LABORATORIO DE REDES DE ÁREA EXTENDIDA

PRÁCTICA N° 1

1. TEMA

CONFIGURACIÓN DE ROUTERS Y SWITCHES (PARTE 1)

2. OBJETIVOS

2.1. Realizar una configuración básica de switches y routers Cisco utilizando la Interfaz de línea de comandos.
2.2. Realizar configuración de listas de acceso estándar.
2.3. Realizar configuración del protocolo de enrutamiento RIPv2.

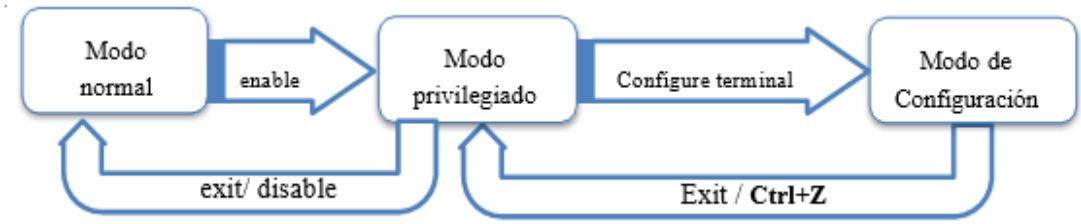
3. MARCO TEÓRICO

SWITCHES Y ROUTERS CISCO

3.1. Modos de operación

Los routers/switches CISCO tienen tres modos de operación en su línea de comando:

- Modo normal de usuario, con prompt >
- Privilegiado o de administración, con prompt #
- De configuración, con la palabra config antes del prompt #



Otros comandos útiles en el CLI

- Para autocompletar comandos se usa el tabulador
- Para pedir ayuda de comandos disponibles u opciones de los mismos se usa el signo?.
- No hace falta escribir los comandos completos. Basta con las letras suficientes para que no haya confusión con otras alternativas. Por ejemplo, es válido *ena* por *enable*, *config term* por *configure terminal*, etc.
- Ctrl+Shift+6 interrumpe la ejecución de un comando que no responde y que se ha quedado “congelado”.

3.2. Contraseña de acceso al modo privilegiado y otros comandos para switches y routers.

3.2.1. Comandos de Verificación

El comando *show* tiene como función básica obtener información acerca del equipo. Por ejemplo, los más usuales son los siguientes:

show version: muestra la versión de IOS que se está utilizando, la información de copyright de CISCO que aparece en el arranque y un resumen de las características e interfaces del equipo.

show running-config: lista la configuración del equipo que está actualmente en ejecución (¡en RAM y no en NVRAM!). Es muy útil para respaldar o guardar "en papel" la configuración de referencia de cada uno de los equipos.

show history: Como casi todos los interfaces en línea de comandos, el CLI de CISCO guarda un historial de las últimas órdenes que se han ejecutado desde la consola. Por defecto se guardan los últimos 10 comandos ejecutados. Si se quiere incrementar ese número se hace desde el modo privilegiado con la siguiente orden: **terminal history size 50**. Si se quisiera desactivar el historial de comandos se ejecuta: **terminal history size 0**

3.2.2. Contraseña de acceso al modo privilegiado

Existen diferentes formas de proteger el acceso al equipo, pero la primera que se debe usar es la que permite asegurar que nadie entre al modo privilegiado sin una contraseña cifrada. Para ello, desde el modo de configuración se tiene que ejecutar el comando *enable secret* y a continuación la contraseña.

Existe otra opción mediante el comando *enable password*, pero en este caso la contraseña se listará en claro al hacer *show running-config*. Se puede cifrar esta contraseña mediante el comando *service password-encryption*.

3.2.3. Comando no

El comando no antepuesto a otro comando sirve, en las ocasiones en las que esto se puede hacer, para eliminar, desactivar, volver atrás o deshacer el efecto de dicho comando. Por ejemplo, para eliminar la contraseña de acceso al modo privilegiado se usa *no enable secret* o para borrar el nombre al equipo se puede usar el comando *no hostname*.

3.2.4. Comando do

Si se quiere ejecutar un comando del modo privilegiado desde el modo configuración y no se desea estar cambiando continuamente de modo, se lo puede hacer anteponiendo el comando *do*.

Por ejemplo, escribiendo *do show ip route* desde el modo de configuración ejecutaría el comando como si estuviera en el modo privilegiado. El único inconveniente de ejecutar comandos con *do* es que no se tiene disponible ni las funciones de autocompletar ni la ayuda con la tecla.

