LABORATORIO DE REDES DE ÁREA EXTENDIDA

PRÁCTICA N° 2

1. TEMA

CONFIGURACIÓN DE ROUTERS Y SWITCHES (PARTE 2)

2. OBJETIVOS

2.1. Realizar configuración de listas de acceso en redes IPv6.
2.2. Realizar configuración del protocolo de enrutamiento RIPng.

3. MARCO TEÓRICO

3.1. Configuración de interfaces con direccionamiento IPv6

La configuración de una interfaz se realiza en tres pasos, siempre desde el modo de configuración: seleccionar el interfaz a configurar, asignarle una IPv6 y el prefijo de esa interfaz y, finalmente, activarla. Para las interfaces serie se necesitará, además, activar una señal de reloj en uno de los extremos de la comunicación.

Por ejemplo si se quiere configurar la interfaz fast ethernet identificada como 0/1 con la IP 2001:A:A:A::5. La secuencia de comandos a aplicar (desde el modo de configuración) sería la siguiente:

- interface f0/0, para seleccionar la configuración de la interfaz
- *ipv6 address 2001:A:A:A::5/64,* para asignarle IPv6 y el prefijo
- *no shutdown*, para activar la interfaz
- *exit*, para salir del modo de configuración de interfaz y volver al modo de configuración normal.

Para verificar la correcta configuración de las interfaces se puede emplear el comando *show ipv6 interface brief*.

3.2. 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.

3.2.1. Creación de ACLs IPv6

En el modo de configuración global, utilice el comando ipv6 **access-list *[*nombre*]*** para crear una ACL de IPv6. Al igual que las ACL de IPv4 con nombre, los nombres en IPv6 son alfanuméricos, distinguen mayúsculas de minúsculas y deben ser únicos. A diferencia de IPv4, no hay necesidad de una opción estándar o extendida.

En el modo de configuración de ACL con nombre, utilice las instrucciones permit o deny para especificar una o más condiciones para determinar si un paquete se debe reenviar o descartar.

3.2.2. Aplicación de ACL extendidas en interfaces IPv6

Después de que se configura una ACL de IPv6, se la vincula a una interfaz mediante el comando *ipv6 traffic-filter*:

- *Router(config-if)# ipv6 traffic-filter nombre-lista-acceso { pre | out }*

Para eliminar una ACL de una interfaz, primero introduzca el comando *no ipv6 traffic-filter* en la interfaz y, luego, introduzca el comando global *no ipv6 access-list* para eliminar la lista de acceso.

3.2.3. Verificar las ACL

El comando **show ipv6 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 ipv6 access-list** seguido del nombre de la lista de acceso.

4. TRABAJO PREPARATORIO

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

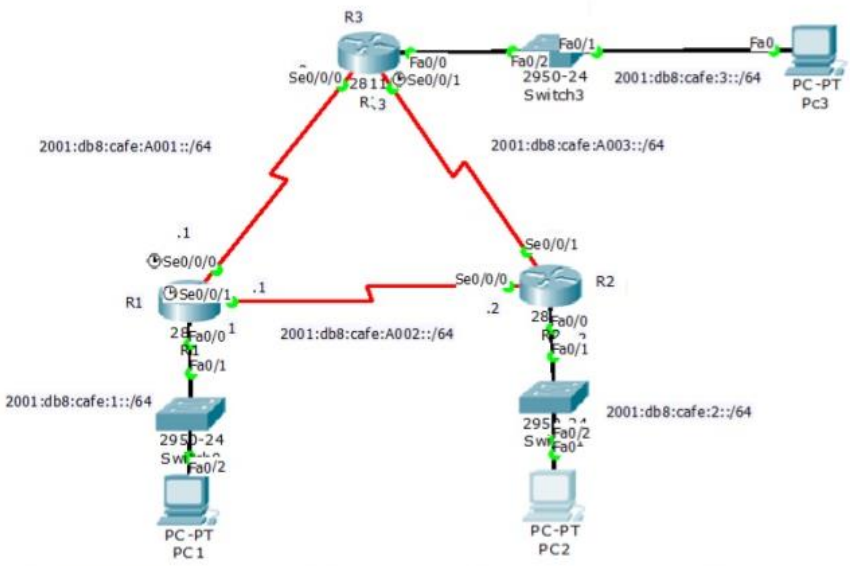
5. EQUIPO Y MATERIALES

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, R2 y R3 configurar RIPng.



- Tanto para PC1, PC2, PC3 configurar una dirección IPv6 válida dentro de las redes especificadas en la topología.

- Activar en todos los routers el enrutamiento IPv6 que viene desactivado de manera predeterminada. El comando de modo global es *ipv6 unicast-routing* (similar a *ip routing*).

```
R1(config)#ipv6 unicast-routing
R2(config)#ipv6 unicast-routing
R3(config)#ipv6 unicast-routing
```

- Configurar las interfaces de los Routers R1, R2 y R3 con direccionamiento IPv6 del diagrama de la topología y probar la correcta configuración por medio de pruebas de *ping* entre las interfaces de un mismo router y redes directamente conectadas.

- Habilitar RIPng en cada uno de los routers.

Para habilitar RIPng solamente se debe ingresar a la interfaz de router que se desea publicar en el proceso RIP e ingresar el comando *ipv6 rip [IDENTIFICADOR] enable* donde "IDENTIFICADOR" es un ID de proceso. Este valor puede ser un número o una palabra. A continuación, ingresaremos en todas las interfaces de R1, R2 y R3 para ingresar este comando. Note que la interfaz f0/1 de R1 y R3 no conectan con ningún otro router, pero sin embargo en ellas también se debe habilitar RIPng para que esas redes se publiquen.

Por ejemplo para R1:

```
R1(config)#int f0/0
R1(config-if)#ipv6 rip REDESCISCO enable
R1(config-if)#int f0/1
R1(config-if)#ipv6 rip REDESCISCO enable
R1(config-if)#int s0/0
R1(config-if)#ipv6 rip REDESCISCO enable
R1(config-if)#end
```

- Verificar si la tabla de enrutamiento se ha actualizado con las redes aprendidas por RIPng (Para ver la tabla de enrutamiento en IPv6 el comando es *show ipv6 route*.). Y realizar pruebas de conectividad entre R1 y R2, R2 y R3, R1 y R3.

- Configuración de Listas de Acceso

a) Habilite un servidor web WAMP o XAMPP en una PC conectada en la LAN 1.
b) Conecte y configure una segunda PC en la LAN2.
c) Cree una lista de acceso IPv6 que impida que la segunda PC en la LAN2 pueda acceder al servidor web de la PC conectada a la LAN1.
d) Aplique la ACL a la interfaz adecuada de cualquier equipo intermedio de la topología.

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.