


INTERCONEXIÓN DE REDES - ENRUTAMIENTO DINÁMICO

Final 7

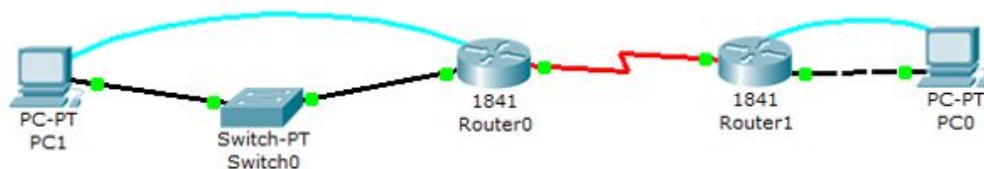
Alumno:	Richard Alvarez Mamani	 UNIVERSIDAD NACIONAL SAN AGUSTIN
Curso:	Redes y Comunicación de Datos	
Docente:	Lucy Angela Delgado Barra	

IV. ACTIVIDADES

PROTOCOLO DINÁMICO RIP V1

1. Construir la siguiente topología para interconectar dos redes corporativas, mediante un enlace Punto a Punto, según el siguiente esquema

Figura 1



2. Realice las configuraciones según la tabla 1

Designación del router	Nombre del router	Dirección LAN	Tipo Interfaz	Dirección WAN	Máscara interfaces	Encapsulamiento
Router0	Principal	182.10.0.1	DCE	182.15.0.1	255.255.0.0	PPP
Router1	Sede	182.20.0.1	DTE	182.15.0.2	255.255.0.0	PPP

Tabla 1

- Nombre de los routers
- Interfaces LAN
- Interfaces WAN
- Encapsulamiento

Recuerde que antes de configurar cualquier enrutamiento, sea estático o dinámico, se debe asegurar de que todas las interfaces estén activadas (up). Para ello puede utilizar el comando:

Principal# show ip interface brief

Ejecute el comando en ambos routers y verifique el estado de las interfaces mostrando los resultados antes y después de la configuración.

3. Configuración de claves: una clave es la seguridad básica en cualquier sistema informático, en relación a los routers, podemos decir que hay diferentes modalidades que las podemos agrupar en:

- a) Claves de acceso al modo usuario: se configuran de acuerdo a la conexión: por consola, por puerto auxiliar y por terminal virtual. El modo usuario permite consultar toda la información relacionada al router sin poder modificarla. El shell es el siguiente:

Router >

- b) Claves de acceso al modo privilegiado: el modo privilegiado permite visualizar el estado del router e importar o exportar imágenes de IOS. El shell es el siguiente:

Router #

En este modo existen dos tipos de clave, cuyos comandos son

- No cifrada: *enable password*
- Cifrada: *enable secret*

Cuando ambas claves están configuradas, el sistema utiliza la clave cifrada. Configuremos ambas modalidades de claves en ambos routers.

3.1 Configuración de una clave de acceso en modo usuario para acceder a la consola:

§ Ingrese los siguientes comandos:

Router>enable

Router#configure terminal

Router(config)#hostname Principal

Principal(config)#line console 0 Se accede a la configuración de la consola

Principal(config-line)#password episunsa Se asigna la clave no cifrada episunsa

Principal(config-line)#login Se indica al router que debe requerir una clave.

Principal(config-line)#exit Sale del modo de configuración de la consola

§ Salga de la sesión de consola, vuelva a acceder al router y verifique la petición de la clave

3.2 Configuración de una clave para acceder modo privilegiado

§ Para configurar las dos claves de acceso al modo privilegiado, escriba:

Principal(config)#enable password epis1

Principal(config)#enable secret epis2

§ Salga de la sesión de consola (*exit*), vuelva a acceder al router y verifique la petición de las claves.

§ Para visualizar las claves utilizadas use el comando:

Principal#show running-config

§ Explique lo que aparece respecto de las claves utilizadas.

§ Luego de verificar que los cambios efectuados funcionan, debe regresar al modo privilegiado y guardar los cambios realizados:

Principal#copy run start

4. Configuración de las interfaces: siguiendo las indicaciones de la práctica anterior configure las interfaces del router, asignándoles las direcciones IP y máscaras apropiadas

5. Repita los pasos 3 y 4 en el router Secundario

6. Configuración del protocolo de enrutamiento dinámico RIP v1

6.1 Verificación básica

§ Visualice y explique los protocolos instalados en el router utilizando el comando:

Principal# show running-config

- #### 6.2 Configuración del protocolo de enrutamiento RIP v1: para configurar el protocolo de enrutamiento RIP se usan los comandos:

Router RIP: activa el protocolo de enrutamiento RIP

Network x.x.x.x: Determina cuáles son las interfaces que participan en el envío y recepción de actualizaciones de enrutamiento. Además permite que el router publique esa red.

