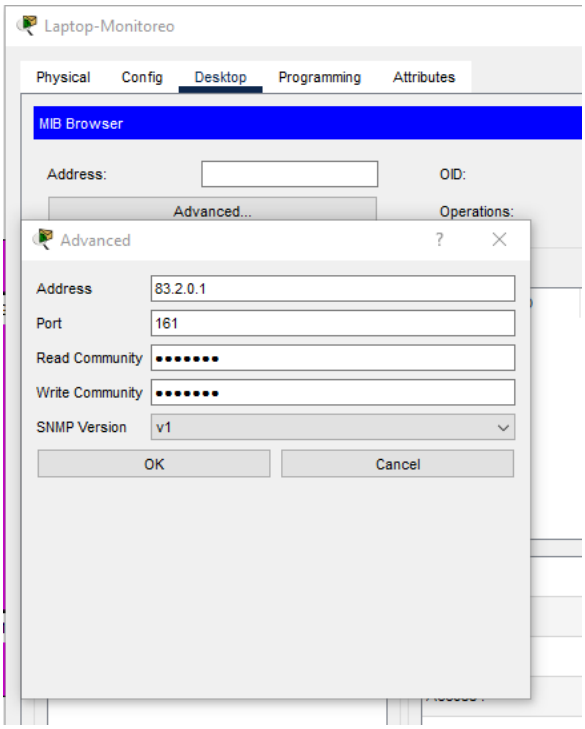
- snmp-server community (nombre de la comunidad) (RO o RW)

RO = permisos solo de lectura
RW = permisos de lectura y escritura

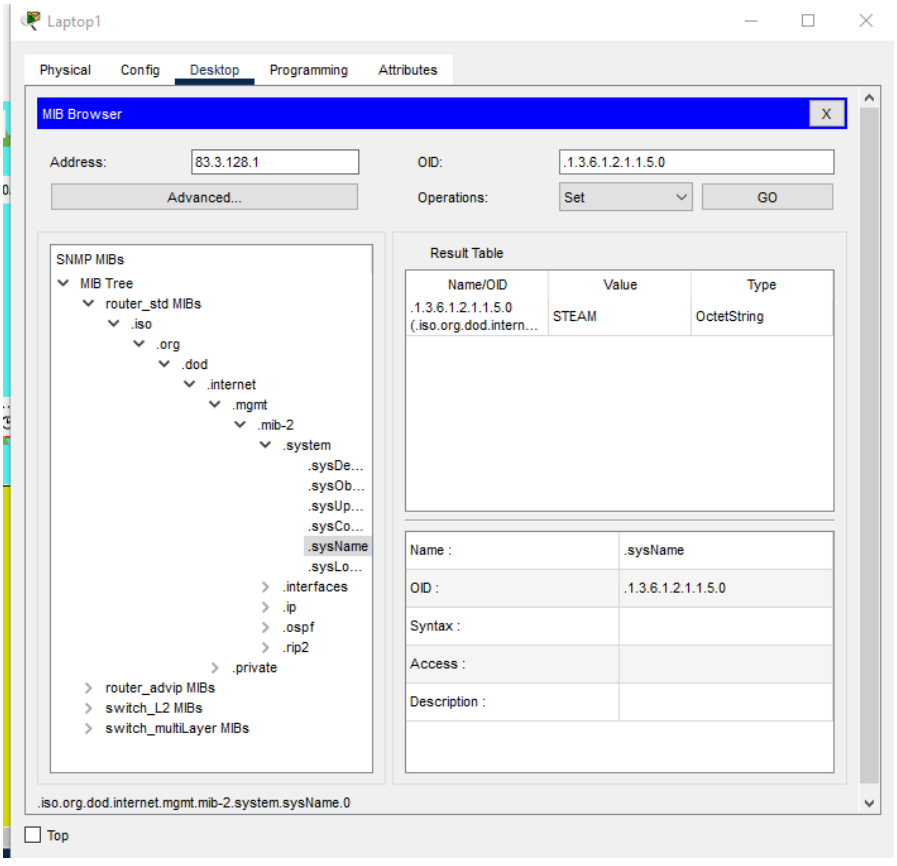
Ejemplo:

```
snmp-server community public RO
snmp-server community private RW
```

Para verificar el usaro de SNMP usaremos una PC y accederemos a MIB Browser
Dentro de ahí pondremos la dirección ip y el nombre de la comunidad



Dentro del apartado buscaremos “SysName” y le daremos el “GO”, dentro de “Set” podemos hacer modificaciones como cambiar interfaz o nombre de un router entre otros.



Mandar copia de configuración de un router Cisco a un Servidor TFTP

Primero guardaremos la configuración de nuestro router

- copy running-config startup-config

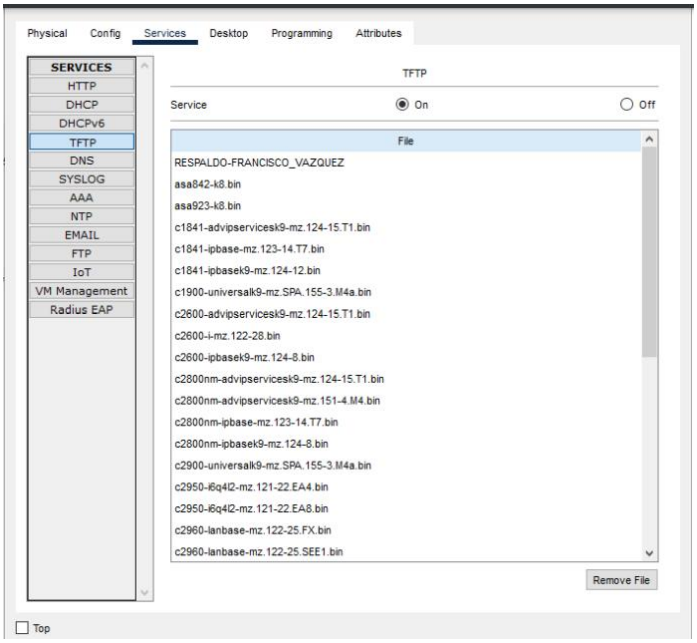
Mandaremos la copia de nuestra configuración al servidor TFTP

- copy running-config tftp:
- Cuando demos enter nos pedirá la dirección ip del servidor TFTP y nos pedirá que le asignemos un nombre a nuestra copia

Ejemplo:

```
Francisco_Vazquez#copy running-config tftp:
Address or name of remote host []? 130.10.0.10
Destination filename [Francisco_Vazquez-confg]? RESPALDO-FRANCISCO_VAZQUEZ

Writing running-config...!!
[OK - 2453 bytes]

2453 bytes copied in 0 secs
Francisco_Vazquez#
```

Si observamos nuestro servidor ya tenemos la copia guardada con el nombre que le asignamos



Ahora procedemos a borrar el archivo de configuración de nuestro router y después reiniciaremos el router usando “reload”

```
Francisco_Vazquez#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

```
Francisco_Vazquez#reload
Proceed with reload? [confirm]
```

Si el proceso se completo correctamente entraremos el modo privilegiado sin configuración

Para cargar la configuración de nuestro router tenemos que configurar la gigabit del router la cual conecta al servidor, dicha dirección ip tiene que ser el Gateway que tiene nuestro servidor TFTP

Procederemos a descargar el archivo de configuración del servidor al router

- copy tftp: running-config
- Cuando demos enter nos pedirá la dirección ip del servidor TFTP y nos pedirá el nombre que le asignemos a nuestra copia

Ejemplo: