FACULTAD DE INGENIERÍA
Y CIENCIAS
AGROPECUARIAS

GENERACIÓN Y DESARROLLO DE UN DOCUMENTO GUÍA DE PRÁCTICAS EN LA MATERIA DE INTERNETWORKING EN LA UDLA

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de Tecnólogo en Redes y Telecomunicaciones

Profesor Guía
Ing. Nelson Esteban Salgado Reyes

Autor
Santiago Samuel Cuasquer Caicedo

Año
2015

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

……..

Nelson Esteban Salgado Reyes

Ingeniero Informático

1709609588

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

……..…….

Santiago Samuel Cuasquer Caicedo

1718216573

AGRADECIMIENTO

Quedo muy agradecido a Dios y cada uno de los miembros de mi familia por ser motivación de cada logro que he conseguido.

DEDICATORIA

Dedico mi trabajo final a todos los miembros de mi familia, a quienes retribuiré los frutos del logro que conseguiré.

RESUMEN

El objetivo de este trabajo es el de estandarizar las prácticas que se realizarán en la materia de Internetworking dictada en la carrera de Redes y Telecomunicaciones de la Escuela de Tecnologías de la UDLA, en la cual se contempla el aprendizaje de protocolos y configuraciones para comunicar redes distintas.

La estandarización de prácticas para esta materia tiene por objetivo la igualdad en los conocimientos adquiridos en esta materia independientemente del profesor que la dicte. Las prácticas en cuestión cubrirán un total de 11 sesiones de clase que estarán contempladas en 10 prácticas donde la última tomará 2 sesiones, estas describen: materiales o herramientas a usarse durante la práctica, objetivo general, objetivos específicos, marco teórico, trabajo preparatorio, desarrollo de la práctica, resultados de aprendizaje, conclusiones y cuestionario para evaluación.

ABSTRACT

The objective of this work is to standardize the practices to realize in the subject of Internetworking on the career Networking and Telecommunications of UDLA University, where is contemplated the learning of protocols and configurations to communicate different networks.

The standardization of these practical laboratories seeks equality at knowledge acquired independently of the teacher. The practical laboratories cover 11 class sessions where is contemplated 10 laboratories and the last one takes two class sessions, these practical laboratories describes: materials or tools to use during the laboratory, general objective, specific objectives, theoretical framework, spadework, development, learning outcomes, conclusions and a quiz for student evaluation.

ÍNDICE

Introducción

El internet está conformado por la conexión de redes distintas a lo largo de todo el mundo, para poder lograrlo se estandarizó los protocolos de comunicación de manera que sea posible el intercambio de información independientemente de la arquitectura de una red, a su vez, se crearon protocolos tales como BGP para interconectar redes con protocolos de enrutamiento distintos y TCP/IP para la comunicación indistintamente del usuario. Internetworking engloba este concepto, el poder interconectar redes con tecnologías diferentes para el intercambio de datos.

Este trabajo tiene por objetivo explicar el funcionamiento de los protocolos que hacen posible la comunicación de redes con tecnologías diferentes y mostrar las opciones que existen para la trasmisión de datos tomando también en consideración que el hardware forma parte de la solución para implementar una red. El dimensionamiento del equipamiento activo, respecto a las capacidades de los dispositivos y las características que brinde el software de los mismos, permitirá las configuraciones y conexiones necesarias para lograr una comunicación entre redes distintas. Este tipo de implementaciones puede estar sujeto al requerimiento de un cliente, considerando este caso, se ha realizado laboratorios en los cuales se presentan casos básicos con requerimientos para que se arme y configure la red en base a los mismos.

Las prácticas representan un procedimiento de implementación en el cual se dimensiona el hardware, sus módulos, el software de los dispositivos de red y las configuraciones necesarias para lograr comunicar dos redes internas LAN a través de un enlace WAN, o redes distintas dentro de la misma LAN.

Se han tomado en cuenta textos principalmente referidos a configuraciones en dispositivos Cisco ya que esta marca y la academia de redes que posee, la convierten en una patente dominante en el mercado y una excelente referencia de entrada al mundo del Internetworking. Libros corporativos, autores de libros

técnicos y personas certificadas en Cisco son los referentes principales para la creación de este trabajo.

También se han hecho referencias para definiciones menores considerando páginas especializadas en material estudiantil y personas relacionadas a la carrera de telecomunicaciones como el caso del Ingeniero Víctor Ochoa.

Los autores corporativos se refieren a aquellas publicaciones hechas por Cisco, mientras que personas particulares como Oscar Gerometta instructor de Cisco y Francisco Valencia, tienen varias e importantes certificaciones en la marca.

CAPÍTULO I CONFIGURACIÓN DE UN ENLACE TRONCAL Y REDES VLAN

Materiales / herramientas

Descripción de los equipos/herramientas/*software* necesitados para la práctica.

- 1 Computador (laboratorio de redes)
- 1 Cisco Packet Tracer

1.1 Objetivo general

Incorporar redes VLAN en una topología para segmentar el dominio de *broadcast* y agregar un enlace troncal para lograr la comunicación entre las distintas redes virtuales creadas.

1.2 Objetivos específicos

1. Desarrollar una topología de red en las tres capas del modelo jerárquico de Cisco.
2. Analizar el segmentado de dominios de *broadcast* en un *switch*.
3. Configurar redes VLAN y enlaces troncales.

1.3 Marco teórico

Los componentes que se configurarán en esta práctica son los siguientes:

1.3.1 Router

> "Dispositivo de red que trabaja en la capa de red del modelo OSI, por lo cual está en la capacidad de intercomunicar redes lógicamente distintas, también se usa para comunicar redes geográficamente alejadas. El *router* tiene varias capacidades ya que incluso puede tener características de capa 4, es decir, se le puede atribuir funcionalidades de *firewall*; puede ser un dispositivo modular para añadir las interfaces que sean necesarias para la implementación de una red, además de

> crear políticas basadas en direcciones IP o en números de puerto.” (Kioskea, 2014).

1.3.2 Switch

El conmutador es un equipo de red que funciona en la capa de enlace de datos del modelo OSI, encargado de transportar tramas entre varios segmentos de red hasta el host apropiado. Este dispositivo de red tiene la capacidad de crear redes lógicas para segmentar los dominios de *broadcast*.

> “Así mismo, existen *switches* modulares y con características de capa de red, e incluso pueden brindar un servicio de equilibrio de carga en donde se puede administrar el tráfico de números de puerto. El *switch* se caracteriza por su capacidad de densidad de puerto, que es lo que le permite manejar gran cantidad de datos entre origen y destino.” (Kioskea, 2014).

1.3.3 Cable de datos

Es el medio físico por el cual se comunican datos entre los dispositivos de red, este medio usualmente puede ser par trenzado o fibra óptica.

1.3.4 Packet tracer

“Es un simulador gráfico de redes desarrollado por Cisco como herramienta de entrenamiento para obtener los conocimientos para certificarse CCNA.” (Ochoa, 2010, p. 5).

1.3.5 Dominio de broadcast

Oscar Gerometta (2007) afirma:

> "El broadcast es la comunicación de una terminal origen a todas las terminales de un dominio de *broadcast* (red, subred o VLAN). (…). Adicionalmente, problemas de configuración o fallos de los dispositivos o de las terminales pueden provocar la presencia de montos muy importantes de *broadcast* en la red que quitan recursos para el procesamiento del tráfico de datos o la operación regular de la red, bajando de modo notable su performance."

1.3.6 Host

"Host o anfitrión es usado en informática para referirse a las computadoras conectadas a una red, que proveen y utilizan servicios de ella." (Wikipedia, 2014).

1.3.7 VLAN

Una VLAN es un conjunto de redes lógicas y autónomas; tienen los mismos atributos que una LAN física, solo que permiten agrupar estaciones finales incluso si no se encuentran físicamente en el mismo segmento de LAN.

> "Las VLAN se asocian generalmente con subredes IP. Por ejemplo, todas las estaciones finales en una subred IP particular, pertenecen a la misma VLAN. El tráfico entre las VLAN se debe dirigir, para esto se asignan puertos LAN a una red VLAN en forma manual." (Cisco, 2012, p. 23_2).

1.3.8 Enlace troncal

El enlace troncal consigue la comunicación entre diferentes VLAN con la ayuda del protocolo 802.1Q, el cual crea un túnel virtual que permite a los dispositivos con capacidades de capa 3 utilizar un solo medio físico para intercomunicar a

clientes con diferentes VLANs, preservando al mismo tiempo los ID de VLAN del cliente y mantener el tráfico en los diferentes usuarios.

Un puerto configurado para soportar un túnel 802.1Q se llama un enlace troncal. Al configurar un túnel, se asigna un puerto de túnel a una VLAN, esto se logra mediante las llamadas interfaces virtuales o sub-interfaces. Los túneles 802.1Q no se limitan a configuraciones de túnel punto a punto. Cualquier puerto correspondiente a una VLAN es un punto de entrada y salida. Un túnel 802.1Q puede tener tantos puertos de túnel como sea necesario para conectar distintas VLAN.

Los *switches* cliente están conectados mediante un enlace troncal con un túnel 802.1Q, sólo utilizan un proveedor de servicios de VLAN para intercomunicarlas todas.

> “Con un túnel 802.1Q, el tráfico etiquetado para los clientes viene desde un puerto de enlace troncal en un dispositivo proveedor de servicios VLAN y entra en el conmutador de acceso para luego entregarlo en el puerto con el ID de la red virtual que corresponda.” (Cisco, 2012, p. 26_1-2).

1.4 Trabajo preparatorio

Conseguir Packet Tracer versión 6.0.1 (mínimo).

Disponer de un computador de laboratorio o propio con características como sistema operativo Windows (7, 8, 8.1), Linux (Ubuntu, Fedora), procesador 200 MHz o superior, 64 MB RAM o superior.

Conocer el funcionamiento básico de Cisco Packet Tracer y los comandos básicos de configuración para dispositivos cisco, como por ejemplo entrar en el modo usuario con privilegios, guardar cambios y visualizar las configuraciones guardadas.

1.5 Desarrollo de la práctica

Pasos a seguir:

1) Colocar los siguientes elementos en el emulador Packet Tracer:

1.1. *Router* 1841, cantidad 1. No es necesario agregar módulos adicionales.

Figura 1. *Router* Cisco 1841, ícono y apariencia física.
Tomado de Cisco Packet Tracer.

1.2. *Switch* 2950, 24 puertos 10/100 Mbps (*Fast ethernet*), cantidad 2.

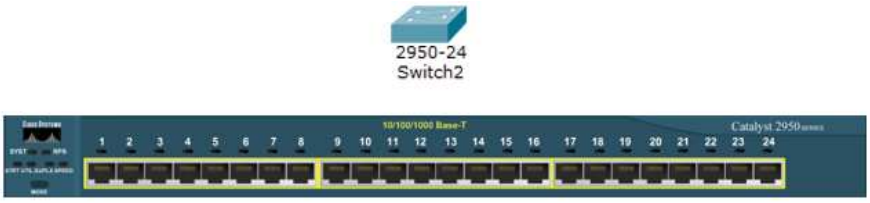

Figura 2. *Switch* Cisco 2950, ícono y apariencia física.
Tomado de Cisco Packet Tracer.

1.3. Host con tarjeta de red *Fast ethernet*, cantidad 6.

Figura 3. Computador, ícono y apariencia física.

Tomado de Cisco Packet Tracer.

2) Realizar la topología de red en Packet Tracer según la Figura 4.

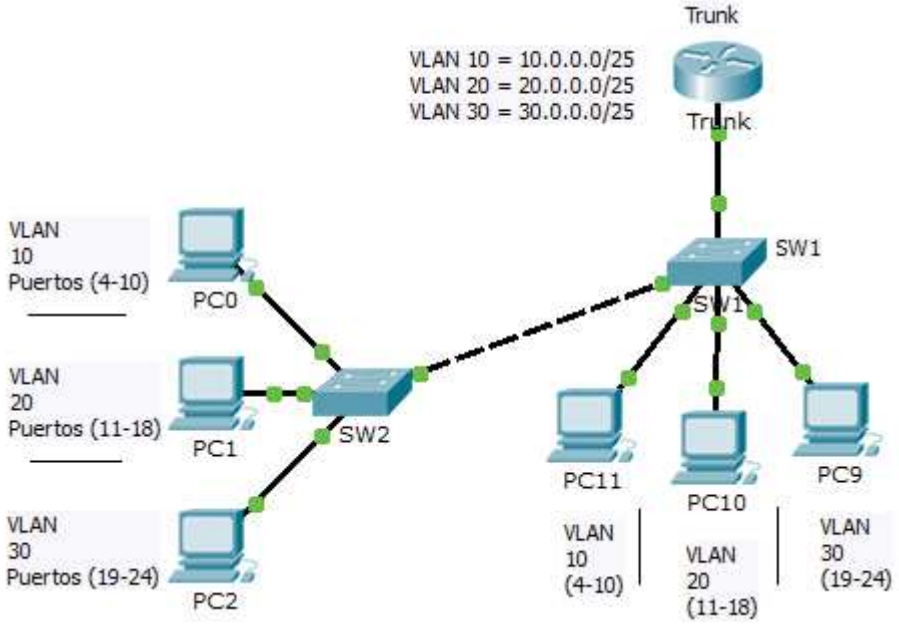

Figura 4. Topología física de la práctica.
Tomado de Cisco Packet Tracer.

3) Asignar nombres a los *Switches* y *Router* de la red.

Router>enable

Router#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#no ip domain-lookup

Router(config)#hostname Trunk

Trunk(config)#

Switch>en
Switch#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname SW1
SW1(config)#

Switch>en
Switch#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname SW2
SW2(config)#

4) Asignar las contraseñas de consola, *enable* y telnet a los *switches* y el *router*.
   Password Enable:
   Trunk(config)#enable secret cisco
   Password Consola:
   Trunk(config)#line console 0
   Trunk(config-line)#password admin
   Trunk(config-line)#login
   Trunk(config-line)#exit
   Password Telnet:
   Trunk(config)#line vty 0 4
   Trunk(config-line)#password admin
   Trunk(config-line)#login

5) Crear el enlace troncal en el *router* mediante la implementación de interfaces virtuales.

5.1. Activar la interfaz fa0/0.

```
Trunk >enable
Trunk #config terminal
Trunk (config)#int fa0/0
Trunk (config-if)#no shut
```

5.2. Crear una interfaz virtual dentro del puerto fa0/0. Seguido de un punto debe estar el número de VLAN correspondiente.

```
Trunk(config)#int fa0/0.10
```

5.3. Especificar que esta interfaz virtual será un túnel para la VLAN 10.

```
Trunk(config-subif)#encapsulation dot1q 10
```

5.4. Asignar la dirección IP correspondiente.

```
Trunk(config-subif)#ip addr 10.0.0.1 255.255.255.0
Trunk(config-subif)#exit
```

5.5. Realizar el mismo procedimiento para cada interfaz virtual considerando la VLAN a la que pertenecerá.

6) Crear las VLAN en cada *switch*.

6.1. Asignar un nombre a cada Vlan.

```
SW1#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#vlan 10
SW1(config-vlan)#name vlan10
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#name vlan20
SW1(config-vlan)#exit
```

SW1(config)#vlan 30
SW1(config-vlan)#name vlan30
SW1(config-vlan)#exit

6.2. Realizar el mismo procedimiento en el segundo *switch* SW2.

7) Asignar los puertos a su correspondiente VLAN según la Figura 4.
SW1(config)#int range fa0/4-10
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#exit
SW1(config)#int range fa0/11-18
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 20
SW1(config-if-range)#exit
SW1(config)#int range fa0/19-24
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 30
SW1(config-if-range)#exit

8) Configurar enlaces troncales.

8.1. Configurar la interfaz fa0/1 del *switch* SW1 como enlace troncal.
SW1(config)#int fa0/1
SW1(config-if)#switchport mode trunk

8.2. Configurar las interfaces que se comuniquen entre los *swtiches* como enlace troncal.
SW1(config)#int fa0/2
SW1(config-if)#switchport mode trunk

SW2(config)#int fa0/2

```
SW2(config-if)#switchport mode trunk
```

9) Asignar una dirección IP a cada computador de acuerdo a su correspondiente VLAN.