Nota. Se ingresa sólo el número de red, ya que esta versión solo soporta redes y no subredes

§ En el router **Principal**, efectúe la siguiente configuración:

Principal(config)#router rip

Principal(config-router)#network 182.10.0.0

Principal(config-router)#network 182.15.0.0

Principal(config-router)#exit

Principal(config)#exit

§ Guarde la configuración del router **Principal**

Principal#copy running-config startup-config

§ En el router **Sede**, efectúe la siguiente configuración:

Sede (config)#router rip

Sede (config-router)#network 182.15.0.0

Sede (config-router)#network 182.20.0.0

Sede (config-router)#exit

Sede (config)#exit

§ Guarde la configuración del router **Sede**

6.3 Visualización de las tablas de enrutamiento

§ Verifique la instalación del protocolo con el comando:

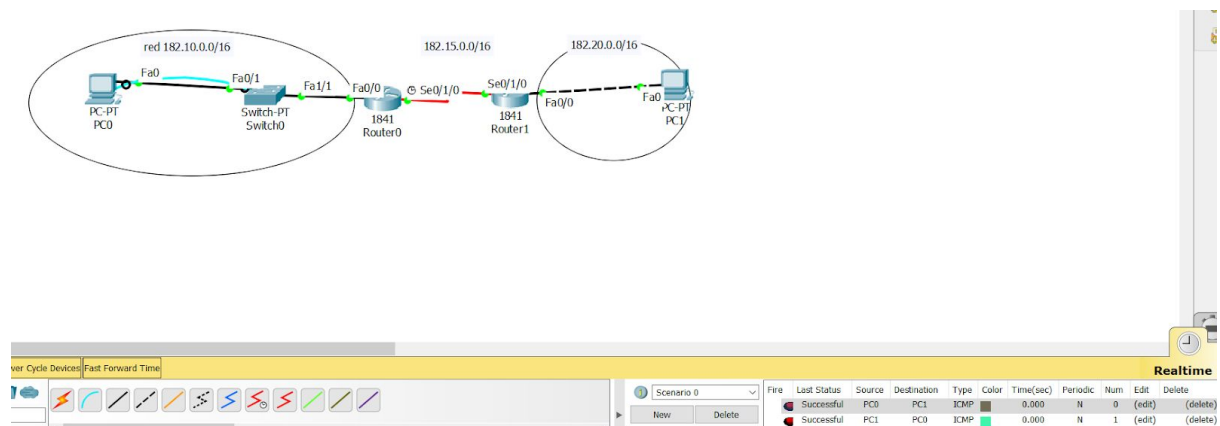
Principal# show running-config

§ Explique la respuesta. Haga lo mismo en el otro router

6.4 Prueba de la conexión

§ Desde ambos routers verifique la conectividad entre ellos usando el comando ping.

§ Verifique la conectividad desde los hosts usando el comando ping.



7. Construya el escenario mostrado en la figura:

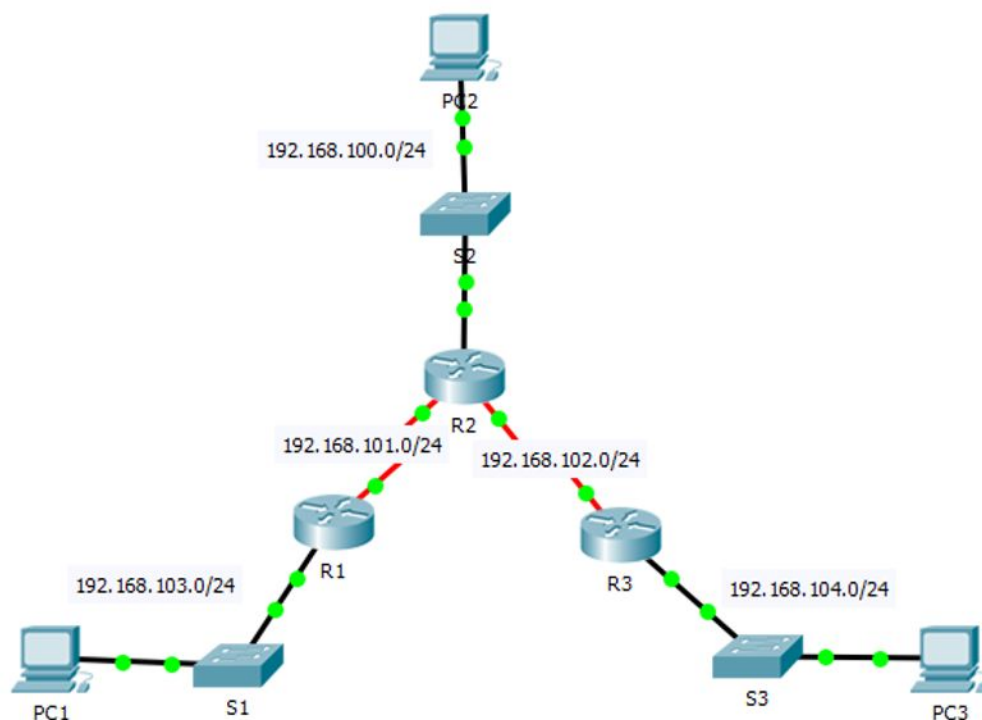


Figura 2

7.1 Realice las configuraciones iniciales de:

- Nombre de routers
- Interfaces LAN y WAN

Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/1/0

Port Status
Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto
Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto
MAC Address 0090.0C9D.1101
IP Configuration
IP Address 192.168.103.1
Subnet Mask 255.255.255.0
Tx Ring Limit 10

Equivalent IOS Commands

```

changed state to up
ip address 192.168.103.1 255.255.255.0
R1(config-if)#ip address 192.168.103.1 255.255.255.0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface FastEthernet0/0
R1(config-if)#

```

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/1/0

Port Status
Duplex ☒ Full Duplex
Clock Rate 128000
IP Configuration
IP Address 192.168.101.1
Subnet Mask 255.255.255.0
Tx Ring Limit 10

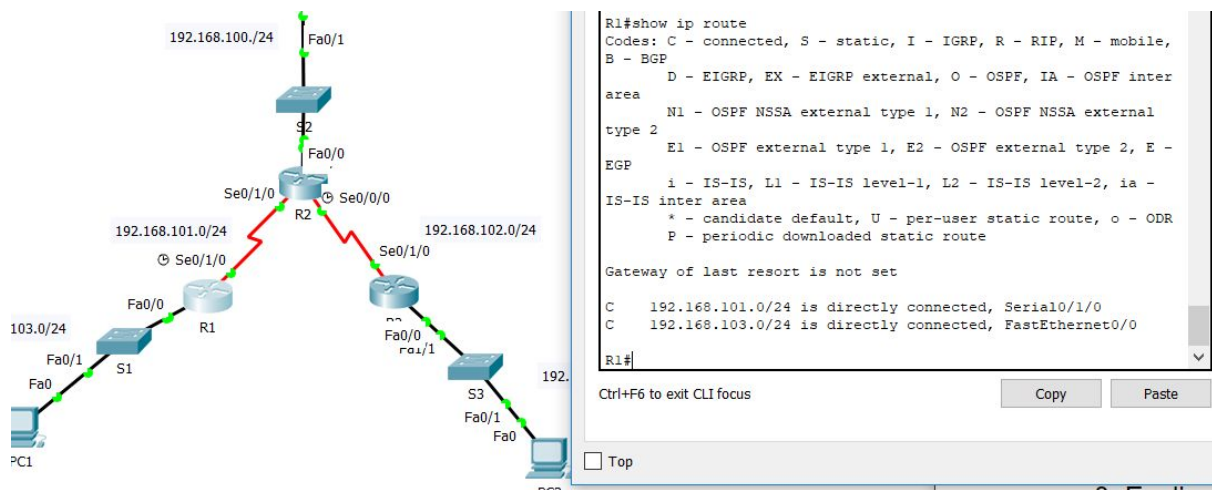
Equivalent IOS Commands

```

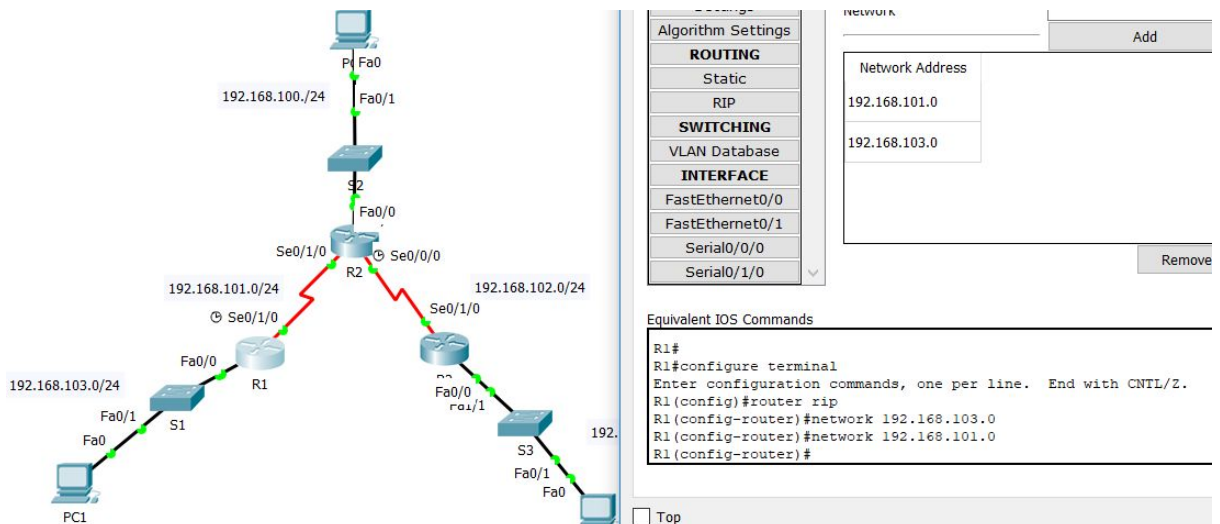
R1(config)#interface Serial0/1/0
R1(config-if)#ip address 192.168.101.1 255.255.255.0
R1(config-if)#ip address 192.168.101.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#

```

- Encapsulamiento
- Verifique el estado de las interfaces
- Muestre la tabla de enrutamiento de cada router

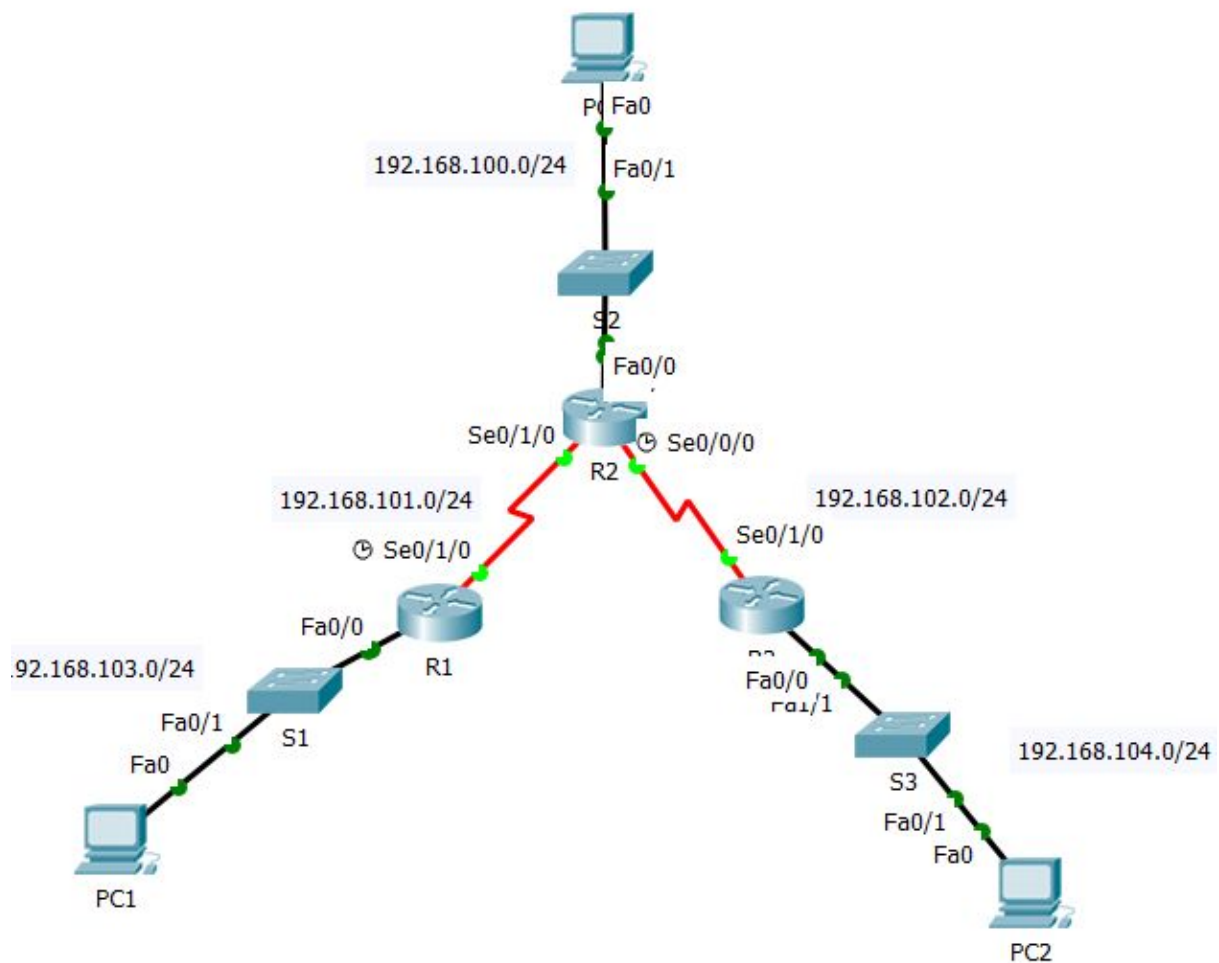


8. Configurar el protocolo de enrutamiento dinámico RIP v1 para todos los routers



9. Visualizar y explicar la tabla de enrutamiento en cada router

10. Elija un registro de alguna de las tablas de enrutamiento mostradas y explicar detalladamente el significado de cada campo del mismo



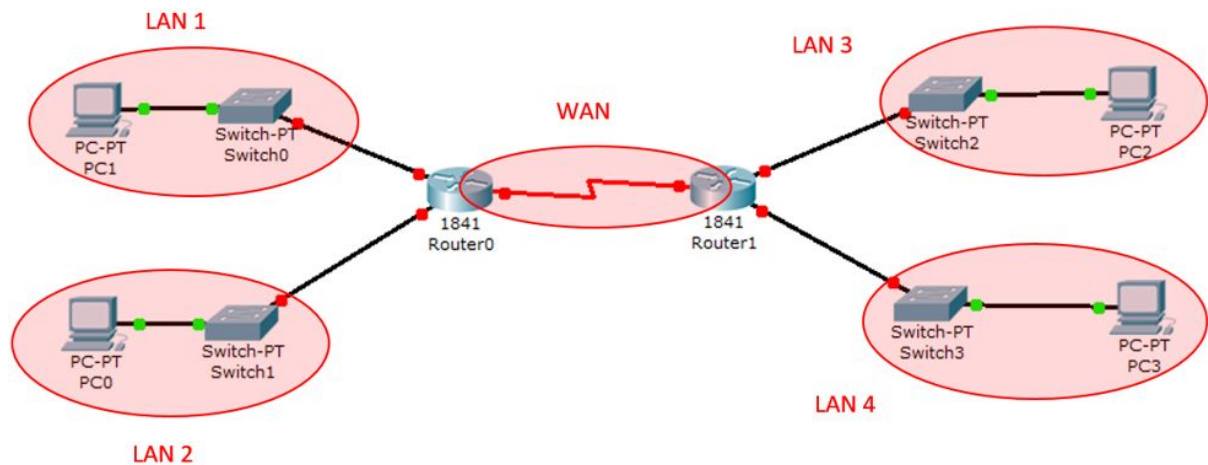
11. Guardar la configuración de cada router
12. Verificar la configuración en cada router usando el comando *show ip protocols*. Este comando muestra el protocolo de enrutamiento configurado actualmente en el router. Se puede utilizar este resultado para verificar la mayoría de los parámetros RIP y confirmar que:
 - El enrutamiento RIP está configurado.
 - Las interfaces correctas envían y reciben las actualizaciones RIP.
 - El router publica las redes correctas.
 - Los vecinos del RIP están enviando actualizaciones.