3.2.5. Otros comandos básicos

hostname <nombre>: desde el modo de configuración, permite cambiar el nombre distintivo del equipo.

banner motd #: también desde el modo de configuración, permite personalizar el mensaje de bienvenida que se recibe al conectarse al equipo. El mensaje finaliza cuando se vuelva a escribir # al principio de una línea y se pulse la tecla INTRO. Se puede usar otro carácter como finalizador cambiándolo en el comando.

reload: desde el modo privilegiado reinicia el equipo. Los cambios no salvados se pierden.

write memory o copy running-config startup-config: desde el modo privilegiado salva la configuración actualmente en ejecución como configuración por defecto.

write erase o erase startup-config: Limpia toda la configuración del equipo y lo deja como recién salido de fábrica.

no ip domain-lookup: Desactiva la traducción de nombres a dirección del dispositivo, ya sea éste un Router o un Switch.

3.3. Configuración básica de interfaces y líneas de acceso en un router

Se pueden listar las interfaces que se tiene con todos sus detalles mediante el comando *show interfaces* desde el modo privilegiado.

Si se desea información sólo de una determinada interfaz se podría colocar por ejemplo el comando *show interface f0/1*.

- **Configuración de interfaces ethernet**

La configuración de una interfaz se realiza en tres pasos, siempre desde el modo de configuración: seleccionar el interfaz a configurar, asignarle una IP y una máscara a ese interfaz y, finalmente, activarla. Para las interfaces serie, se necesitará además, activar una señal de reloj en uno de los extremos de la comunicación (DCE).

Por ejemplo, si se quiere configurar la interfaz fast ethernet identificada como 0/1 con la IP 192.168.0.1 de la subred 192.168.0.0/25. La secuencia de comandos a aplicar (desde el modo de configuración) sería la siguiente:

- *interface f0/0*, para seleccionar la configuración de la interfaz
- *ip address 192.168.0.1 255.255.255.128*, para asignarle IP y máscara de subred
- *no shutdown*, para activar la interfaz
- *exit*, para salir del modo de configuración de interfaz y volver al modo de configuración normal.

El comando *show ip interface brief* muestra un listado resumen de todas las interfaces del router y el estado en el que se encuentran.

- **Configuración de rutas estáticas**

Las rutas estáticas se introducen en el router a través de los tres mismos parámetros que se usa en las ventanas de asistencia del Packet tracer. Un ejemplo del comando a usar (desde el modo de configuración) para una ruta estática es el siguiente:

- *ip route 192.168.3.0 255.255.255.0 192.168.0.2*

Donde 192.168.3.0 es la dirección de la red a la que se quiere llegar, 255.255.255.0 su máscara y 192.168.0.2 el próximo salto, que es la dirección IP de otro router.

El comando *show ip route* muestra todas las redes que el router conoce, distinguiendo si está conectado directamente a ellas (C), si tiene alguna ruta estática configurada (S) o cualquier otra condición.

3.4. Configuración a través de consola de un switch

Para esta configuración se utiliza un cable de consola (rollover) generalmente RJ-45 – DB-9. Este cable debe ser conectado en el puerto RS-232 de una PC y el puerto de consola del equipo. En el PC se pueden utilizar diferentes programas para este propósito, tales como Hyperterminal, Tera Term, Minicom, entre otros.

A continuación, se presentan algunos comandos iniciales para configuración vía consola:

Para configuración del Hostname

```
Switch#configure terminal
Switch(config)#hostname [Nombre]
Nombre(config)#Ctrl + z
Nombre#
```

Configuración de Password

- **Enable Password**

```
Nombre#configure terminal
Nombre(config)#enable password [password] Nombre(config)#Ctrl + z
Nombre#
```

- **Líneas de terminal virtual**
  Nombre#configure terminal
  Nombre(config)#line vty 0 4
  Nombre(config-line)#login
  Nombre(config-line)#password [password]
  Nombre(config-line)#Ctrl + z
  Nombre#

- **Consola**
  Nombre#configure terminal
  Nombre(config)#line console 0
  Nombre(config-line)#login
  Nombre(config-line)#password [password]
  Nombre(config-line)#Ctrl + z
  Nombre#

- **Enable Secret**
  Nombre#configure terminal
  Nombre(config)#enable secret [password]
  Nombre(config)#Ctrl + z

- **Configuración de Mensaje del día**
  Nombre#configure terminal
  Nombre(config)#banner motd #
  Enter TEXT message. End with the carácter '#'
  Mensaje #

- **Configuración de la descripción de las Interfaces**
  Nombre#configure terminal
  Nombre(config)#interface [interface]
  Nombre(config-if)#description [descripción]
  Nombre(config-if)#Ctrl + z

- **Configuración de una dirección IP en un switch**
  Nombre#configure terminal
  Nombre(config)#interface vlan1
  Nombre(config-if)#ip address [dirección IP] [máscara] Nombre(config-if)#no shutdown
  Nombre(config-if)#exit
  Nombre(config)#ip default-gateway [dirección IP]