10) Comprobar las VLAN creadas en los *switches* mediante el comando “show vlan”.

```
SW1#sh vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3
10   vlan10                            active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10
20   vlan20                            active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
30   vlan30                            active    Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24

SW2#sh vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/3
10   VLAN10                            active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10
20   vlan20                            active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
30   vlan30                            active    Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
```

11) Comprobar la conectividad realizando un ping entre computadores de distintas VLAN.

1.6 Resultados de aprendizaje

- Emplear configuraciones iniciales básicas en *routers* y *switches.*
- Listar los comandos para crear de redes virtuales VLAN, asignación a puertos físicos, identificación por nombres y comprobación de las configuraciones.

- Emplear configuraciones para logar comunicación entre redes virtuales mediante un enlace troncal con el protocolo IEEE 802.1Q.

1.7 Conclusiones

- Se puede segmentar un dominio de *broadcast* mediante redes VLAN para optimiza el ancho de banda de una red.
- Es posible crear enlaces troncales para conseguir la comunicación entre redes virtuales.
- Para transmitir varias redes virtuales por un mismo medio físico, se debe crear un enlace troncal.

1.8 Tiempo estimado de la práctica

Una sesión de clase.

1.9 Evaluación/ cuestionario

1. ¿Concluyó con éxito el ping realizado entre computadores de distintas VLAN?
2. ¿Cuál es el modo de puerto que se debe configurar entre dos *switches* que poseen redes virtuales VLAN?
3. ¿Es necesario que la VLAN y la interfaz virtual del *router* tengan el mismo número?

CAPÍTULO II CONFIGURAR UN SERVIDOR Y CLIENTES VTP

Materiales / herramientas

Descripción de los equipos/herramientas/*software* necesitados para la práctica.

- 1 Computador (laboratorio de redes)
- 1 Cisco Packet Tracer

2.1 Objetivo general

Incorporar el protocolo VTP a una topología para simplificar y reducir el tiempo de administración de los *switches* en una red.

2.2 Objetivos específicos

a) Configurar el protocolo VTP para permitir administrar las VLAN de una red con varios conmutadores, mediante la implementación de un servidor y varios clientes VTP.
b) Analizar las ventajas de centralizar la gestión de redes VLAN mediante un solo dispositivo.

2.3 Marco teórico

2.3.1 VTP

> "VLAN *Trunk Protocol* es un protocolo de mensajes de nivel 2 propietario de Cisco, que circula a través de puertos de *trunk* (ISL o IEEE 802.1q) en la VLAN 1 y que permite mantener la consistencia en las VLAN de la red. (…)." (Valencia, 2011, p. 51).

> "VTP crea un dominio identificado con un nombre, y los *switches* que están en ese dominio comparten la configuración de la VLAN, de modo que se asegura la consistencia de esta información. Lo que se comparte el dominio de administración, el número de revisión de configuración y las VLAN conocidas con sus parámetros. Además, permite VTP *prunning*, la cual es una característica que permite ahorrar ancho de

banda en los enlaces *trunk*, eliminando los paquetes de una VLAN que no tenga puertos configurados en los *switches* que se conecten al que recibe la trama.

Los *router* no soportan VTP, por eso, si se introduce un *router* en medio de una red de *switches*, el dominio VTP se segmenta, y los *switches* no actualizarán su información de un lado a otro del *router*.

Se puede agregar una clave al tráfico VTP que los *switches* deberán emplear para dar información de las VLAN.

Cuando se modifica una VLAN en un *switch* servidor VTP, éste le pasa la nueva tabla a los demás que se configuran de acuerdo con esta si el número de revisión es superior al que tienen éstos.

Se puede configurar un *switch* para que trabaje en uno de estos tres modos:

- Servidor: En modo servidor se puede agregar, modificar o eliminar VLAN, y éste le mandará la información configurada a los otros *switches* del dominio. También se configura de otros servidores. Es el modo por defecto. Almacena la información en la NVRAM.
- Cliente: Recibe la información de un servidor. En él no se puede configurar VLAN. No almacena la información en la NVRAM.
- Transparente: No participan en del protocolo VTP, solo hacen envío de las tablas que los servidores envían a los clientes. Se puede crear VLAN, pero éstas no serán enviadas a nadie." (Valencia, 2011, p. 51).

"VTP minimiza los errores de configuración y las inconsistencias que pueden resultar en problemas como nombres de VLAN duplicados,

especificaciones incorrectas de tipo de VLAN y violaciones de seguridad. (…). Con VTP, se puede hacer cambios centralizados de configuraciones desde uno o más *switches* y se comunican automáticamente a los demás." (Cisco, 2012, p. 22_1-2).

2.4 Trabajo preparatorio

Conseguir Packet Tracer versión 6.0.1 (mínimo).

Disponer de un computador de laboratorio o propio con características como sistema operativo Windows (7, 8, 8.1), Linux (Ubuntu, Fedora), procesador 200 MHz o superior, 64 MB RAM o superior.

Conocer el funcionamiento básico de Cisco Packet Tracer.

Realizar con anticipación la topología de este laboratorio.

2.5 Desarrollo de la práctica

Pasos a seguir:

1) Colocar los siguientes elementos en el emulador Packet Tracer:

1.1. *Router* 1841, cantidad 1. No es necesario agregar módulos adicionales.

Figura 5. Router Cisco 1841, ícono y apariencia física.
Tomado de Cisco Packet Tracer.

1.2. *Switch* 2950, 24 puertos 10/100 Mbps (*Fast ethernet*), cantidad 4.

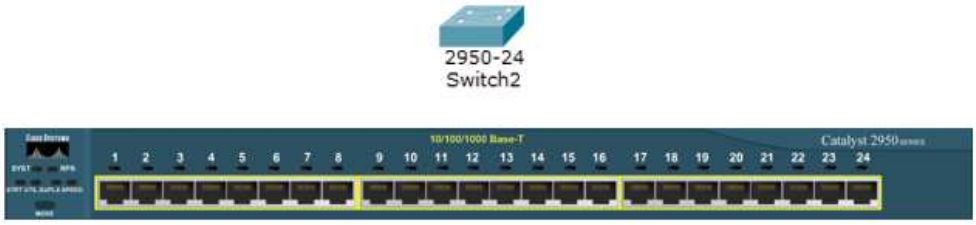

Figura 6. Switch Cisco 2950, ícono y apariencia física.

Tomado de Cisco Packet Tracer.

1.3. Servidor genérico de Cisco Packet Tracer, cantidad 1.

Figura 7. Servidor, ícono y apariencia física.

Tomado de Cisco Packet Tracer.

1.4. Host con tarjeta de red *fast ethernet*, cantidad 12.

Figura 8. Computador, ícono y apariencia física.

Tomado de Cisco Packet Tracer.

2) Realizar la topología de red en Packet Tracer según la Figura 9.

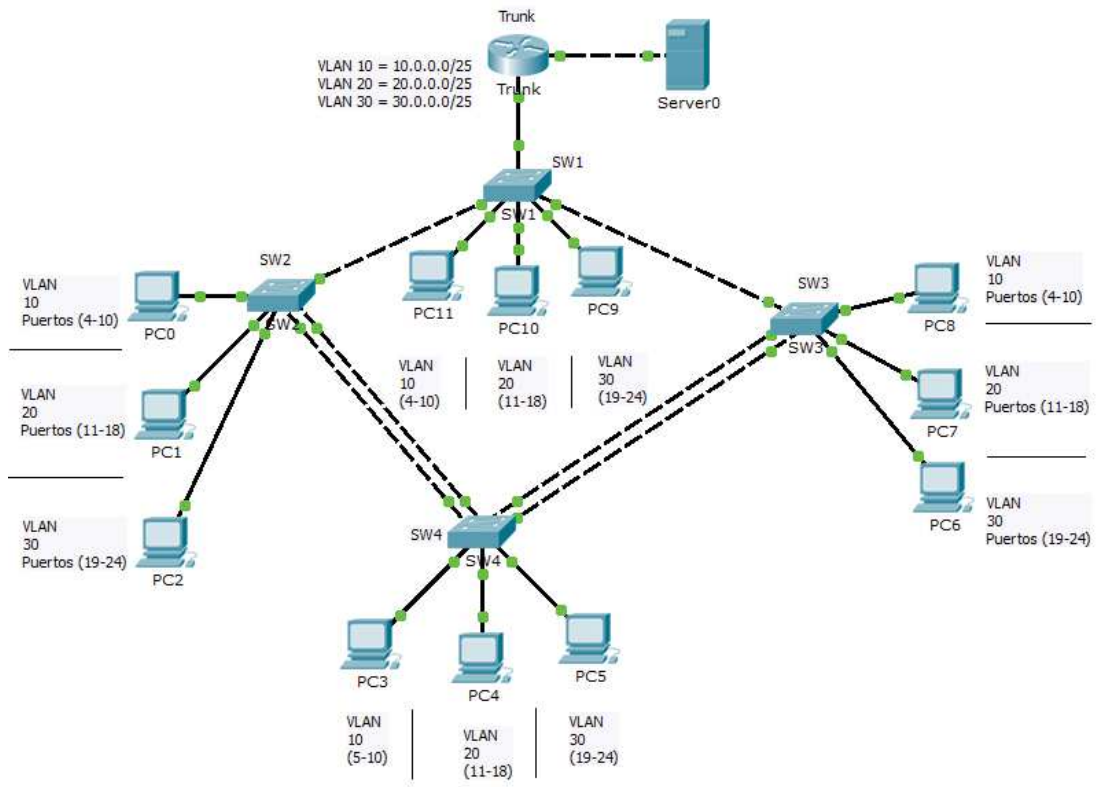

Figura 9. Topología de la práctica.

Tomado de Cisco Packet Tracer.

3) Asignar nombres a los s*witches* y r*outer* de la red. Ejemplo:

Router>enable

Router#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#no ip domain-lookup

Router(config)#hostname Trunk

Trunk(config)#

4) Crear el enlace troncal en el r*outer* llamado *trunk* mediante la implementación de interfaces virtuales.

4.1. Activar la interfaz fa0/0.

Trunk >enable

Trunk #config terminal
Trunk (config)#int fa0/0
Trunk (config-if)#no shut
Trunk (config-if)#exit

4.2. Crear una interfaz virtual dentro del puerto fa0/0, seguido de un punto debe estar el número de VLAN correspondiente.
Trunk(config)#int fa0/0.10

4.3. Especificar que esta interfaz virtual será un túnel para la VLAN 10. Considerar que el número de VLAN tiene que ser igual al número asignado a la sub-interfaz virtual en el *router*.
Trunk(config-subif)#encapsulation dot1q 10

4.4. Asignar la dirección IP correspondiente.
Trunk(config-subif)#ip addr 10.0.0.1 255.255.255.0
Trunk(config-subif)#exit

4.5. Realizar el mismo procedimiento para cada interfaz virtual considerando la VLAN a la que pertenecerá.

4.6. Crear la VLAN de administración:
Trunk(config)#int fa0/0.91
Trunk(config-subif)#enc dot1q 91 native
Trunk(config-subif)#ip addr 91.0.0.1 255.255.255.0
Trunk(config-subif)#exit

5) Crear las VLAN en el *switch* 1 (SW1).

5.1. Asignar un nombre a cada VLAN.
SW1#config ter
Enter configuration commands, one per line. End with CNTL/Z.

SW1(config)#vlan 10
SW1(config-vlan)#name vlan10
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#name vlan20
SW1(config-vlan)#exit
SW1(config)#vlan 30
SW1(config-vlan)#name vlan30
SW1(config-vlan)#exit
SW1(config)#vlan 91
SW1(config-vlan)#name admin
SW1(config-vlan)#exit

5.2. Cambiar la dirección IP de administración a la VLAN 91. Normalmente es la VLAN 1, se sugiere cambiarla por seguridad.
SW1(config)#int vlan 91
SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan91, changed state to up

SW1(config-if)#ip addr 91.0.0.2 255.255.255.0
SW1(config-if)#exit

6) Asignar los puertos a su correspondiente VLAN para todos los *switches* tal como en la Figura 9. Como ejemplo, los siguientes comandos:
SW1(config)#int range fa0/1-3
SW1(config-if-range)#switchport access vlan 91
SW1(config)#int range fa0/4-10
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#exit
SW1(config)#int range fa0/11-18
SW1(config-if-range)#switchport mode access

SW1(config-if-range)#switchport access vlan 20
SW1(config-if-range)#exit
SW1(config)#int range fa0/19-24
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 30
SW1(config-if-range)#exit

7) Configurar los enlaces troncales en el SW1.
SW1(config)#int range fa0/1-3
SW1(config-if-range)#switchport mode trunk
SW2(config-if-range)#switchport trunk vlan 91
SW2(config-if-range)#exit

8) Configurar a SW1 como servidor VTP.
SW1(config)#vtp mode server
Device mode already VTP SERVER.
SW1(config)#vtp domain udla.ec
Changing VTP domain name from NULL to udla.ec
SW1(config)#vtp version 2
SW1(config)#vtp password vtp1
Setting device VLAN database password to vtp1

9) Configurar VTP cliente en los *switches* SW2, SW3, SW4 como en el siguiente ejemplo:
SW2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW2(config)#vtp domain udla.ec
Changing VTP domain name from NULL to udla.ec
SW2(config)#vtp password vtp1
Setting device VLAN database password to vtp1

10) Crear enlaces troncales en cada *switch* y asignar los puertos a la correspondiente VLAN.

```
SW2(config)#int range fa0/1-3
SW2(config-if-range)#switchport mode trunk
SW2(config-if-range)#switchport trunk native vlan 91
SW2(config-if-range)#exit
SW2(config)#int range fa0/4-10
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 10
SW2(config-if-range)#exit
SW2(config)#int range fa0/11-18
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 20
SW2(config-if-range)#exit
SW2(config)#int range fa0/19-24
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 30
SW2(config-if-range)#exit
```

11) Configurar la dirección IP 91.0.0.1 como puerta de enlace predeterminada en todos los *switches* y asignar una dirección IP distinta a la interfaz “vlan 91” para la administración de cada *switch*, de la siguiente manera:

```
SW2(config)#ip default-gateway 91.0.0.1
SW2(config)#int vlan 91
SW2(config-if)#ip addr 91.0.0.2 255.255.255.0
```

12) Realizar el mismo proceso de configuración con los demás *switches* considerando la información de las VLAN en la Figura 9.

13) Configurar el servidor DNS según la Figura 10 y 11.

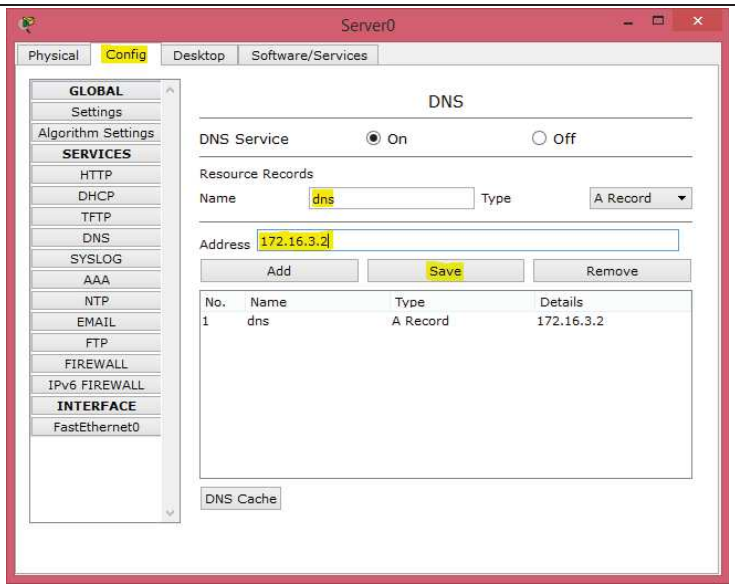

Figura 10. Ventana de configuración de servicios del servidor.

Tomado de Cisco Packet Tracer.

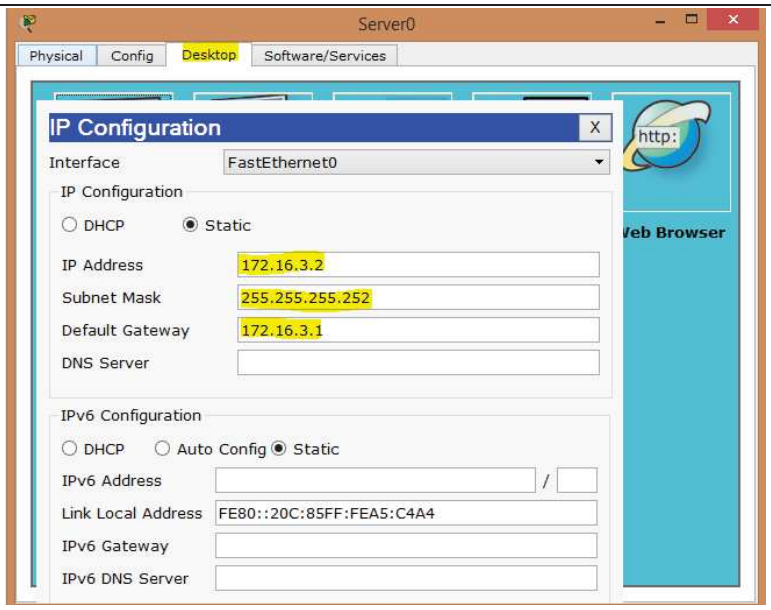

Figura 11. Ventana de configuración de interfaz del servidor.

Tomado de Cisco Packet Tracer.

14) Configurar la interfaz del *router* a la cual se conecte el servidor.

```
Trunk(config)#int fa0/1
Trunk(config-if)#ip addr 172.16.3.1 255.255.255.252
Trunk(config-if)#no shut
```

15) Asignar una dirección IP a cada computador de acuerdo a su correspondiente VLAN y el DNS 172.16.3.2

16) Comprobar las VLAN creadas en todos los clientes VTP mediante el comando "*show vlan*".

```
SW4#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   vlan10                            active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
20   vlan20                            active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
30   vlan30                            active    Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
91   admin                             active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode
Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
91   enet  100091     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
SW4#
```

17) Cambiar la configuración del *switch* SW4, de modo cliente a transparente.

SW4(config)#vtp mode transparent

18) Añadir una VLAN adicional en el *switch* SW4.

```
SW4(config)#vlan 50
SW4(config-vlan)#name prueba
SW4(config-vlan)#exit
SW4(config)#int fa0/24
SW4(config-if)#switchport access vlan 50
SW4(config-if)#end
```

19) Añadir una VLAN adicional en el *switch* SW1 y verificar en SW2 que se añada automáticamente.

```
SW1(config)#vlan 49
SW1(config-vlan)#name adicional
SW1(config-vlan)#end
```

```
SW2#sh vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   vlan10                            active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10
20   vlan20                            active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
30   vlan30                            active    Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
49   adicional                         active
91   admin                             active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

20) Comprobar la conectividad realizando un ping entre computadores de distintas VLAN.

21) Verificar en cualquier host, en la pestaña "*Desktop*", en la opción "*Web Browser*", si se conecta al servidor al momento de introducir su dirección IP.

2.6 Resultados de aprendizaje

- Emplear la configuración del protocolo VTP para una administración de redes VLAN jerarquizada
- Diferenciar entre los distintos modos que posee VTP.

2.7 Conclusiones

- La creación de redes VLAN en varios *switches* mediante un servidor VTP, resulta simple y útil a futuro si se quiere hacer modificaciones.
- Se puede administrar un dominio VTP desde diferentes *switches* servidores.
- Gracias a los diferentes modos de configuración que tiene VTP, si se desea mantener a un *switch* al margen del dominio VTP, se lo puede configurar en modo transparente y aún crear VLAN dentro de sí mismo sin afectar al resto de los *switches*.

2.8 Tiempo estimado de la práctica

Una sesión de clase.

2.9 Evaluación/ cuestionario

1. ¿Concluyó con éxito el ping realizado entre computadores?
2. ¿Qué sucede si se intenta añadir una VLAN en un *switch* cliente VTP?
3. Si se aumenta una VLAN en el servidor VTP ¿Se añade la configuración en los clientes VTP?
4. Al ingresar al servidor por medio de un host (paso 21) ¿Qué aparece en el primer link de la página HTML?

CAPÍTULO III CONFIGURACIÓN PORTFAST Y SEGURIDADES DE PUERTO

Materiales / herramientas
Descripción de los equipos/herramientas/*software* necesitados para la práctica.

- 1 Computador (laboratorio de redes)
- 1 Cisco Packet Tracer

3.1 Objetivo general

Incorporar el protocolo p*ortfast* para lograr una rápida convergencia en los puertos redundantes de una red de *switches* para evitarse tiempos prolongados de inactividad y efectuar la configuración de seguridades de puerto.

3.2 Objetivos específicos

1. Analizar la importancia de la rápida convergencia de enlaces redundantes.
2. Analizar la diferencia en el tiempo de convergencia de una red con *portfast* y sin el mismo.
3. Configurar seguridades en los puertos de los *switches* que asocien una dirección MAC a un puerto, para evitar conexión de host no autorizados.

3.3 Marco teórico

3.3.1 Portfast

"Es una característica de los *switches* Cisco que permite a los puertos pasar de los diferentes estados de *spanning tree,* y proceder directamente al modo de envío. *Portfast* debe ser habilitado solo en los puertos que no tengan *switches* conectados." (Donabue, G., 2012, p. 95).

> "Este protocolo nos ayuda a asignar la identidad de puerto de extremo a una interfaz, tiene capacidad para acelerar el proceso de establecimiento

> de la convergencia del protocolo *spanning tree*, es equivalente a indicar que el puerto que no está conectado a otro *switch* y no se generarán los problemas de bucles de los enlaces redundantes. (…). Portfast es una herramienta que merece consideración en toda red. Portfast puede significar la diferencia entre una tolerancia a fallos transparente y un corte de 30-50 segundos. De otra manera, portfast toma 20 segundos en pasar un puerto a modo envío.” (Kennedy & Hamilton, 2001).

3.3.2 Seguridad de puertos

La implementación de seguridad en una red es imperativa y debe aplicarse a todos los niveles jerárquicos de una red, razón por la cual el nivel acceso que es donde se conectan los usuarios finales no están libres de dicha medida.

Los *switches* que sirven de punto de vinculación a la red para usuarios finales, pueden proporcionar restricción de acceso a usuarios que no pertenezcan a la red, esta medida puede agregar un nivel de seguridad en la prevención de robo de información.

Las medidas que se pueden tomar para la protección de los puertos se detallan a continuación:

- El comando *switchport* port-security mac-address sticky, aprende la primera MAC que se conecta al Puerto.
- El comando *switchport* port-security mac-address xx:xx:xx:xx:xx:xx, permite el acceso solo a la dirección MAC ingresada.
- *Switchport* port-security violation protect. Deja de transmitir datos en el puerto.
- *Switchport* port-security violation restrict. Envía una alerta SMTP al administrador y se anulan los paquetes a una MAC distinta a la permitida.
- *Switchport* port-security violation shutdown. El puerto se desactiva.

3.4 Trabajo preparatorio

Conseguir Packet Tracer versión 6.0.1 (mínimo). Disponer de un computador.

Usar la topología de la práctica anterior o realizarla con anticipación.

3.5 Desarrollo de la práctica

Pasos a seguir:

1) Armar una red tomando como punto de partida la topología realizada en la práctica 2.

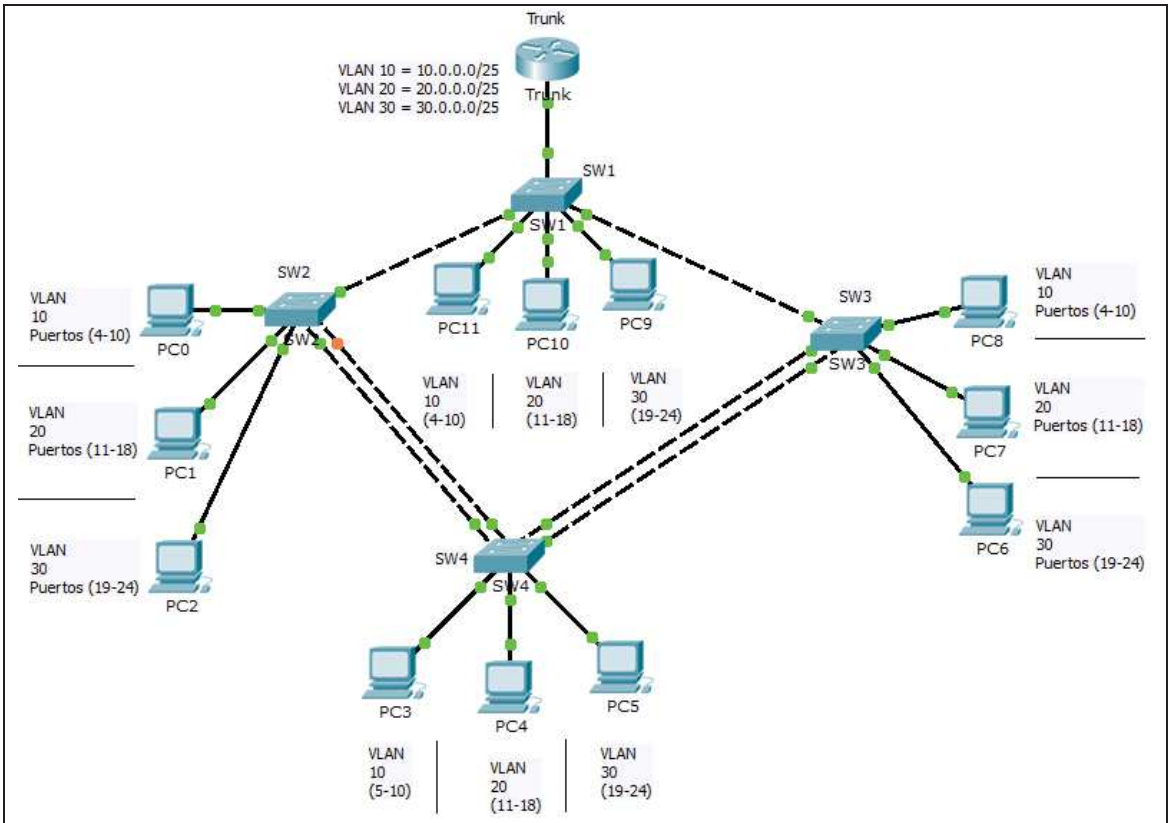

Figura 12. Topología de la práctica.
Tomado de Cisco Packet Tracer

2) Levantar el servicio *portfast* en todos los puertos de los *switches* que se conecten a usuarios finales.
   SW1(config)#int range fa0/4-24

SW1(config-if-range)#spanning-tree portfast

SW2(config)#int range fa0/4-24
SW2(config-if-range)#spanning-tree portfast

SW3(config)#int range fa0/4-24
SW3(config-if-range)#spanning-tree portfast

SW3(config)#int range fa0/5-24
SW3(config-if-range)#spanning-tree portfast

3) Configurar seguridades de puerto según la dirección MAC de los host en el *switch* SW1, permitir máximo una dirección MAC. Por ejemplo:
   SW1(config)#int fa0/4
   SW1(config-if)#switchport port-security
   SW1(config-if)#switchport port-security maximum 1
   SW1(config-if)#switchport port-security mac-address 0001.9771.0104
   SW1(config-if)#switchport port-security violation protect
   SW1(config-if)#exit
   SW1(config)#int fa0/11
   SW1(config-if)#switchport port-security
   SW1(config-if)#switchport port-security maximum 1
   SW1(config-if)#switchport port-security mac-address 0090.217e.c318
   SW1(config-if)#switchport port-security violation protect
   SW1(config-if)#exit
   SW1(config)#int fa0/19
   SW1(config-if)#switchport port-security
   SW1(config-if)#switchport port-security maximum 1
   SW1(config-if)#switchport port-security mac-address 0001.63bb.a11e
   SW1(config-if)#switchport port-security violation protect
   SW1(config-if)#end

4) Configurar seguridades de puerto según la primera dirección MAC que se conecte al *switch* SW2, permitir máximo una dirección MAC.

```
SW2(config)#int range fa0/4-24
SW2(config-if-range)#switchport port-security
SW2(config-if-range)#switchport port-security maximum 1
SW2(config-if-range)#switchport port-security mac-address sticky
SW2(config-if-range)#switchport port-security violation shutdown
SW2(config-if-range)#end
```

5) Desactivar los puertos que no se utilicen como medida de seguridad a usuarios no autorizados. Por ejemplo:

```
SW1(config)#int range fa0/5-10
SW1(config-if-range)#shutdown
SW1(config-if-range)#int range fa0/12-18
SW1(config-if-range)#shutdown
SW1(config-if-range)#int range fa0/20-24
SW1(config-if-range)#shutdown
```

6) Verificar las seguridades de los puertos reemplazando un computador por cualquier otro en los *switches* SW1 Y SW2, ejemplo Figura 13.

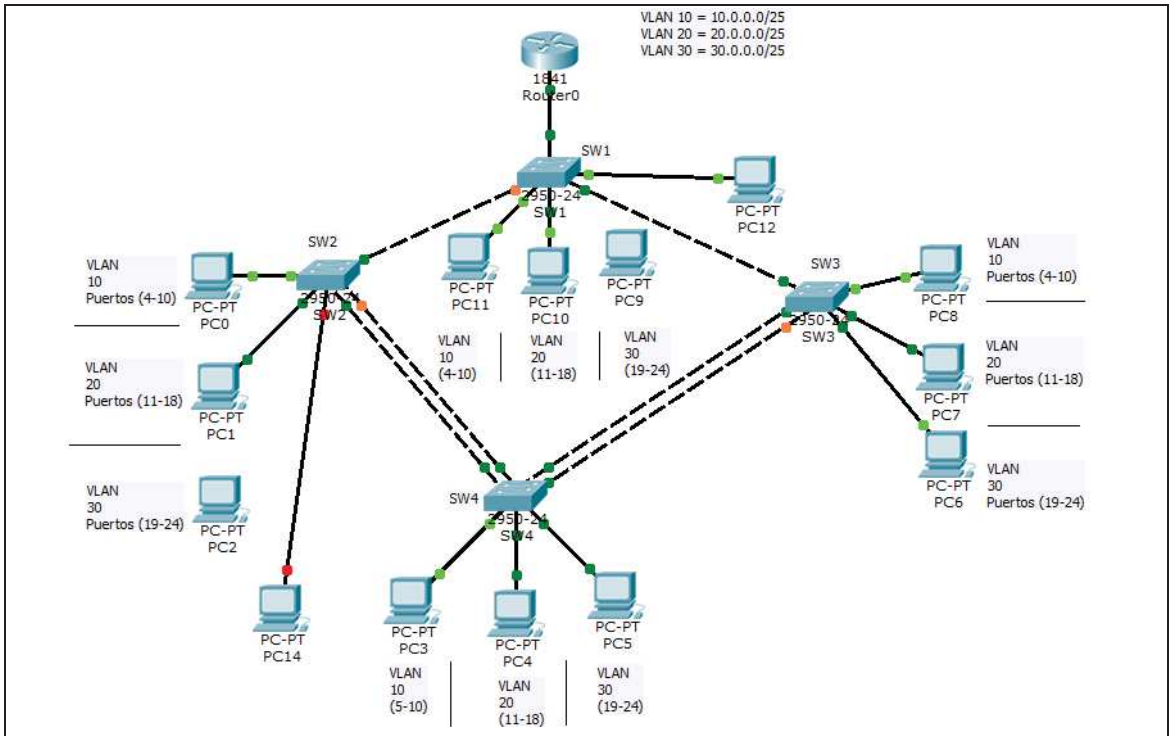

Figura 13. Cambio de computador en puerto del *switch* SW2.
Tomado de Cisco Packet Tracer

Notar que el puerto del *switch* SW2 al que se conectó el nuevo computador está desactivado como medida de seguridad tal como fue configurado, mientras el puerto del SW1 no envía datos al PC12 debido a que no corresponde a la MAC configurada (Figura 14).

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
	Failed	PC14	PC5	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PC12	PC5	ICMP		0.000	N	1	(edit)	(delete)

Figura 14. Comprobación de seguridad de puerto.
Tomado de Cisco Packet Tracer.

3.6 Resultados de aprendizaje

- Emplear *portfast* como complemento de una red conmutada redundante para conseguir una red eficaz mediante la reducción de los tiempos de falla, identificando los puertos que no están propensos a bucles.

- Identificar los diferentes modos de bloqueo de un puerto al momento de violar una restricción.

3.7 Conclusiones

- Una red eficiente es la que tiene menos puntos de falla.
- Se puede eliminar el envío de paquetes TCN (Notificaciones de cambio de topología) gracias a la configuración de *portfast*. Sin esta característica, los puertos que se conectan a los usuarios finales también entrarían en el proceso de *spanning-tree* para activar un puerto en modo envío.
- Las seguridades en los puertos ayudan a permitir la conexión únicamente de host autorizados por el administrador y evitar la conexión a puertos abiertos.
- Los puertos que no están propensos a bucles, son los que no están conectados a otro *switch*.

3.8 Tiempo estimado de la práctica

Una sesión de clase.

3.9 Evaluación/ cuestionario

1. ¿Cómo ayuda la configuración de portfast al tiempo de respuesta de un *switch* al presentarse de cambios en la topología?
2. ¿Qué pasa si introduzco el comando "*switchport* port-security mac-address sticky" en el puerto de un *switch*?
3. ¿Qué tipo de restricciones se puede configurar en un *switch*?
4. ¿Es aconsejable dejar puertos activos aunque no se utilicen?

CAPÍTULO IV CONFIGURACIÓN DEL PROTOCOLO STP

Materiales / herramientas

Descripción de los equipos/herramientas/*software* necesitados para la práctica.

- 1 Computador (laboratorio de redes)
- 1 Cisco Packet Tracer

4.1 Objetivo general

Incorporar el protocolo STP *Spanning Tree Protocol* para evitar bucles a nivel de capa 2 en una red con redundancia.

4.2 Objetivos específicos

1. Configurar y verificar el funcionamiento del protocolo STP.
2. Desarrollar una topología donde se combine el protocolo STP con las características de Portfast.
3. Analizar el comportamiento de la red al manipular el Bridge ID para seleccionar manualmente un puente raíz.
4. Analizar las diferencias entre STP y su variación RSTP, además de la importancia de los mismos.

4.3 Marco teórico

4.3.1 STP

> "El protocolo bridge IEEE 802.1D, trabaja en la capa 2 del modelo OSI y proporciona enlaces redundantes mientras previene bucles indeseables. Para que la capa 2 funcione correctamente, solo debe haber un enlace activo entre dos estaciones. La operación de STP es trasparente para las estaciones finales que no pueden detectar si están conectados a un solo segmento de LAN o una LAN conmutada de múltiples segmentos." (Cisco, 2012, p. 28-2).

“Es evidente la necesidad de poner redundancia en las redes basadas en *switches*, pero esto puede causar tormentas de broadcast, bucles, duplicación de tramas, e inestabilidad en la tabla MAC de los *switches*. Para solucionarlo se emplea el protocolo STP. (…). Todos los *switches* de la red participan en el protocolo STP mediante unas tramas llamadas BPDU (Bridge Protocol Data Unit). Estas tramas son usadas para elegir al *switch* root mediante el protocolo STP, elegir un *switch* designado para cada segmento y eliminar los bucles, poniendo los puertos en estado de bloqueo. Se envían cada 2 segundos a la dirección MAC multicast 01.80.C2.00.00.00 para asegurar una arquitectura estable.

Los parámetros importantes en esta trama son:

- *Root* ID: Identificador del *switch* root.
- *Root cost*: Conste para alcanzar a la raíz, depende de la velocidad de los enlaces (1000/ancho de banda de la línea). Si está conectado directamente al puente raíz es 0.
- *Bridge* ID: identificador del *switch* que lanza la trama. Está compuesto por una prioridad administrativa de 2 bytes y la dirección MAC del swtich.
- *Port* ID: El port ID del puerto que ha enviado el BPDU.
- *Configuration* BPDU: Se envía en condiciones normales, para asegurar que todo sigue funcionando bien.
- *Topology Change Notification* (TCN) BPDU: Enviadas al principio y durante un cambio en la red, para que se calcule quien será el puente raíz y cuales los puertos raíz de cada equipo.
- *Disabled*: En este modo administrativo, el puerto es inactivo y no participa en STP.
- *Blocked*: En este modo, los puertos ni reciben ni transmiten tramas, únicamente los BPDU. STP pone en este estado un puerto cuando existe otro camino.

- Listen: Los puertos pasan del estado bloqueado al estado escucha. Permanecen en este estado un tiempo para intentar aprender si existen otros caminos para alcanzar la raíz. Durante este tiempo, el puerto recibe tramas, pero no transmite nada. El tiempo de permanencia en este estado es el retraso de envío (*forward delay*).
- *Learn*: Es similar al estado Listen, pero el puerto añade a la tabla de direcciones las direcciones que ha conocido. El tiempo en este estado es también el retraso de envío.
- *Forward*: El puerto es capaz de enviar y recibir tramas." (Valencia, 2011, p. 34).

Entendiendo los temporizadores de STP, tenemos:

- "Hello Time: Es el tiempo entre cada BPDU que es enviado por un puerto. Este tiempo es igual a 2 segundos por defecto.
- Forward delay: Es el tiempo que se ocupa en los estados de escucha y aprendizaje. Este tiempo es igual a 15 segundos por defecto.
- Max Age: El temporizador Max Age controla la longitud máxima de tiempo que transcurre antes de que un puerto de puente guarde su BPDU de configuración. Este tiempo es de 20 segundos de forma predeterminada." (Cisco, 2006, p. 3 - 4).

"STP utiliza un dispositivo principal llamado puente raíz o *switch* raíz, para determinar qué puertos deben bloquearse y cuales deben estar en modo envío. (…). El puente raíz se lo elige según el ID del puente (BID o Bridge ID). El BID se crea a partir del valor de prioridad del puente y la dirección MAC, escogiéndose el más bajo.

> La prioridad por defecto de los *switches* es 32768. Si un *switch* tiene una dirección MAC 00:E1:6D:BB:06:23, el BID correspondiente a ese *switch* sería 32768: 00:E1:6D:BB:06:23.” (Martínez, 2011).

Los puertos designados son otros de los dos componentes del STP, es la ruta de menor costo administrativo hacia el puente raíz, en toda comunicación redundante entre *switches* hay puertos designados.

4.3.2 RSTP

> “Provee una rápida convergencia del *spanning tree* asignando roles de puerto y aprendiendo la actividad de la topología. RSTP está construido sobre 802.1D STP para seleccionar el *switch* con la más alta prioridad (valor numérico más bajo). (…). Tiene dos estados aprendiendo y enviando. RSTP disminuye el tiempo de convergencia en hasta 6 segundos.” (Cisco, 2012, p. 28_2).

Tabla 1. Comparación de los estados de puerto en RTP y RSTP.
Adaptado de Odom, 2004, p. 50)

Estado operacional	**Estado STP (802.1d)**	**Estado RSTP (802.1w)**	**Estado incluido en la topología RSTP**
Activo	Bloqueando	Descartando	No
Activo	Escuchando	Descartando	No
Activo	Aprendiendo	Aprendiendo	Si
Activo	Enviando	Enviando	Si
Desactivado	Desactivado	Descartando	No

4.4 Trabajo preparatorio

Conseguir Packet Tracer versión 6.0.1 (mínimo).

Disponer de un computador de laboratorio o propio con características como sistema operativo Windows (7, 8, 8.1), Linux (Ubuntu, Fedora), procesador 200 MHz o superior, 64 MB RAM o superior.

Usar el mismo archivo Packet Tracer de la práctica 3.

Investigar sobre el funcionamiento del modo de simulación del Packet Tracer, ubicado en la parte inferior derecha de la ventana del programa (se puede acceder presionando las teclas shift+S).

4.5 Desarrollo de la práctica

Pasos a seguir:

1) Habilitar STP en los siguientes *switches*:

   Al introducir los siguientes comandos se declara como *switch* raíz al SW1, ya que la prioridad es más baja que la por defecto, luego le seguirá el SW3.

   SW1(config)#spanning-tree vlan 1 priority 4096
   SW1(config)#spanning-tree vlan 91 priority 4096
   SW1(config)#spanning-tree vlan 30 priority 4096

   SW2(config)#spanning-tree vlan 10 root primary
   SW2(config)#spanning-tree vlan 20 root secondary

   SW3(config)#spanning-tree vlan 20 root primary
   SW3(config)#spanning-tree vlan 10 root secondary

2) Identificar el puente raíz y la raíz designada.

   2.1. Enviar un paquete desde el computador de la VLAN 10 del SW1 hasta el PC de la VLAN 10 en el SW3 (Figura 15). Observar cual es el camino que se toma para el envío de paquetes.

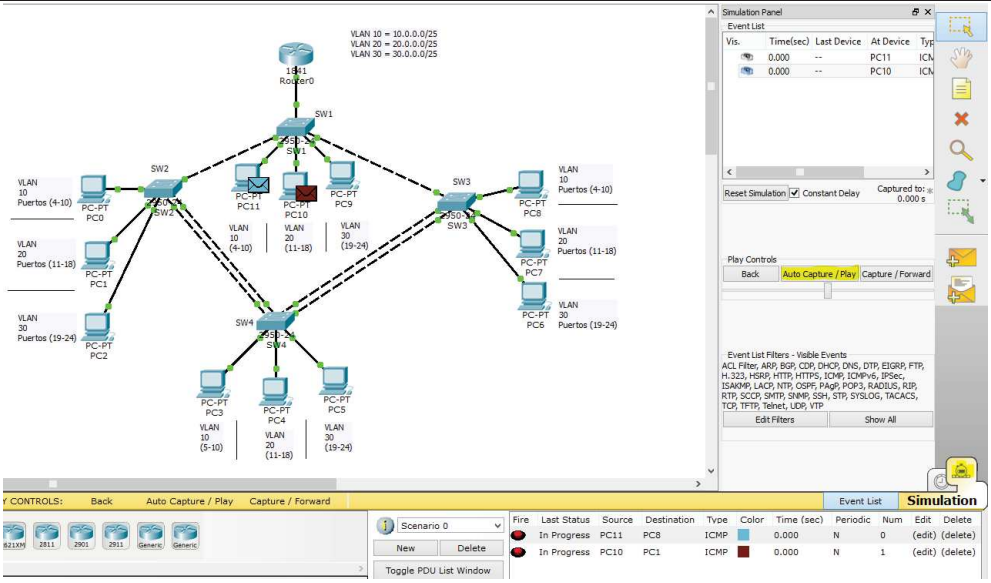

Figura 15. Modo Simulación Packet Tracer.

Tomado de Cisco Packet Tracer.

2.2. Introducir el comando *show spanning-tree* en el *switch* SW1 y al igual que en el paso 2.1 para poder visualizar un resultado como el de los siguientes pasos:

2.2.1. Introducir el comando para observar el puente raíz.

```
SW1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
             Address     0002.1656.CD3A
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097  (priority 4096 sys-id-ext 1)
             Address     0002.1656.CD3A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20
```

2.2.2. Introducir el comando para observar el puente designado con el ID más alto que le sigue al *root bridge*.

```
SW3#sh spanning-tree
```

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    16394
             Address     0001.634C.81C3
             Cost        19
             Port        3(FastEthernet0/3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    20490  (priority 20480 sys-id-ext 10)
             Address     0006.2A11.BC96
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    28692
             Address     0001.634C.81C3
             Cost        19
             Port        3(FastEthernet0/3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28692  (priority 28672 sys-id-ext 20)
             Address     0006.2A11.BC96
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Root FWD 19        128.3    P2p
Fa0/11           Desg FWD 19        128.11   P2p
```

3) Desconectar el enlace que comunica el puente raíz al puerto designado del *switch* con el segundo BID de preferencia, como por ejemplo en la Figura 16. Comprobar cuánto tiempo se demora en converger la nueva topología y observar el recorrido de los paquetes de datos.

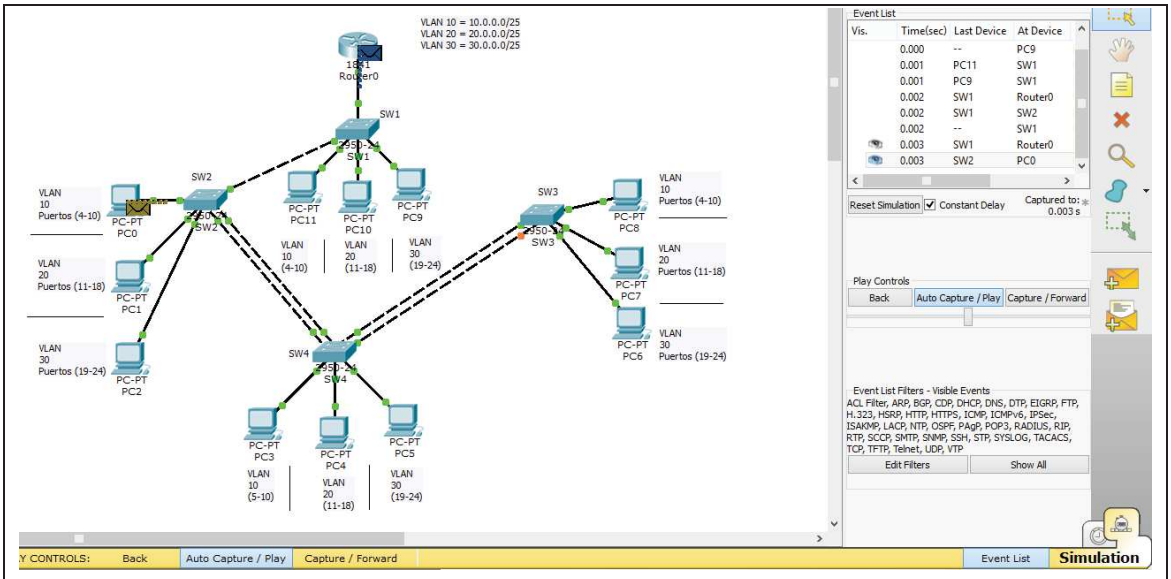

Figura 16. Cambio en la topología en el emulador Packet Tracer.
Tomado de Cisco Packet Tracer

4) Configurar RSTP, introduciendo el siguiente comando en todos los *switches*:
SW1(config)#spanning-tree mode rapid-pvst

5) Realizar la misma prueba del paso 3 y verificar el tiempo que se demora en converger la red.

4.6 Resultados de aprendizaje

- Emplear configuraciones de STP y RSTP, como forma de disminuir el tiempo de inactividad de una red conmutada al momento de un cambio en su topología y la diferencia en la implementación entre los dos protocolos.
- Distinguir entre STP y RSTP.
- Seleccionar un puente raíz y puente designado.

4.7 Conclusiones

- STP es un protocolo útil para lograr una redundancia eficaz que previene una prolongada discontinuidad en la transmisión de datos.
- La combinación de STP o RSTP con *portfast* hecho entre los laboratorios 3 y 4, son la configuración ideal para que una red se estabilice rápidamente ante un cambio de la topología redundante.
- La configuración de prioridades del BID, permite al administrador de red predefinir el dispositivo que hará las veces de puente raíz y puente designado, acelerando el proceso de restablecimiento de la red ya que con anterioridad ha sido designada una sucesión a seguir, mediante la implementación de prioridades.
- Las prioridades además de asignarse a *switches*, también se pueden asignar a las VLAN, que en conjunto con la dirección MAC más baja, da la oportunidad para determinar el puente raíz.
- Al momento de haber un cambio de topología, RSTP tiene un tiempo de convergencia menor a STP.

4.8 Tiempo estimado de la práctica

Una sesión de clase.

4.9 Evaluación/ cuestionario

1. ¿Para qué sirve STP y su variación RSTP?
2. ¿Cómo se designa el puente raíz?
3. ¿Cómo ayuda la combinación de STP o RSTP junto con *portfast*?

CAPÍTULO V CONFIGURACIÓN DE UNA RED WAN CON 2 ROUTERS

Materiales / herramientas

Descripción de los equipos/herramientas/*software* necesitados para la práctica.

- 1 Computador (laboratorio de redes)
- 1 Cisco Packet Tracer

5.1 Objetivo general

Incorporar rutas estáticas en un enlace serial para lograr la comunicación entre dos redes geográficamente separadas e implementar listas de acceso.

5.2 Objetivos específicos

1. Desarrollar la topología de una red dimensionando el equipamiento activo de acuerdo al requerimiento entregado por un cliente y colocar módulos adicionales en los dispositivos de red que lo necesiten para armar la topología requerida.
2. Configurar rutas estáticas.
3. Configurar DHCP.
4. Analizar el funcionamiento de las listas de acceso.

5.3 Marco teórico

5.3.1 Módulo de comunicación serial síncrono/asíncrono

> “La comunicación serial consiste en el en envío de información (bits) uno a continuación de otro, es decir en forma secuencial. (…). Para la conexión serial entre *router*s se utilizan puertos WIC (WAN *interface Card*), estos puertos son de comunicación serial punto a punto y pueden ser síncronos o asíncronos, por lo cual solo a uno se le configurará un rango de reloj (*clock rate*) para determinar cuál es el DTE y DCE entre los dos dispositivos.” (Rueda, 2001).

5.3.2 DCE/DTE

> “El DCE (Equipo comunicador de datos), es el puerto síncrono en la comunicación serial entre r*outer*s, mientras que el DTE (Equipo terminación del circuito de datos), es el puerto asíncrono en la comunicación entre los *router*s, por lo cual se le configura el *clock rate* el cual es representa una señal de reloj que sincroniza la transmisión de datos.” (Rueda, 2001).

5.3.3 Rutas estáticas

> “Las rutas estáticas son una implementación manual de la ruta que deben seguir los paquetes que estén etiquetados con una dirección IP destino que no esté conectada directamente al *router* que las recibe, sino que están en el siguiente *router* llamado también siguiente salto. Las rutas estáticas no requieren del mismo procesamiento por parte del *router* en comparación a los protocolos de enrutamiento. Es decir conservan de mejor manera los recursos de la red y del *router*. Pero como desventaja requiere más trabajo por parte del administrador dependiendo del tamaño de la topología.
>
> Este tipo de configuración se recomiendo donde el ancho de banda es limitado y en caso que la cantidad de *router*s en la red no numerosa al punto de dificultar la administración y fácil escalabilidad.” (Collado, 2009, p. 20).

5.3.4 Lista de acceso

Las listas de acceso también conocidas como ACL, son medidas de seguridad implementadas en dispositivos con capacidades de capa 3 y cumplen el

objetivo de permitir o denegar el tráfico entrante o saliente dependiendo de cómo se las configure.

Existen dos tipos de ACL, las estándar y las extendidas, las estándar permiten un filtrado de tráfico basado en una dirección IP o bloque de direcciones, en cambio, las ACL extendidas admiten un filtrado más específico, siendo posible determinar números de puerto, tipo de tráfico de capa 4 y direcciones IP de origen y destino. A las listas de acceso estándar se les asigna un número entre 1 y 99, 1300 y 1999; las listas de acceso extendidas tienen números entre 100 y 199, 2000 y 2699. También existe un tipo de listas de acceso nombradas, en donde la diferencia es que simplemente anteponiendo el comando "ip" antes de la sentencia "*access-list*", se le puede asignar un nombre ya sea a una ACL estándar o extendida, quedando de la siguiente manera:

Router(config)# ip access-list (standard o extended) # puerto

Luego del ingreso del comando mencionado se puede escribir las sentencias de permitir o denegar el tráfico.

Otro de los componentes de una ACL es la *wildcard*, la cual es el opuesto a una máscara de subred, por ejemplo en el caso que se tenga una máscara de subred 255.255.255.0 la *wildcard* es 0.0.0.255. Cuando se quiere especificar un host en particular la *wildcard* es 0.0.0.0 pero también se puede colocar la palabra "host" y si se quiere hacer referencia a una red cualquiera se puede escribir la palabra "any".

La forma como se ejecutan las sentencias de las listas de acceso es similar al de una pila FIFO en programación, es decir y aplicado a este caso, que la primera sentencia en configurarse es la primera en ejecutarse, esto se debe tener en cuenta al momento de hacer una ACL colocando en las primeras líneas el tráfico más concurrente que se desee bloquear o el más concurrente que se deba permitir, de forma que al *router* le tome menos tiempo determinar el tráfico permitido y el bloqueado. Otro aspecto importante a considerarse es

que debe existir al menos una línea que permita tráfico, ya que lo no especificado se deniega automáticamente, es como si hubiera una negación de tráfico implícita al final de toda lista de acceso independientemente de que se la configure o no.

Las listas de acceso estándar se colocan cerca del destino ya que la estructura de las sentencias es más general en comparación a las ACL extendidas, estas últimas en cambio se colocan más cerca del origen. Se recomienda configurar las ACL luego de comprobar la correcta comunicación en toda la red.

5.3.5 DHCP

Por su significado en inglés *Dynamic Host Configuration Protocol*, este un protocolo que tiene por objetivo la asignación dinámica de direcciones IP a los host de una determinada red mediante la propagación en *broadcast*. Los host que tengan la configuración correspondiente recibirán una dirección IP del *pool* de direcciones configurado en el servidor DHCP.

Puede usarse especialmente para reducir el tiempo de implementación de una red con gran o mediana cantidad de usuarios, esta configuración se la puede realizar en un *router* con esta capacidad.

5.4 Trabajo preparatorio

Conseguir Packet Tracer versión 6.0.1 (mínimo).

Disponer de un computador de laboratorio o propio con características como sistema operativo Windows (7, 8, 8.1), Linux (Ubuntu, Fedora), procesador 200 MHz o superior, 64 MB RAM o superior.

Se recomienda que el segundo ejercicio de este laboratorio sea realizado como deber luego de realizar en clase la primera parte.

5.5 Desarrollo de la práctica

Pasos a seguir:

Primera parte del Laboratorio:

1) Revisar el requerimiento del cliente:

1.1. Una empresa en crecimiento desea hacer una conexión entre su matriz y su nueva sucursal, para lo cual se desea conectar 2 *routers* ubicados en lugares remotos como se muestra a continuación (Figura 17). La empresa adquirió un enlace y direcciones IP para sus *routers*, el suministro de equipos y configuración de los mismos correrá por parte de un oferente, es este caso el estudiante. La comunicación será mediante rutas estáticas.

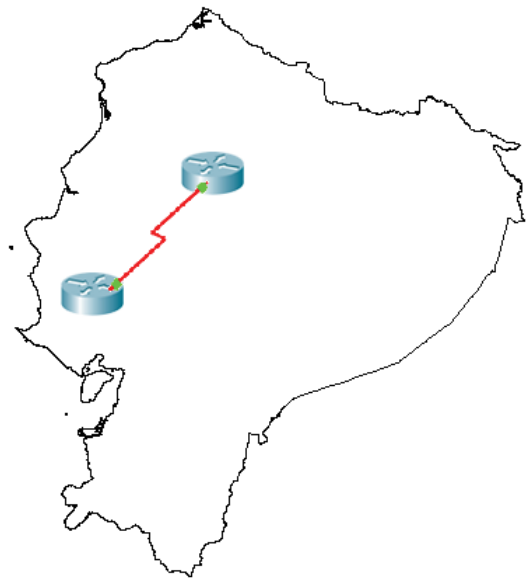

Figura 17. Mapa geográfico representativo del tipo de red a realizar. Adaptado de imagui.com

1.2. La Red-1 y la Red-2 tienen un *Router* ISR de la serie 1800, cada red deberá tener un *Switch* de por lo menos 12 puertos o superior para la conexión de 3 computadores en la Red-1 y uno solo en la Red-2 como se muestra a continuación. (Figura 18).

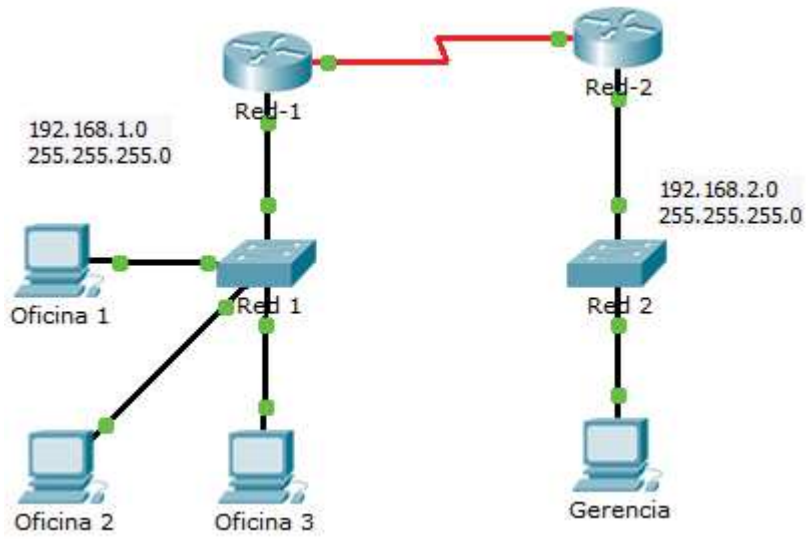

Figura 18. Topología física de red.
Tomado de Cisco Packet Tracer.

1.3. Los *Router*s deberán contar con los módulos de expansión necesarios para la comunicación entre los mismos. Se deberá arrastrar el módulo hasta la ranura con el *router* apagado (Figura 19). Los *routers* deberán ser del tipo ISR (*Router* de servicios integrados), para brindarle la oportunidad que en un futuro se pueda implementar una pequeña solución de telefonía IP.

Figura 19. Ventana del *software* Packet Tracer para colocar interfaces. Adaptado de Cisco Packet Tracer.

1.4. La empresa utiliza un correo con POP3 y quiere bloquear aquellos que funcionan con IMAP (puerto 143) para todos los host de la red 1 (*router* Red-1). El resto del tráfico se permitirá.

2) Considerar los siguientes equipos de red para la implementación de la red:

2.1. *Router* ISR 1841 con una interfaz WIC-2T. Cantidad 2. Para colocar la interfaz serial el *router* debe estar apagado.

Figura 20. Router Cisco ISR 1841.
Tomado de Cisco Packet Tracer.

Figura 21. Interfaz serial WIC-2T.
Tomado de Cisco Packet Tracer.

2.2. *Switch* 2950 de 24 puertos 10/100/1000 Mbps. Cantidad 2.

Figura 22. *Switch* Cisco 2950.
Tomado de Cisco Packet Tracer.

2.3. Computadores. Cantidad 4.

3) Realizar el diagrama de red en Packet Tracer de acuerdo a la Figura 18 tomando en consideración los mismos nombres para los elementos de red.

Nota explicativa: Hay dos tipos de cable serial en el Packet Tracer, el DCE y DTE. Al seleccionar el cable serial DCE y conectarlo al *router*, especifica que aquel tendría que ser el DCE y el segundo *router* en el que se termine la conexión del cable será el DTE; si se escoge el otro cable (serial DTE), el resultado sigue la misma lógica.

4) Configurar los dispositivos de red de acuerdo a los siguientes datos:

4.1. Configurar enlaces Seriales. Tabla 2.

Tabla 2. Tabla de direccionamiento IP de enlaces seriales.

Líneas Seriales			
Nombre del *Router*	**Dirección IP**	**Mascara de Subred**	***Clock Rate***
Red-1	192.168.0.1	255.255.255.252	64000
Red-2	192.168.0.2	255.255.255.252	N/A

Router>en
Router#config ter
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname RED-1
RED-1(config)#no ip domain-lookup
RED-1(config)#int s0/0/0
RED-1(config-if)#ip addr 192.168.0.1 255.255.255.252
RED-1(config-if)#clock rate 64000
RED-1(config-if)#no shut

Router>en
Router#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RED-2
RED-2(config)#no ip domain-lookup
RED-2(config)#int s0/0/0
RED-2(config-if)#ip addr 192.168.0.2 255.255.255.252
RED-2(config-if)#no shut

4.2. Configurar red LAN en cada *router*. Tabla 3.

Tabla 3. Tabla de direccionamiento IP de enlaces *fast ethernet*.

Líneas *Fast ethernet* de los *Routers*		
Nombre del *Router*	**Dirección IP**	**Mascara de Subred**
Red-1	192.168.1.0	255.255.255.0
Red-2	192.168.2.0	255.255.255.0

RED-1(config)#int fa0/0
RED-1(config-if)#ip addr 192.168.1.1 255.255.255.0
RED-1(config-if)#no shut

RED-2(config)#int fa0/0
RED-2(config-if)#ip addr 192.168.2.1 255.255.255.0
RED-2(config-if)#no shut

4.3. Asignar direcciones IP a los Host de acuerdo a su respectiva red. Tabla 4.

Tabla 4. Tabla de asignación de direcciones IP en los computadores.

PC	Dirección IP	Mascara de Subred	Puerta de Enlace
Oficina 1	192.168.1.10	255.255.255.0	192.168.1.1
Oficina 2	192.168.1.20	255.255.255.0	192.168.1.1
Oficina 3	192.168.1.30	255.255.255.0	192.168.1.1
Gerencia	192.168.2.40	255.255.255.0	192.168.2.1

5) Configurar las rutas estáticas en el enlace serial de los *router*s de acuerdo a la siguiente estructura:
Red remota– Máscara de red – Siguiente salto

5.1. Configurar ruta estática de la Red-1.
RED-1(config)#ip route 192.168.2.0 255.255.255.0 192.168.0.2

5.2. Configurar ruta estática de la Red-2.
RED-2(config)#ip route 192.168.1.0 255.255.255.0 192.168.0.1

6) Comprobar conexión mediante un ping entre los computadores de las dos redes.

7) Configurar una ACL estándar que impida la comunicación entre el host "Oficina 3" y toda la red LAN del router "Red-2".

7.1. Ingresar los siguientes comandos en el router "Red-2" para crear la lista de acceso.
Red-2(config)#access-list 1 deny 192.168.1.30
Red-2(config)#access-list 1 permit any

7.2. Aplicar la lista de acceso a una interfaz e indicar si el tráfico entrará o saldrá por dicha interfaz. Se coloca como tráfico de entrada en el caso que venga desde fuera y como salida si el tráfico sale desde el mismo *router*.

```
Red-2(config)#int s0/0/0
Red-2(config-if)#ip access-group 1 in
Red-2(config-if)#exit
```

8) Realizar un ping desde los host Oficina 3 hacia Gerencia y desde Oficina 2 hacia Gerencia.

9) Configurar una ACL extendida considerando el requerimiento del cliente en el paso 1.4.

```
Red-1(config)#access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 143
Red-1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 any
Red-1(config)#int fa0/0
Red-1(config-if)#ip access-group 100 in
```

10) Comprobar que la ACL extendida funcione correctamente.

Segunda parte del Laboratorio:

1) Armar la siguiente topología de red.

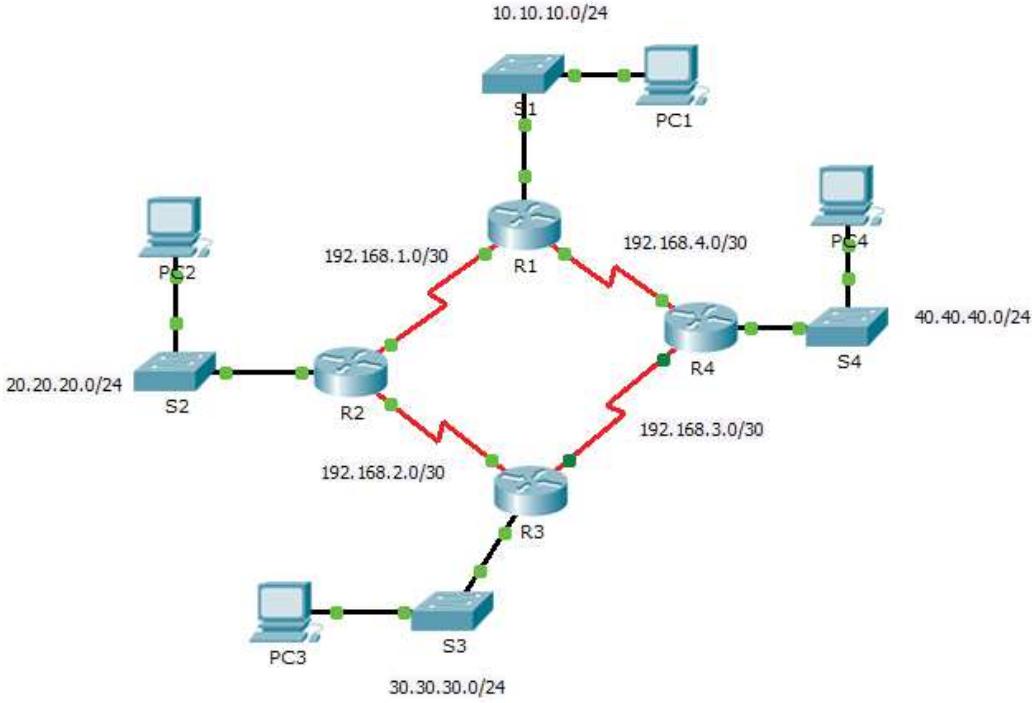

Figura 23. *Topología para la segunda parte de la práctica.*
Tomado de Cisco Packet Tracer

2) Ingresar a cada *router* y hacer las configuraciones básicas, como en el siguiente ejemplo:

2.1. Cambiar el nombre del dispositivo

```
Router(config)#hostname R1
```

2.2. Configurar las claves de acceso y asignarlas a la consola del dispositivo y a las líneas de terminal virtual vty.

```
R1(config)#enable password 123
R1(config)#enable secret abc
R1(config)#line console 0
R1(config-line)#password 123
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password abc
```

R1(config-line)#login
R1(config-line)#exit

3) Realizar las configuraciones básicas en los *switches*, usando los mismos comandos anteriormente descritos.

4) Configurar las direcciones IP de acuerdo a la topología de esta práctica, la colocación del DCE debe ser realizada por el estudiante. El siguiente ejemplo muestra como hacerlo:
   R1#config ter
   R1(config)#int fa0/0
   R1(config-if)#ip addr 10.10.10.1 255.255.255.0
   R1(config-if)#no shut
   R1(config-if)#exit
   R1(config)#int s0/0/0
   R1(config-if)#no shut
   R1(config-if)#ip addr 192.168.1.1 255.255.255.252
   R1(config-if)#clock rate 64000
   R1(config-if)#exit
   R1(config)#int s0/0/1
   R1(config-if)#no shut
   R1(config-if)#ip addr 192.168.4.1 255.255.255.252
   R1(config-if)#clock rate 64000
   R1(config-if)#end

5) Configurar DHCP en los *routers* R1 y R3 como en el siguiente ejemplo:
   R1#config ter
   R1(config)#ip dhcp excluded-address 10.10.10.1
   R1(config)#ip dhcp pool R1
   R1(dhcp-config)#network 10.10.10.0 255.255.255.0
   R1(dhcp-config)#default-router 10.10.10.1

6) Asignar direcciones IP a los *host* PC2 y PC4. En cuanto a los *host* PC1 y PC3 colocarlos en DHCP.

7) Configurar ruteo estático en toda la red procurando ingresar todas las redes remotas.

```
R1(config)#ip route 20.20.20.0 255.255.255.0 192.168.1.2
R1(config)#ip route 30.30.30.0 255.255.255.0 192.168.1.2
R1(config)#ip route 192.168.2.0 255.255.255.252 192.168.1.2
R1(config)#ip route 192.168.3.0 255.255.255.252 192.168.4.2
R1(config)#ip route 40.40.40.0 255.255.255.0 192.168.4.2
R1(config)#ip route 30.30.30.0 255.255.255.0 192.168.4.2
```

8) Comprobar conectividad realizando ping entre los host.

5.6 Resultados de aprendizaje

- Seleccionar los dispositivos y módulos necesarios para la creación de una topología de red.
- Emplear rutas estáticas para comunicar dos redes distintas y geográficamente separadas.
- Distinguir entre las listas de acceso extendidas y estándar.
- Emplear listas de acceso del tipo que el caso amerite y en la interfaz que corresponda.
- Emplear DHCP para Emplear un protocolo de enrutamiento dinámico para que una topología tenga mayor escalabilidad y mejorar los tiempos de administración.

5.7 Conclusiones

- La selección de equipamiento de red debe considerar las características mínimas o superiores respecto a lo que el cliente pide, considerando un futuro crecimiento de la red.

- El *clock rate* debe ser configurado en el DCE y el cable debe ser conectado de forma que corresponda a esta configuración.
- Las rutas estáticas ahorran recursos de red y de procesamiento en el *router*.
- Es necesario documentar las configuraciones que se haga en los dispositivos de red, tales como direcciones IP y demás configuraciones ya que es necesario tener un registro de tales datos en caso de necesitarse realizar alguna actividad en la red.
- Una ACL debe ser configurada considerando que al menos una sentencia permitirá tráfico y aplicada a una interfaz analizando si el tráfico es de entrada o salida.
- El protocolo DHCP es una manera muy útil de reducir tiempos en la implementación de una red con muchos usuarios.

5.8 Tiempo estimado de la práctica

Una sesión de clase.

5.9 Evaluación/ cuestionario

1. ¿Para qué sirve el clock rate?
2. ¿Cuándo es recomendable configurar rutas estáticas?
3. ¿Cómo es la estructura que debe tener una ruta estática?
4. Al aplicar una ACL teniendo un *router* con una interfaz Ethernet y otra interfaz serial, el tráfico del programa emule (puertos 4662 y 4672) que se desea bloquear proviene de internet y se dirige hacia un computador de la LAN. ¿Qué tipo de ACL sería, en qué interfaz se debe aplicar y en qué sentido, entrada o salida?
5. ¿En qué caso resulta especialmente necesario configurar DHCP?

CAPÍTLULO VI CONFIGURACIÓN UNA RED WAN CON 3 *ROUTER*S

Materiales / herramientas
Descripción de los equipos/herramientas/*software* necesitados para la práctica.

- 1 Computador (laboratorio de redes)
- 1 Cisco Packet Tracer

6.1 Objetivo general

Incorporar doble *stack* a una red para conseguir una fácil transición a IPv6 en un futuro, mientras se considera el crecimiento de una red.

6.2 Objetivos específicos

1. Configurar IPv6 en *host* y *router*s.
2. Configuración de rutas estática para la comunicación IPV4 e IPv6.
3. Analizar el requerimiento del cliente y elegir el equipamiento con sus respectivos módulos, necesarios para el crecimiento de la red.
4. Desarrollar la topología y las configuraciones de red con las consideraciones necesarias para lograr la comunicación entre los host de todas las redes.

6.3 Marco teórico

6.3.1 IPv6

"Internet protocol versión 6, es el remplazo para IPv4 que acabó su último bloque de direcciones al entregarlos al continente asiático a inicios del año 2010." (Mun & Lee, 2005, prefacio).

> "Este número se representa como un conjunto de 8 bloques de 4 números hexadecimales cada uno, separados por dos puntos. Para abreviar un conjunto de números en los cuales solo haya ceros, se los

> omite colocando juntos doble signo de dos puntos, y si hay un número cero a la izquierda de otro, también se lo puede omitir, por ejemplo, 2800:68:C:214::2.” (Duarte, 2013).
>
> “Los nodos IPv6 pueden ser compatibles con los nodos IPv4 por medio de la implementación de los dos *stack* IP y corren un apropiado protocolo dependiendo del *stack* de comunicación del otro par. Los nodos en los cuales corren ambos IPv4 e IPv6 son llamados sistemas de doble *stack*. (...). Un doble *stack* permite la interoperación entre los nodos basados en IPv4 a IPv6. En los sistemas de doble *stack*, cualquier aplicación basada en tan solo un *stack* IP (por ejemplo IPv6) puede coexistir y usarse con otras aplicaciones basadas sobre el otro *stack* IP (por ejemplo IPv4).” (Mun & Lee, 2005, p. 116).

Por *stack* se entiende a una estructura de datos en la que los mismos se procesan con el método de primero en entrar, primero en salir (FIFO, *first in, first out*).

“IPv6 tiene las siguientes características:

- Posee una gran cantidad de direcciones gracias a su esquema de 128 bits, llegando a ser más de 340 sextillones en total.
- Permite un enrutamiento escalable y eficiente en internet.
- ARP se sustituye por el envío de paquetes multicast.
- Un encabezado distinto que permite mayor flexibilidad.
- Es más seguro que su versión anterior.
- Permitirá una transición sin problemas de IPv4 a IPv6.
- La eficiencia es mayor ya que tiene una cabecera más simple y fija, reduciendo el tiempo de procesamiento de los paquetes de datos.” (Millan, s.f.).

Se puede tomar como referencia la Figura 24.

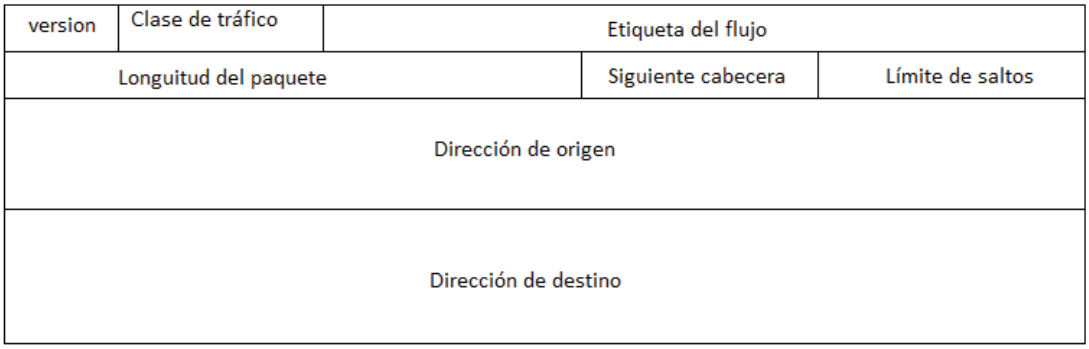

Figura 24. *Cabecera de IPv6.*

"Versión (4 *bits*): Corresponde al protocolo IP, en este caso IPv6.
Clase de tráfico (8 *bits*): Usado para definir el tipo de tráfico transportado en la trama, por ejemplo los valores asignados entre 0 a 7 son para datos, mientras que aquellos entre 8 y 15 son para audio y video.
Etiqueta de flujo (20 *bits*): Es un identificador asignado a los paquetes correspondientes a un mismo flujo de información.
Longitud del paquete (16 *bits*): Sirve para indicar el tamaño total de la trama.
Siguiente cabecera (8 bits): Indica el tipo de cabecera que le sigue.
Límite de saltos (8 bits). La cantidad de saltos que le quedan al paquete y son determinados por el origen. Si tal llega a cero entonces el paquete se descarta.
Dirección origen (128 bits) y dirección destino (128 bits): como su nombre lo dice, el origen y destino del paquete." (Millan, s.f.).

6.4 Trabajo preparatorio

Conseguir Packet Tracer versión 6.0.1 (mínimo).

Disponer de un computador de laboratorio o propio con características como sistema operativo Windows (7, 8, 8.1), Linux (Ubuntu, Fedora), procesador 200 MHz o superior, 64 MB RAM o superior.

Usar la topología de la práctica anterior (práctica 5).

6.5 Desarrollo de la práctica

Pasos a seguir:

1) Revisar el requerimiento del cliente:

1.1. Utilizando la topología de la práctica 5, ahora se necesita implementar una red adicional al norte del país, esta se conectará con la matriz. Esta red estará configurada con un doble stack de forma que la empresa esté lista para un futuro uso de IPv6. Figura 25.

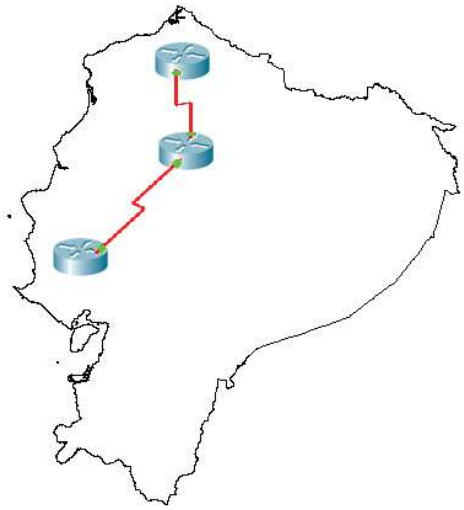

Figura 25. Mapa geográfico representativo del tipo de red a realizar. Adaptado de imagui.com

1.2. La nueva red estará en la capacidad de conectarse con la red existente y deberá tener un *switch* con capacidad de al menos 24 usuarios, se conectarán dos equipos el mismo tal como se ilustra en la Figura 26.

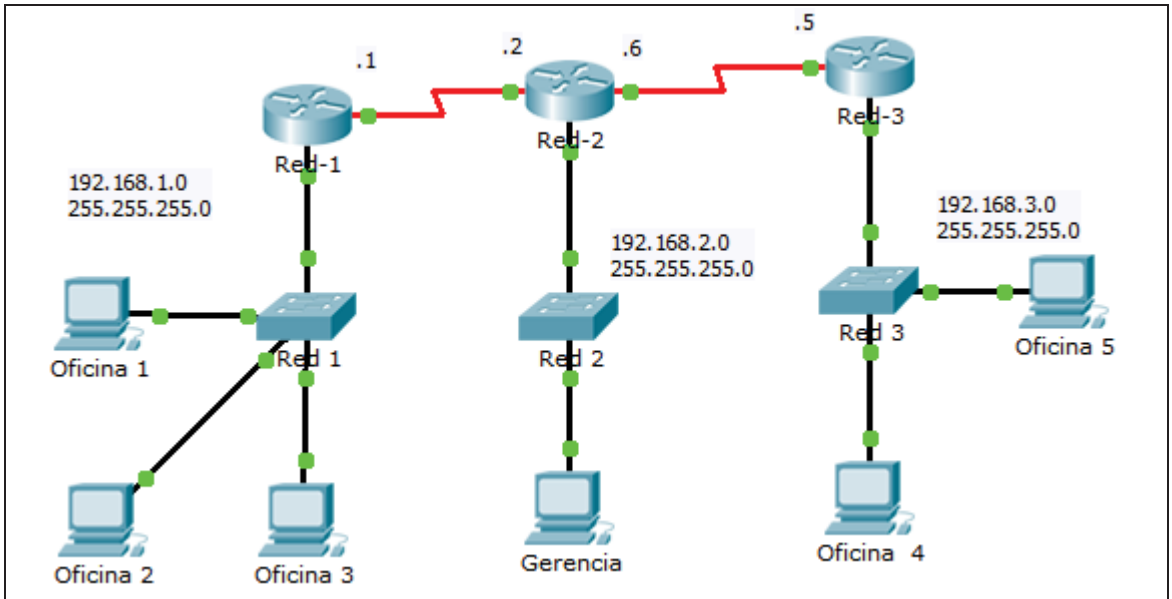

Figura 26. Topología física de red.

Tomado de Cisco Packet Tracer

1.3. Los *Router*s deberán contar con los módulos necesarios para la comunicación entre los mismos.

2) Considerar los siguientes equipos de red para la implementación de la red:

2.1. *Router* ISR 1841 con una interfaz WIC-2T. Cantidad 1. Para colocar la interfaz serial el *router* debe estar apagado.

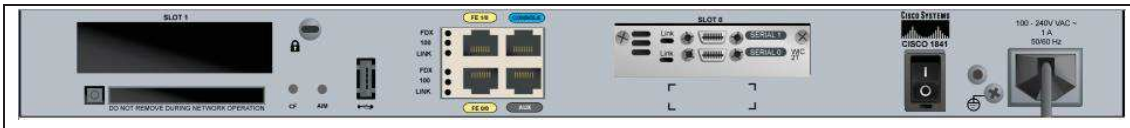

Figura 27. Router Cisco ISR 1841.
Tomado de Cisco Packet Tracer.

Figura 28. Interfaz serial WIC-2T.

Tomado de Cisco Packet Tracer.

2.2. *Switch* 2950 de 24 puertos 10/100/1000 Mbps. Cantidad 1.

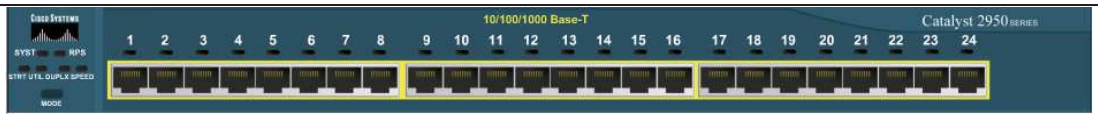

Figura 29. *Switch* Cisco 2950.
Tomado de Cisco Packet Tracer.

2.3. Computadores. Cantidad 2.

3) Realizar el diagrama de red en Packet Tracer tomando como base el ejercicio de la práctica 5 y completarlo para quedar tal como en la Figura 26 de esta práctica.

4) Configurar los dispositivos de red de acuerdo a los siguientes datos:

4.1. Configurar enlaces Seriales. Tabla 5.

Tabla 5. Tabla de direccionamiento IP de enlaces seriales.

Línea Serial			
Nombre del *Router*	**Dirección IP**	**Mascara de Subred**	**Clock Rate**
Red-3	192.168.0.5	255.255.255.252	64000
Red-2	192.168.0.6	255.255.255.252	

Router>en
Router#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Red-3
RED-3(config)#no ip domain-lookup
RED-3(config)#int s0/0/0
RED-3(config-if)#ip addr 192.168.0.5 255.255.255.252

```
RED-3(config-if)#clock rate 64000
RED-3(config-if)#no shut
```

Nota: Si no se conoce cuáles son las interfaces de un dispositivo de red, se puede ingresar el comando show ip interface brief, para poder ver las interfaces existentes en un dispositivo y su estatus.

```
RED-2>en
RED-2#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        192.168.2.1     YES manual up                    up

FastEthernet0/1        unassigned      YES unset  administratively down down

Serial0/0/0            192.168.0.2     YES manual up                    up

Serial0/0/1            unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
RED-2#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
RED-2(config)#int s0/0/1
RED-2(config-if)#ip addr 192.168.0.6 255.255.255.252
RED-2(config-if)#no shut
```

4.2. Configurar red LAN en cada *router*. Tabla 6.

Tabla 6. Tabla de direccionamiento IP del *router* Red-3.

Línea FastEthernet del *Router*		
Nombre del *Router*	**Dirección IP**	**Mascara de Subred**
Red-3	192.168.3.0	255.255.255.0

RED-3(config)#int fa0/0
RED-3(config-if)#ip addr 192.168.3.1 255.255.255.0
RED-3(config-if)#no shut

4.3. Asignar direcciones IP a los Host de acuerdo a su respectiva red. Tabla 7.

Tabla 7. Tabla de direcciones IP de los Host.

PC	**Dirección IP**	**Mascara de Subred**	**Puerta de Enlace**
Oficina 4	192.168.3.50	255.255.255.0	192.168.3.1
Oficina 5	192.168.3.60	255.255.255.0	192.168.3.1

5) Configurar las rutas estáticas en el enlace serial de los *router*s de acuerdo a la siguiente estructura:
Red remota– Máscara de red – Siguiente salto

5.1. Configurar rutas estáticas en el *router* Red-3.
RED-3(config)#ip route 192.168.2.0 255.255.255.0 192.168.0.6
RED-3(config)#ip route 192.168.1.0 255.255.255.0 192.168.0.6

5.2. Configurar rutas estáticas en el *router* Red-2
RED-2(config)#ip route 192.168.3.0 255.255.255.0 192.168.0.5

5.3. Configurar rutas estáticas en el *router* Red-1
RED-1(config)#ip route 192.168.3.0 255.255.255.0 192.168.0.2

6) Comprobar conexión mediante un ping entre los computadores de las tres redes.

7) Asignar las direcciones IPv6 de acuerdo a la Tabla 8, 9 y 10 e introducir los comandos como en el siguiente ejemplo:

```
RED-1(config)#int fa0/0
RED-1(config-if)#ipv6 enable
RED-1(config-if)#ipv6 addr 2001:db8:1::1/64
RED-1(config-if)#end
```

Tabla 8. Tabla de direccionamiento IP del *router* Red-1.

Red-1		
Interfaz	**Dirección IP**	**Longitud del prefijo**
Fa0/0	2001:db8:1::1/64	64
S0/0/0	2001:db8:2::1/64	64

Tabla 9. Tabla de direccionamiento IP del *router* Red-2

Red-2		
Interfaz	**Dirección IPv6**	**Longitud del prefijo**
Fa0/0	2001:db8:3::1/64	64
S0/0/0	2001:db8:2::2/64	64
S0/0/1	2001:db8:4::1/64	64

Tabla 10. Tabla de direccionamiento IP del *router* Red-3.

Red-3		
Interfaz	**Dirección IP**	**Longitud del prefijo**
Fa0/0	2001:db8:5::1/64	64
S0/0/0	2001:db8:4::2/64	64

8) Comprobar conectividad mediante el comando ping entre las interfaces de los *router*s que se comunican directamente, si el resultado es positivo continuar al siguiente paso, caso contrario revisar las configuraciones realizadas.

9) Configurar direcciones IP a los host de acuerdo a su red correspondiente.

10) Configurar las rutas estáticas IPv6 hacia cada una de las redes no conectadas directamente, en todos los *router*s. Por ejemplo:

```
RED-1(config)#ipv6 route 2001:db8:3::/64 2001:db8:2::2
RED-1(config)#ipv6 route 2001:db8:4::/64 2001:db8:2::2
RED-1(config)#ipv6 route 2001:db8:5::/64 2001:db8:2::2
```

11) Comprobar la conectividad desde el *router* Red-1, el resultado debe ser positivo como en el siguiente ejemplo:

```
Sending 5, 100-byte ICMP Echos to 2001:db8:5::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/6 ms
```

6.6 Resultados de aprendizaje

- Emplear dual *stack* para el funcionamiento de los protocolos IPv6 e IPv4 de forma simultánea en la misma red.
- Emplear rutas estáticas en una red con IPv6.
- Identificar las interfaces disponibles en un dispositivo y verificar su estado, mediante el comando "*show ip interface brief*".

6.7 Conclusiones

- Por motivo de preparar una red para IPv6, es posible que una topología coexista con ambos protocolos al mismo tiempo, IPV4 e IPv6.

- Configurar una red con más de dos *router*s mediante rutas estáticas requiere de una mayor intervención por parte de administrador de la red en comparación a una red con protocolo de ruteo dinámico.
- En la configuración de rutas estáticas, para el envío de paquetes entre todos los host de diferentes redes como en esta práctica, es necesario dar a conocer al *router* incluso las redes remotas que se encuentran a más de un salto de distancia.

6.8 Tiempo estimado de la práctica

Una sesión de clase.

6.9 Evaluación/ cuestionario

1. ¿La estructura del comando de configuración de rutas estáticas IPV6 es diferente a IPv4?
2. ¿Es necesario dar a conocer al *router* Red-1 la dirección de la red LAN del *router* Red-3 y viceversa?
3. Si un *router* quiere comunicarse con una red remota no conectada directamente, y con ayuda de rutas estáticas ¿Cómo debe ser la estructura seguida al comando “ip route…”?
4. ¿Con qué comando se puede ver las interfaces que dispone un dispositivo, el estado de las mismas y su dirección IP?

CAPÍTULO VII CONFIGURACIÓN DE UNA RED WAN CON 4 *ROUTER*S

Materiales / herramientas

Descripción de los equipos/herramientas/*software* necesitados para la práctica.

- 1 Computador (laboratorio de redes)
- 1 Cisco Packet Tracer

7.1 Objetivo general

Incorporar el protocolo RIPv2 para mostrar las ventajas del ruteo dinámico frente al estático.

7.2 Objetivos específicos

1. Configurar una red IPv4 con RIPv2.
2. Configurar VLSM.
3. Analizar la diferenciar en la administración entre una red configurada con enrutamiento estático y una configuración con ruteo dinámico.
4. Analizar el tiempo que toma la configuración de RIPv2 frente a las rutas estáticas, y dar a conocer sus ventajas y desventajas.

7.3 Marco teórico

7.3.1 RIP

> “RIP es un protocolo de routing de vector distancia muy extendido en todo el mundo por su simplicidad en comparación con otros protocolos. RIP se trata de un protocolo abierto a diferencia de otros protocolos de routing como por ejemplo IGRP y EIGRP propietarios de Cisco *Systems* o VNN propietario de Lucent *Technologies*.

RIP está basado en el algoritmo Bellman Ford y busca su camino óptimo mediante el conteo de saltos, considerando que cada *router* atravesado para llegar a su destino es un salto.

Al contar únicamente saltos, como cualquier protocolo de vector distancia no tiene en cuenta datos como por ejemplo ancho de banda o congestión del enlace. Permite un máximo de 15 saltos o *router*s. (…).

RIP versión 2, tiene las siguientes características:

- Autenticación para la transmisión de información de RIP entre vecinos.
- Utilización de máscaras de red, con lo que ya es posible utilizar sub redes.
- Sumarización de direcciones IP.
- Envío de actualizaciones de tablas de RIP mediante la dirección de multicast 224.0.0.9

Por supuesto además de estas mejoras RIPv2 nos permite la distribución de rutas externas aprendidas por otros protocolos de routing.” (Collado, 2009, p. 74-76).

Gil, Pomares & Candelas (2010) aseguran:

“Con RIP el máximo número de saltos se sitúa en 15, y por ello es utilizado en redes reducidas en cuanto al número de nodos encaminadores. De hecho, una métrica de 16 indica el valor infinito. La descripción del protocolo RIP (Routing Information Protocol) está publicado en la norma RFC 2453, para la versión 2 de este protocolo.” (p. 184).

7.3.2 VLSM

Las máscaras de subred de tamaño variable permiten aprovechar las direcciones IPv4 de forma que pueda asignar un grupo de direcciones IP según la cantidad de host que tenga una red.

Para entender VLSM de mejor manera se lo representará en un ejercicio tomando en cuenta una red con tres oficinas donde tienen 54, 15, 8 host y dos enlaces seriales.

Para la creación de subredes se debe sumar la cantidad total de *host* que tenga la red a implementar para ver el bloque de direcciones a partir del cual se empezará. Hay dos recomendaciones importantes, considerar que a cada red se debe aumentar una dirección IP más que vendría a ser la del *Default Gateway* o puerta de enlace por defecto y un posible aumento del 10% en la cantidad de usuarios (en caso que el cliente no tenga ya un plan al respecto), es decir, se puede suponer una red de 93 direcciones en total incluyendo crecimiento para la implementación de este ejemplo.

Según la Tabla 11, se puede visualizar la forma como se debe tomar las redes empezando desde la más grande hasta la más pequeña que vienen a ser los enlaces seriales.

Tabla 11. Procedimiento para creación de subredes mediante VLSM.

Dirección IPv4											**Descripción**
1er octeto	2do octeto	3er octeto	4to octeto								
192	168	1	0	0	0	0	0	0	0	0	
			2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	Representación base dos elevado a x potencia
			128	64	32	16	8	4	2		Representación mediante números decimales
			126	62	30	14	6	2	0		Cantidad de host admitidos
255	255	255	128	192	222	240	248	252			Máscara de subred correspondiente

En la Tabla 12 se detalla el direccionamiento IP tomando en consideración la Tabla 11.

Tabla 12. Direccionamiento IP para las redes propuestas.

Red	Usuarios	Dirección de red/máscara	Rango disponible	*Broadcast*
Red-1	61	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
Red-2	18	192.168.1.64/27	192.168.1.65 - 192.168.1.94	192.168.1.95
Red-3	10	192.168.1.96/28	192.168.1.97 - 192.168.1.98	192.168.1.99
Enlace serial 1	2	192.168.1.112/30	192.168.1.113 - 192.168.1.114	192.168.1.115
Enlace serial 2	2	192.168.1.116/30	192.168.1.117 - 192.168.1.118	192.168.1.119

7.4 Trabajo preparatorio

Conseguir Packet Tracer versión 6.0.1 (mínimo).

Disponer de un computador de laboratorio o propio con características como sistema operativo Windows (7, 8, 8.1), Linux (Ubuntu, Fedora), procesador 200 MHz o superior, 64 MB RAM o superior.

Usar la topología de la práctica anterior (práctica 6), eliminando las direcciones IPv6. Eliminar las configuraciones IPv6 de la práctica anterior.

Se recomienda que el segundo ejercicio de este laboratorio sea realizado como deber luego de realizar en clase la primera parte.

7.5 Desarrollo de la práctica

Pasos a seguir:

Primera parte del Laboratorio:

1) Revisar el requerimiento del cliente:

   1.1. Esta es una red nueva en la que se desea implementar cuatro *routers*, uno por cada sucursal de la empresa. El protocolo de enrutamiento que

se desea configurar es RIPv2 para permitir una adición de redes en forma más fácil por parte del equipo de sistemas de dicha empresa Figura 30.

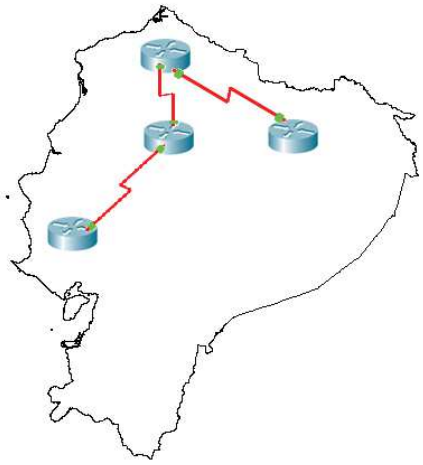

Figura 30. Mapa geográfico representativo del tipo de red a realizar. Adaptado de imagui.com

1.2. La distribución de equipos en esta red será como en la figura a continuación Figura 31.

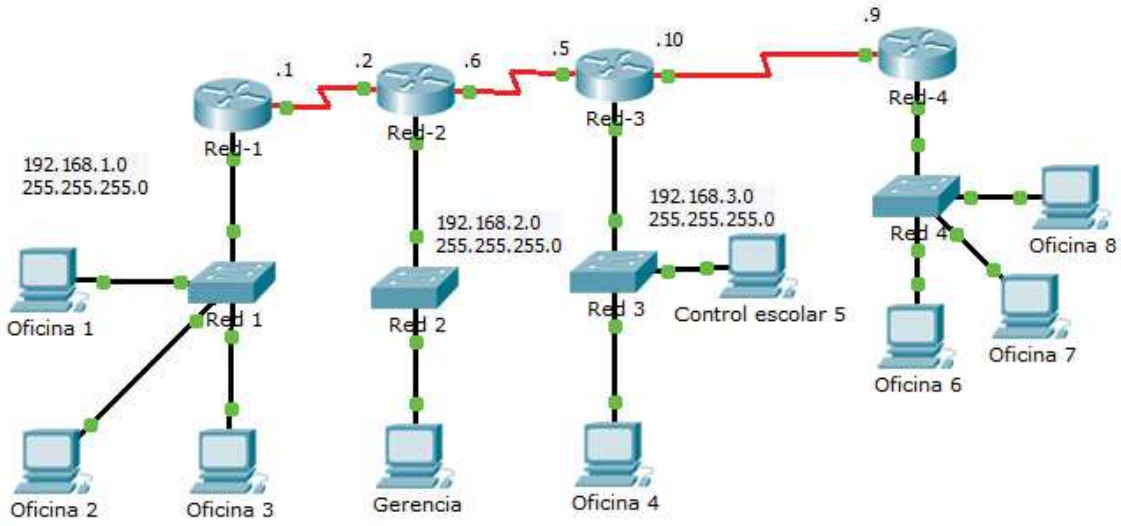

Figura 31. Topología física de red. Tomado de Cisco Packet tracer.