PROTOCOLO DE ENRUTAMIENTO RIP v2

Calculadora IP

VI. Ejercicio Propuesto

En el escenario de la figura 1, haga las modificaciones del caso para colocar dos switchs en los extremos de la comunicación de modo que se pueda ampliar la red a otras PCs, tal como se muestra en la figura 11:



Considere que las LAN tienen la siguiente cantidad de hosts:

LAN 1: 5 hosts

LAN 2: 2 hosts

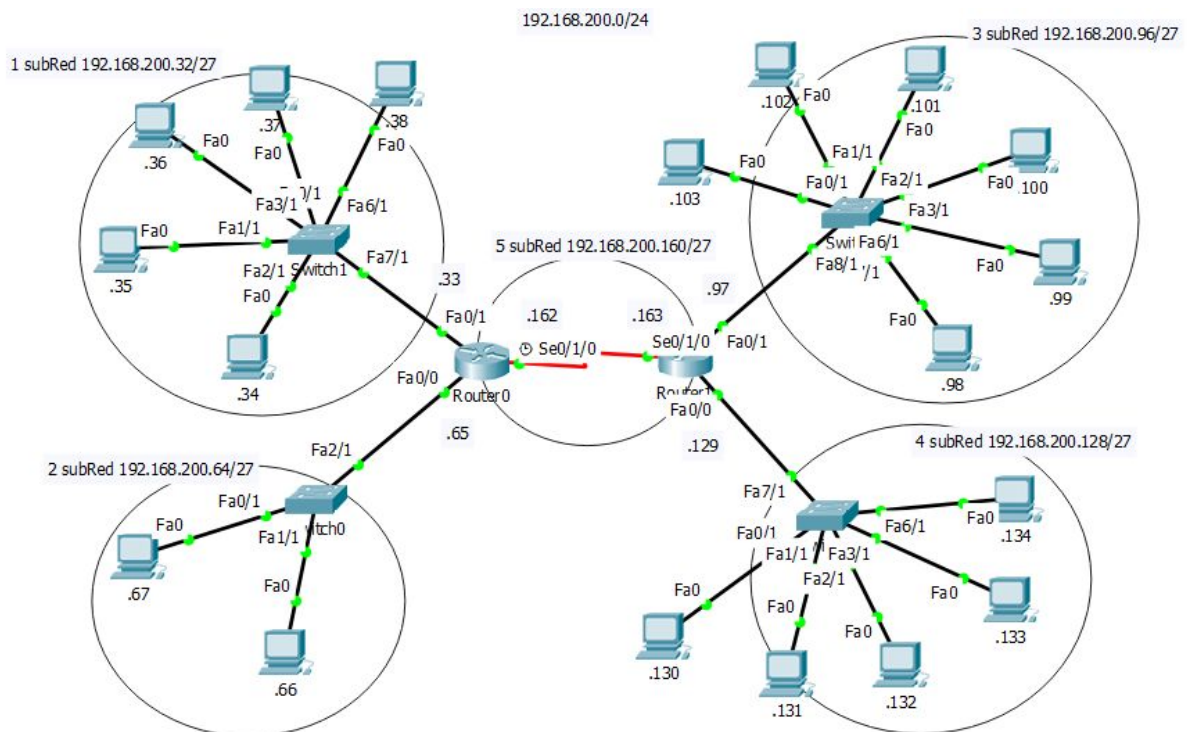
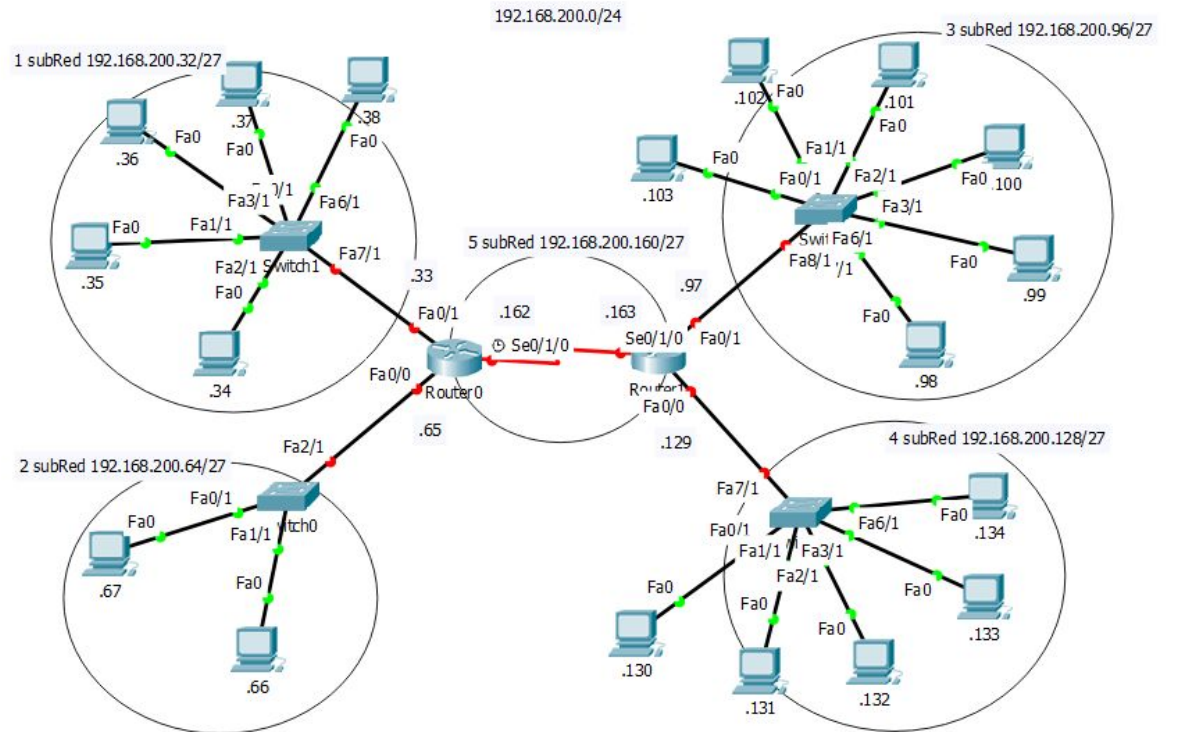
LAN 3: 6 hosts