- **Configuración de velocidad y duplex de cada interfaz del switch**
  Nombre(config-if)# speed [10|100|1000|auto]
  Nombre(config-if)# duplex [auto|full|half]

- **Verificación de la configuración y funcionamiento del equipo**
  Nombre # show interfaces
  Nombre # show interfaces description
  Nombre # show interfaces status
  Nombre # show interfaces counters
  Nombre # show ip interface brief
  Nombre # show version
  Nombre # show running-config

Uno de los elementos fundamentales de un switch es su tabla de direcciones MAC, la cual le permite relacionar estas direcciones con el puerto por el cual se alcanzan. Se puede ver dicha tabla del conmutador con el comando:

 # show mac address-table

Vlan Mac Address Type Ports
---- ----------- -------- -----
All 000f.9056.e9c0 STATIC CPU
All 0100.0ccc.cccc STATIC CPU
All 0100.0ccc.cccd STATIC CPU
All 0100.0cdd.dddd STATIC CPU

La primera es una de las direcciones MAC del conmutador, que se empleará seguramente al enviar tramas. Las tres siguientes son direcciones MAC multicast empleadas por protocolos propietarios de Cisco (DTP, VTP, CDP, SSTP, CGMP).

3.5. Listas de Control de Acceso

Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar), conocidas como “entradas de control de acceso” (ACE). Las ACE también se denominan comúnmente “instrucciones de ACL”. Cuando el tráfico de la red atraviesa una interfaz configurada con una ACL, el router compara la información dentro del paquete con cada ACE, en orden secuencial, para determinar si el paquete coincide con una de las ACE.

El filtrado de paquetes controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o el descarte de estos según criterios determinados. Las ACL estándar filtran sólo en la Capa 3. Las ACL extendidas filtran en las capas 3 y 4.

3.5.1. ACL estándar

El comando de configuración global access-list define una ACL estándar con un número entre 1 y 99. La versión 12.0.1 del software IOS de Cisco amplió ese intervalo y permite que se utilicen los números que van de 1300 a 1999 para las ACL estándar. Esto permite que se genere un máximo de 798 ACL estándar posibles

La sintaxis completa del comando de ACL estándar es la siguiente:

- *Router(config)# access-list número acl { deny | permit | remark } origen [wildcard-origen][log]*

Debido a que en las ACL estándar no se especifican las direcciones de destino, se las suele colocar tan cerca del destino como sea posible. Si coloca una ACL estándar en el origen del tráfico, evitará de forma eficaz que ese tráfico llegue a cualquier otra red a través de la interfaz a la que se aplica la ACL.

3.5.2. El comando access-class

El comando access-class configurado en el modo de configuración de línea restringe las conexiones de entrada y salida entre una VTY determinada (en un dispositivo de Cisco) y las direcciones en una lista de acceso.

La sintaxis del comando access-class es la siguiente:

- *Router (config)# access-class access-list-number { in [vrf-also] | out }*

El parámetro **in** limita las conexiones de entrada entre las direcciones en la lista de acceso y el dispositivo de Cisco, mientras que el parámetro **out** limita las conexiones de salida entre un dispositivo de Cisco en particular y las direcciones en la lista de acceso.

3.5.3. Verificar las ACL

El comando ***show ip interface*** se utiliza para verificar la ACL en la interfaz. El resultado de este comando incluye el número o el nombre de la lista de acceso y el sentido en el que se aplicó la ACL.

Para ver una lista de acceso individual, utilice el comando **show access-lists** seguido del número o el nombre de la lista de acceso.

4. TRABAJO PREPARATORIO

4.1. Revisar el marco teórico para la realización de la práctica.

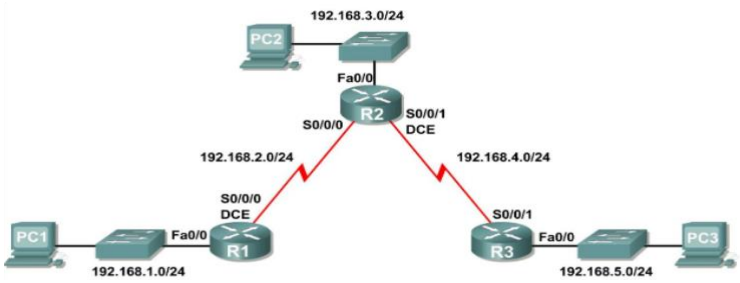
5. EQUIPO Y MATERIALES

Materiales por grupo de trabajo

- 3 PC (Putty / Hyperterminal)
- 3 Switches
- 3 Routers
- Cables seriales, directos y cruzados

6. PROCEDIMIENTO

6.1. En los enlaces entre R1 y R2, así como entre R2 y R3 configurar RIP v2



- Realizar las configuraciones básicas en los switches de acuerdo con las siguientes instrucciones:

a) Configurar el *hostname*
b) Desactivar la búsqueda DNS.
c) Configurar una contraseña de modo EXEC.
d) Configurar un mensaje del día.
e) Configurar contraseña para las conexiones de la consola.
f) Configurar una contraseña para las conexiones de VTY.