LAN 4: 5 hosts

Para el direccionamiento, considere que sólo se dispone de la red IP 192.168.200.0 /24 y emplee enrutamiento dinámico con RIP v2. Presente el escenario obtenido

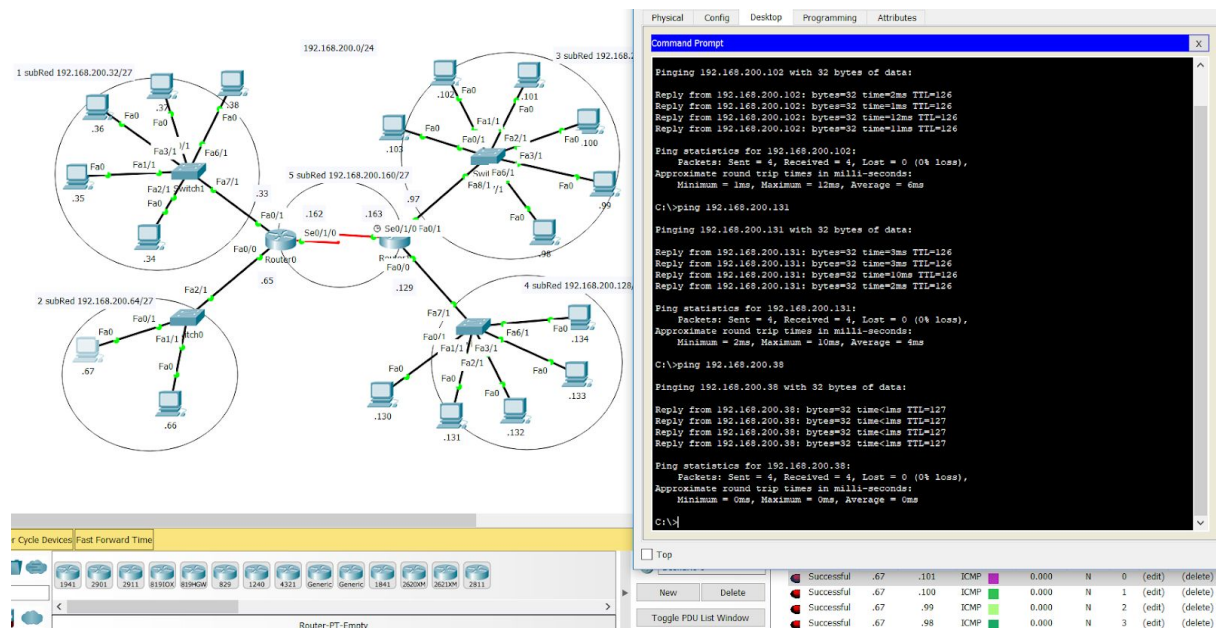
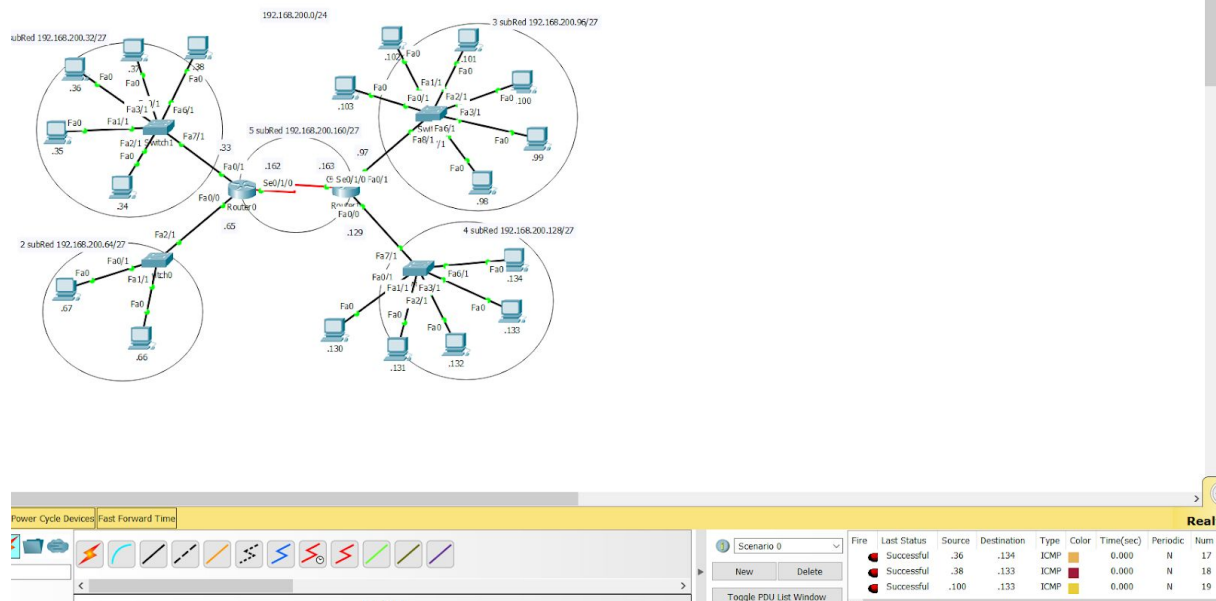
Nota: para activar la versión 2 y permitir el subneteo para trabajar en una sola red al configurar los routers, deberán incluir el comando version 2

```
Router(config)# router rip
Router(config-router)# network X.X.X.X
Router(config-router)# network Y.Y.Y.Y
Router(config-router)# versión 2
Router(config-router)# exit
```

```
Router(config)#router rip
Router(config-router)#network 192.168.200.0
Router(config-router)#version 2
Router(config-router)#exit
```

```
Router(config)#router rip
Router(config-router)#network 192.168.200.0
Router(config-router)#version 2
Router(config-router)#exit
```



VI. CONCLUSIONES.

PRIMERA: El enrutamiento dinámico, permite buscar el mejor camino a base de las métricas. (saltos)

SEGUNDA: La versión 2 del enrutamiento permite el subneteo, versatilidad.

TERCERA: El comando show ip config, permite saber el enrutamiento y alcance de la red.

CUARTA: De igual manera el comando show ip protocol muestra el protocolo usado y sus características.

VII. CUESTIONARIO

6.1 ¿Cómo se borran las claves?

```
(config)#line console 0
(config-line)#no password
(config-line)#Exit
(config)#config-register 0x2102
(config)#exit
#copy running-config startup-config
#reload [1]
```

6.2 ¿Cómo se eliminan rutas?

```
Router1(config)# no ip route
Deshabilitar rip: Router1(config)# no router rip
Deshabilitar summarización automática de ruta por defecto en RIPv2:
Router1(config-router)# no auto-summary [2]
```

6.3 Indique los comandos para colocar clave a los modos de conexión auxiliar y terminales virtuales

Configurar una contraseña al Puerto Auxiliar

```
delfirosales# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
delfirosales(config)# line aux 0
delfirosales(config-line)# password passaux
delfirosales(config-line)# login
delfirosales(config-line)#
```

Configurar un Password para la Consola

```
delfirosales(config)# line console 0
delfirosales(config-line)# password passconsole
delfirosales(config-line)# login
delfirosales(config-line)# [3]
```

6.4 Indique las características más importantes del protocolo de enrutamiento RIP v1 y v2

- V1:

RIPv1 es un protocolo de enrutamiento vector-distancia .

RIPv1 es un protocolo de enrutamiento con clase. Los protocolos de enrutamiento con clase solo admiten las redes que no están divididas en subredes. Los protocolos de enrutamiento con clase no envían información de máscara de subred con sus actualizaciones de enrutamiento. En otras palabras, si tiene una red en subredes en su dominio de enrutamiento RIPv1, RIPv1 anunciará esa red a otra como una red no suscrita.

RIPv1 no admite VLSM (máscara de subred de longitud variable) .

RIPv1 admite el valor métrico máximo (conteo de saltos) de 15. Cualquier enrutador que se encuentre a más de 15 saltos de distancia se considera como inalcanzable.

RIPv1 envía actualizaciones de enrutamiento periódicamente cada 30 segundos como transmisiones utilizando la dirección IP de destino como dirección IP de difusión limitada 255.255.255.255 . Dado que las actualizaciones se envían utilizando la dirección IP de destino de la dirección IP de difusión limitada 255.255.255.255, cada enrutador debe procesar los mensajes de actualización de enrutamiento (ya sea que estén ejecutando RIPv1 o no).

RIPv1 no admite la autenticación de mensajes de actualización (texto sin formato o MD5).

- V2:

RIPv2 es un protocolo de enrutamiento híbrido . Un protocolo de enrutamiento híbrido es básicamente un protocolo de vector de distancia que incluye algunas características de los protocolos de enrutamiento de estado de enlace .

RIPv2 es un enrutamiento sin clase, lo que nos permite usar redes subred también.

RIPv2 tiene la opción de enviar una máscara de red en la actualización para permitir el enrutamiento sin clase.

RIPv2 admite VLSM (enmascaramiento de subred de longitud variable) .

RIPv2 admite el valor métrico máximo (conteo de saltos) de 15. Cualquier enrutador que se encuentre a más de 15 saltos de distancia se considera como inalcanzable.

RIPv2 soporta actualizaciones activadas.

Las actualizaciones de enrutamiento RIPv2 se envían como tráfico de multidifusión en la dirección de multidifusión de destino de 224.0.0.9. Las actualizaciones de multidifusión reducen el tráfico de red. Las actualizaciones de enrutamiento de multidifusión también ayudan a reducir la sobrecarga de procesamiento de mensajes de actualización de enrutamiento en enrutadores que no ejecutan RIPv2. Solo los enrutadores que ejecutan RIPv2 se unen al grupo de multidifusión 224.0.0.9. Otros enrutadores que no ejecutan RIPv2 pueden simplemente filtrar el paquete de actualización de enrutamiento en la Capa 2.

RIPv2 admite la autenticación de mensajes de actualización RIPv2 (texto sin formato o MD5). La autenticación ayuda a confirmar que las actualizaciones provienen de fuentes autorizadas. [4]

6.5 ¿Qué significa actualizaciones desencadenadas?

Las actualizaciones activadas envían actualizaciones parciales (no completas) cuando ocurre un cambio de métrica. Reduce la posibilidad de problemas de conteo a infinito, acelera la convergencia y ahorra ancho de banda de enlace ya que la actualización solo contiene las redes afectadas. Si tenemos R1, R2 y R3 tan pronto como R2 pierde la ruta a R3, debe informar inmediatamente a R1 que se pierde la ruta a R3. Así R1 instalará inmediatamente la ruta alternativa. [5]

6.6 ¿Qué se entiende por convergencia de la red?