- Realizar las configuraciones básicas del router R1, R2 y R3 de acuerdo con las siguientes instrucciones:

a) Configurar el nombre de host del router.
b) Desactivar la búsqueda DNS.
c) Configurar una contraseña de modo EXEC.
d) Configurar un mensaje del día.
e) Configurar contraseña para las conexiones de la consola.
f) Configurar una contraseña para las conexiones de VTY.

- Configurar y activar las direcciones serial y Ethernet.

a) Configurar las interfaces de R1, R2 y R3 con las direcciones IP del Diagrama de topología.
b) Verificar de direccionamiento IP y las interfaces, utilizando el comando *show ip interface brief* para verificar que el direccionamiento IP es correcto y que las interfaces están activas.
c) Configurar las interfaces Ethernet de PC1, PC2 y PC3 con las direcciones IP y gateways por defecto en función del diagrama de topología.
d) Probar la configuración de la PC ejecutando un ping desde la PC al gateway por defecto.

- Configurar el protocolo RIP v2.

a) Habilitar un enrutamiento dinámico.

Para habilitar un protocolo de enrutamiento dinámico, ingrese al modo de configuración global y utilice el comando router. Para habilitar RIP, ingrese el comando *router rip* en el modo de configuración global. Se ingresa el comando versión 2 para habilitar RIP v2 y se deshabilita la sumarización automática.

```
R1(config)#router rip
R1(config-router)# version 2
R3(config-router)#no auto-summary
R1(config-router)#
```

b) Ingresar direcciones de red con clase una vez que se encuentre en el modo de configuración de enrutamiento, se deberá ingresar la dirección de red con clase para cada red conectada directamente por medio del comando *network*.

```
R1(config-router) #network 192.168.1.0
R1(config-router)#network 192.168.2.0
R1(config-router)#end
R1#write
```

Comando network:

• Habilita a RIP en todas las interfaces que pertenezcan a esta red. Ahora estas interfaces enviarán y recibirán actualizaciones RIP.

• Notifica esta red en actualizaciones de enrutamiento RIP que se envían a otros routers cada 30 segundos.

c) Configurar RIP en el router R2 por medio de los comandos *router rip* y *network*.

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.3.0
R2(config-router)#network 192.168.4.0
R2(config-router)#end
R2#copy run start
```

d) Configure RIP en el router R3 por medio de los comandos ***router rip*** y ***network***.

```
R3(config)#router rip
R3(config-router) #version 2
R3(config-router) #no auto-summary
R3(config-router) #network 192.168.4.0
R3(config-router) #network 192.168.5.0
R3(config-router) #end
R3#copy run start
```

e) Verificar el enrutamiento RIP utilizando el comando *show ip route* para verificar que cada router cuente con todas las redes en la topología ingresadas en la tabla de enrutamiento.

f) Utilizar el comando *show ip protocols* para visualizar la información acerca de los procesos de enrutamiento que se producen en el router.

Se puede utilizar este resultado para verificar los parámetros RIP para confirmar que:

- El uso del enrutamiento RIP está configurado.
- Las interfaces correctas envían y reciben las actualizaciones RIP.
- El router notifica las redes correctas.
- Los vecinos RIP están enviando actualizaciones.

- Configuración de Listas de Acceso
  a) Compruebe que R3 posea el hostname “R3”
  b) Configure el nombre de dominio
     - *Router(config)#ip domain-name epn.com*
  c) Genere una llave pública
     - Router(config)#crypto key generate rsa
  d) Cree un usuario y contraseña en R3.
  e) Configure las líneas vty para acceso local y tráfico ssh.
  f) Cree una lista de acceso estándar que permita que solo PC2, pueda acceder a la configuración remota vía SSH de R3.
  g) Verificar el funcionamiento de la lista de acceso estándar.

7. INFORME

7.1. Presente la configuración realizada en el laboratorio.
7.2. Presentar las capturas de pantalla de los comandos de visualización, con la debida explicación de los resultados mostrados.
7.3. Conclusiones y Recomendaciones
7.4. Bibliografía.

8. REFERENCIAS

CCNA R&S: Routing and Switching Essentials 6.0.

Elaborado por: Ing. Víctor H. Reyes C. – Técnico Docente

Revisado por: Ing. Pablo Hidalgo, MSc. –Responsable de la asignatura de Redes de Área Extendida.