La convergencia de la red se produce cuando todos los routers tienen información completa y precisa acerca de toda la red, como se muestra en la figura 1. El tiempo de

convergencia es el tiempo que los routers tardan en compartir información, calcular las mejores rutas y actualizar sus tablas de enrutamiento. Una red no es completamente operativa hasta que la red haya convergido; por lo tanto, la mayoría de las redes requieren tiempos de convergencia breves.[6]

6.7 Qué diferencia hay entre la orden: *copy run start* y la orden: *copy running-config startup-config*?

Las configuraciones actuales del router son almacenadas en la memoria RAM, este tipo de memoria pierde el contenido al apagarse el router. Para que esto no ocurra es necesario poder hacer una copia a la NVRAM. El comando copy se utiliza con esta finalidad, identificando un origen con datos a guardar y un destino donde se almacenaran esos datos. Se puede guardar la configuración de la RAM a la NVRAM, de la RAM a un servidor TFTP, etc.

MADRID#copy running-config startup-config
Copia de la RAM a la NVRAM

MADRID#copy startup-config running-config
Copia de la NVRAM a la RAM [7]

6.8 ¿Cómo se almacena la configuración del router en una USB?

Router# dir usbflash0:

Directory of usbflash0:/

1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T
63158272 bytes total (33033216 bytes free)

Lo ideal es que la memoria flash USB pueda contener varias copias de las configuraciones de Cisco IOS y varias configuraciones del router. La memoria flash USB permite que un administrador mueva y copie fácilmente esos archivos y configuraciones de IOS de un router a otro. En numerosas ocasiones, el proceso de copiado puede ser mucho más rápido que a través de una LAN o una WAN.

6.9 ¿Cuáles son los modos de usuario admitidos por los routers CISCO?

Modo usuario: permite consultar toda la información relacionada al router sin poder modificarla. El shell es el siguiente:

Router >

- Modo usuario privilegiado: permite visualizar el estado del router e importar o exportar imágenes de IOS. El shell es el siguiente:

Router #

- Modo de configuración global: permite utilizar los comandos de configuración generales del router. Shell:

Router (config) #

- Modo de configuración de interfaces: permite utilizar comandos de configuración generales del router. Shell:

Router (config-if) #

- Modo de configuración de línea: permite configurar una línea (ej. Acceso al router por Telnet). Shell:
Router (config-line)#

6.10 ¿Qué otros protocolos dinámicos existen? Describa

- Open Short Path First (OSPF)

OSPF es un protocolo universal basado en el algoritmo de estado de enlace, desarrollado por el IETF para sustituir a RIP. Básicamente, OSPF utiliza un algoritmo que le permite calcular la distancia más corta entre la fuente y el destino al determinar la ruta para un grupo específico de paquetes.

- Interior Gateway Protocol (IGRP)

IGRP fue diseñado por Cisco a mediados de los ochenta, para corregir algunos de los defectos de RIP y para proporcionar un mejor soporte para redes grandes con enlaces de diferentes anchos de banda, siendo un protocolo propietario de Cisco. IGRP es un protocolo de enrutamiento por vector de distancia capaz de utilizar hasta 5 métricas distintas (ancho de banda K1, retraso K3, carga, fiabilidad, MTU), utilizándose por defecto únicamente el ancho de banda y el retraso. Estas métricas pueden referirse al ancho de banda, a la carga (cantidad de tráfico que ya gestiona un determinado router) y al coste de la comunicación (los paquetes se envían por la ruta más barata).

- Enhanced IGRP – EIGRP

Basado en IGRP y como mejora de este, es un protocolo híbrido que pretende ofrecer las ventajas de los protocolos por vector de distancia y las ventajas de los protocolos de estado de enlace. EIGRP soporta VLSM y soporta una convergencia muy rápida. EIGRP publica sus rutas sólo a los routers vecinos. Para la configuración de OSPF se requiere un número de proceso, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers. Los administradores acostumbran usar un número de SA como número de proceso.

- Border Gateway Protocol (BGP)

Es un protocolo de enrutamiento por vector de distancia usado comúnmente para enrutar paquetes entre dominios, estándar en Internet. BGP gestiona el enrutamiento entre dos o más routers que sirven como routers fronterizos para determinados Sistemas Autónomos. BGP versión 4 (BGP-4), es el protocolo de enrutamiento entre dominios elegido en Internet, en parte porque administra eficientemente la agregación y la propagación de rutas entre dominios. Aunque BGP-4 es un protocolo de enrutamiento exterior, también puede utilizarse dentro de un SA como un conducto para intercambiar actualizaciones BGP.

VIII. BIBLIOGRAFÍA

[1] *Poner y Eliminar el Password del Router Cisco*

<https://aldovillagas.wordpress.com/2011/05/05/poner-y-eliminar-el-password-del-router-cisco/>

[2] *Routers Cisco | Comandos Packet Tracer*

<http://eltallerdelbit.com/comandos-configuracion-routers-cisco>

[3] *Configuraciones Básicas de un Router o Switch Cisco*

<https://delfirosales.blogspot.com/2011/02/configuraciones-basicas-de-un-router-o.html>

[4] *Diferencia entre RIPv1 y RIPv2*

<http://www.omniseu.com/cisco-certified-network-associate-ccna/difference-between-ripv1-and-ripv2.php>

[5] *Actualizaciones desencadenadas*

<https://www.certificationkits.com/cisco-certification/ccna-articles/cisco-ccna-distance-vector-routing-protocols-2/cisco-ccna-triggered-updates/>

[6] *Aspectos básicos de la operación de los protocolos de routing*

<http://www.itesa.edu.mx/netacad/switching/course/module7/7.1.3.5/7.1.3.5.html>

[7] *Guardar, copiar y borrar las configuraciones*

<http://aprenderedes.com/2006/09/guardar-copiar-y-borrar-las-configuraciones/>