1.3. Los *routers* deben permitir la colocación de al menos dos módulos de comunicación serial y poseer capacidad para dos módulos seriales más de forma que se pueda crecer en un futuro. A los *routers* se les colocará un módulo de expansión para comunicación serial asincrónico y de esa manera poder realizar la comunicación entre ellos.

2) Considerar los siguientes equipos de red para la implementación de la red:

2.1. *Router* ISR 1841 con una interfaz WIC-2T. Cantidad 1. Para colocar la interfaz serial el *router* debe estar apagado.

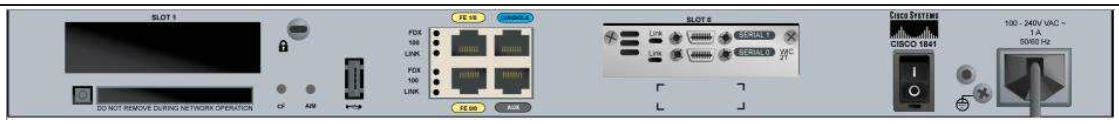

Figura 32. Router Cisco ISR 1841.
Tomado de Cisco Packet Tracer.

Figura 33. Interfaz serial WIC-2T.
Tomado de Cisco Packet Tracer.

2.2. *Switch* 2950 de 24 puertos 10/100/1000 Mbps. Cantidad 1.

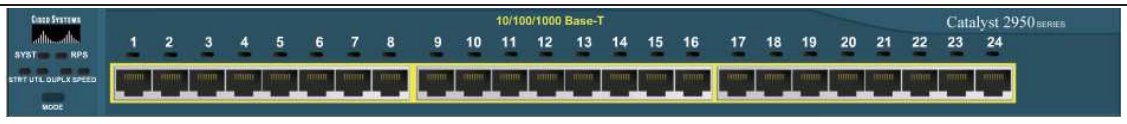

Figura 34. Switch Cisco 2950.
Tomado de Cisco Packet Tracer.

2.3. Computadores. Cantidad 3.

3) Realizar el diagrama de red en Packet Tracer tomando como base el ejercicio de la práctica 6 y completarlo para quedar tal como en la Figura 31 de esta práctica.

4) Realizar las configuraciones iniciales en el *router* de la red-4, tal como en los demás *router*s. Llenar la Tabla 13.

Tabla 13. Tabla de direccionamiento IP de enlaces seriales.

Línea Serial			
Nombre del *Router*	**Dirección IP**	**Mascara de Subred**	**Clock Rate**
Red-3			
Red-4			

5) Configurar el protocolo de enrutamiento dinámico RIP v2. Se debe escribir todas las rutas conectadas directamente al *router* como en el siguiente ejemplo:

```
RED-1(config)#router rip
RED-1(config-router)#version 2
RED-1(config-router)#network 192.168.0.0
RED-1(config-router)#network 192.168.1.0

RED-2(config)#router rip
RED-2(config-router)#version 2
RED-2(config-router)#network 192.168.0.0
RED-2(config-router)#network 192.168.2.0
RED-2(config-router)#network 192.168.0.4

RED-3(config)#router rip
RED-3(config-router)#version 2
RED-3(config-router)#network 192.168.0.4
```

RED-3(config-*router*)#network 192.168.0.8
RED-3(config-*router*)#network 192.168.3.0

RED-4(config)#router rip
RED-4 (config-router)#version 2
RED-4 (config-router)#network 192.168.0.8
RED-4 (config-*router*)#network 192.168.4.0

6) Asignar direcciones IP a los Host. Llenar la tabla 14.

Tabla 14. Tabla de asignación de direcciones IP para los computadores.

PC	**Dirección IP**	**Mascara de Subred**	**Puerta de Enlace**
Oficina 6			
Oficina 7			
Oficina 7			

7) Comprobar conexión mediante un *ping* entre los computadores de las tres redes.

Segunda parte del Laboratorio:

1) Armar la siguiente topología de red:

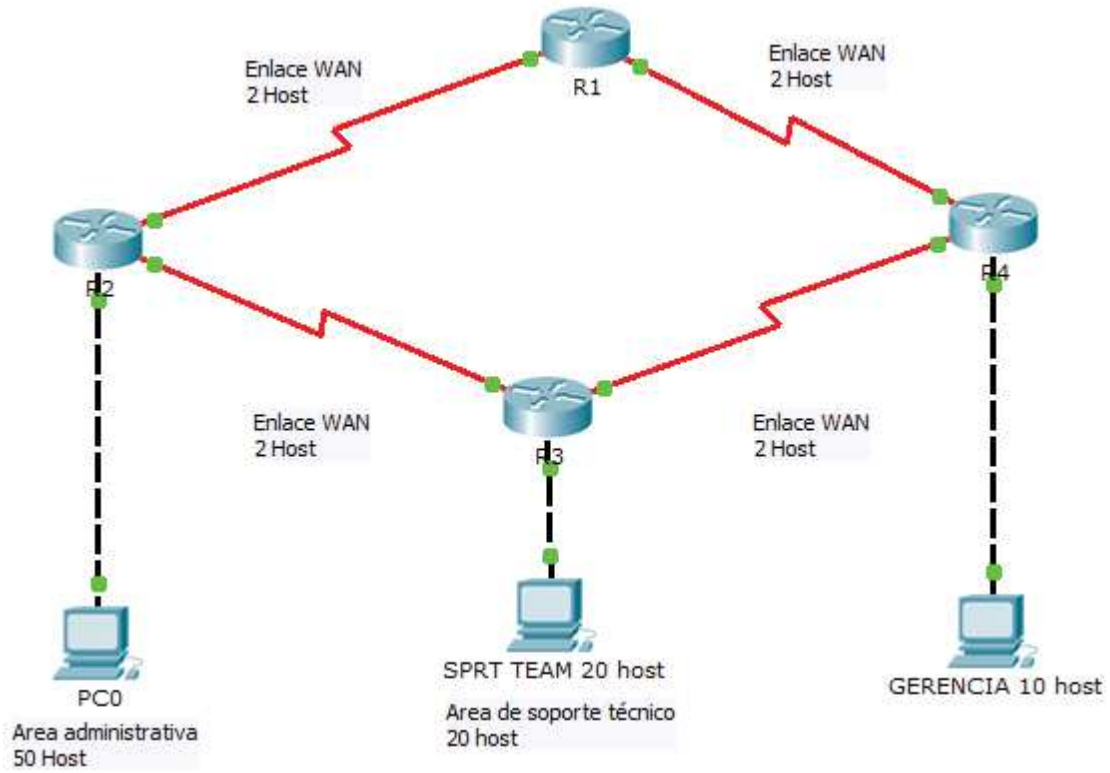

Figura 35. *Topología para la segunda parte de la práctica.*
Tomado de Cisco Packet Tracer

2) Elaborar el direccionamiento IP con VLSM considerando el requerimiento específico para esta topología:
   Partiendo de la dirección 192.168.0.0/24
   Para el área ADMINISTRATIVA se requieren 50 host
   Para el área de SOPORTE TÉCNICO se requieren 20 host
   Para el área de GERENCIA se requieren 10 host
   Para 4 enlaces seriales.

3) Llenar la siguiente tabla con el direccionamiento IP para la topología.

Tabla 15. Direccionamiento IP.

Áreas de la red	**Dirección de red**	**Rango IP disponible**	**Broadcast**
Área administrativa			
Área de soporte técnico			
Área de gerencia			
Enlaces seriales			

4) Configurar el protocolo RIPv2 en los routers de la topología.

5) Comprobar la conectividad entre host.

7.6 Resultados de aprendizaje

- Adecuar una red configurada con rutas estáticas, para que funcione con el protocolo RIP v2.
- Emplear un protocolo de enrutamiento dinámico para que una topología tenga mayor escalabilidad y mejorar los tiempos de administración.
- Listar ventajas y desventajas del ruteo estático y dinámico.
- Emplear VLSM para el aprovechamiento de las direcciones IP.

7.7 Conclusiones

- Un protocolo de enrutamiento dinámico disminuye el tiempo y complejidad en la administración de una red.
- RIP y otros protocolos de enrutamiento permiten una mejor escalabilidad de la red ya que al aumentar *router*s basta con incluir las nuevas rutas en la configuración de RIP.
- Para el direccionamiento lógico de una red hay que tomar en cuenta si el cliente tiene un plan de crecimiento a futuro de su red, sino tomar la precaución de dimensionar bloques de direcciones IP con un posible crecimiento de usuarios.

7.8 Tiempo estimado de la práctica

Una sesión de clase.

7.9 Evaluación/ cuestionario

1. ¿Por qué RIP v2 permite una administración más rápida y mejor escalabilidad en una red WAN?
2. ¿Se admite VLSM en la configuración de RIP v2?
3. ¿Cuántos *router*s permite una topología configurada con RIP v2?
4. ¿Es necesario especificar las redes del *router* Red-4 en las configuraciones del *router* Querétaro? Explicar por qué si o por qué no.
5. ¿Qué factores hay que tomar en cuenta para dimensionar un bloque de direcciones IP con VLSM?

CAPÍTULO VIII CONFIGURACIÓN DE UNA RED WAN CON 5 *ROUTER*S

Materiales / herramientas

Descripción de los equipos/herramientas/*software* necesitados para la práctica.

- 1 Computador (laboratorio de redes)
- 1 Cisco Packet Tracer

8.1 Objetivo general

Incorporar el protocolo RIPng para ruteo dinámico en una red con IPv6.

8.2 Objetivos específicos

1. Configurar el protocolo RIPng para IPv6.
2. Analizar la diferencia en la configuración de IPv4 frente a la de IPv6.
3. Desarrollar un conocimiento base para la implementación de IPv6 en un entorno real.

8.3 Marco teórico

8.3.1 RIPng

> "RIPng es un protocolo basado en el algoritmo de vector distancia llamado Bellman-Ford. Muchos de los conceptos de RIPng han sido tomados de RIPv1 y RIPv2, los cuales ha tenido implementado IPv4 por mucho tiempo.
>
> RIPng usa un simple mecanismo para determinar la métrica (costo) de una ruta. Básicamente cuenta el número de *router*s (saltos) hacia el destino. Cada *router* cuenta como un salto. Los *router*s con una distancia administrativa mayor a 15 o igual a 16 son considerados como inalcanzables. El *router* periódicamente distribuye información sobre sus

rutas hacia los *router*s conectados a él usando mensajes de respuesta RIPng.” (Hagen, 2014, p. 137).

“Básicamente, las principales características de RIPng son las mismas que RIPv2. Todavía usa multicast para actualizaciones, pero en IPv6 se usa FF02::9. Probablemente los mayores cambios con la nueva versión (y con todos los protocolos de enrutamiento que funcionan con IPv6), es que tienes que activar o anunciar a la interfaz de red que se usará la versión 6 del protocolo IP.” (Lammle, 2007, p. 751).

8.4 Trabajo preparatorio

Conseguir Packet Tracer versión 6.0.1 (mínimo).

Disponer de un computador de laboratorio o propio con características como sistema operativo Windows (7, 8, 8.1), Linux (Ubuntu, Fedora), procesador 200 MHz o superior, 64 MB RAM o superior.

Usar la topología de la práctica anterior. Comprobar que tenga direcciones IP configuradas en las interfaces de los dispositivos.

8.5 Desarrollo de la práctica

Pasos a seguir:

1) Revisar el requerimiento del cliente:

1.1. Se plantea una época en el que las redes migrarán hacia IPv6. Una empresa se plantea la creación una red con comunicación IPv6 en su totalidad, es decir, en sus cinco oficinas a nivel nacional donde además se requerirá de una actualización de equipos, para lo cual se considerará el equipamiento necesario para dicha actualización considerando que en cada oficina pueden tener un crecimiento de 10 hasta 20 empleados a futuro (Figura 36 y 37).

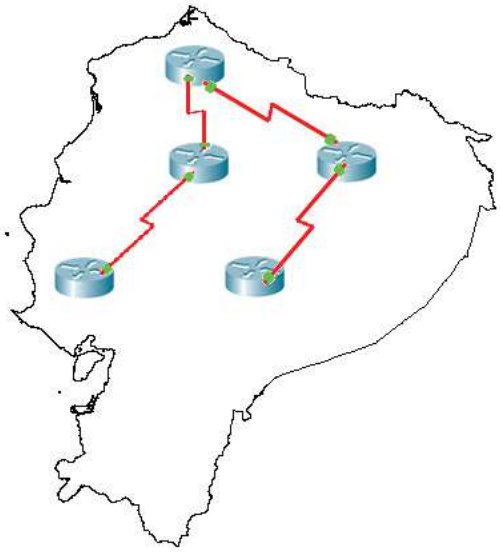

Figura 36. Mapa geográfico representativo del tipo de red a realizar.
Adaptado de imagui.com

1.2. Cada red tendrá conectado un switch y la cantidad de computadores mostrada en la Figura 37.

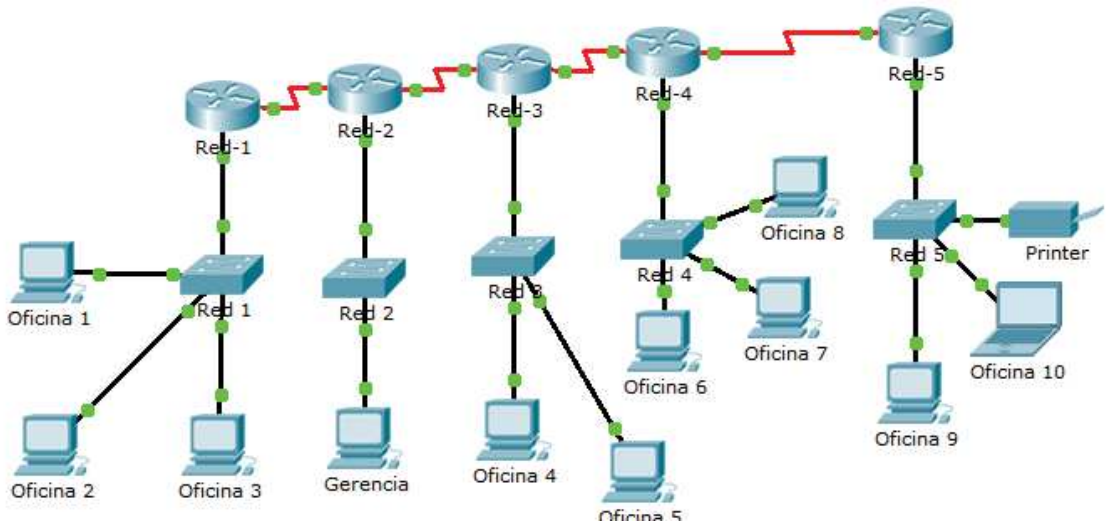

Figura 37. Topología física de red.
Tomado de Cisco Packet Tracer.

2) Armar la topología de la Figura 37, usar como base la anteriormente hecha en la práctica 7. Considerar los siguientes equipos de red para la implementación de la red:

2.1. *Router* ISR 1841 con una interfaz WIC-2T. Cantidad 2. Para colocar la interfaz serial el *router* debe estar apagado.

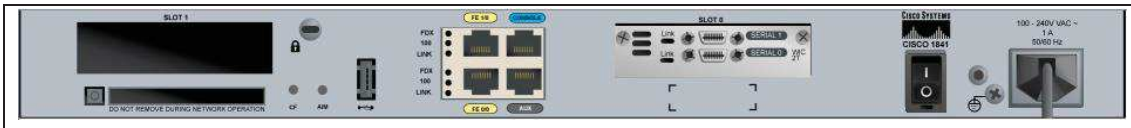

Figura 38. Router Cisco ISR 1841.
Tomado de Cisco Packet Tracer.

Figura 39. Interfaz serial WIC-2T.
Tomado de Cisco Packet Tracer.

2.2. *Switch* 2950 de 24 puertos 10/100/1000 Mbps. Cantidad 2.

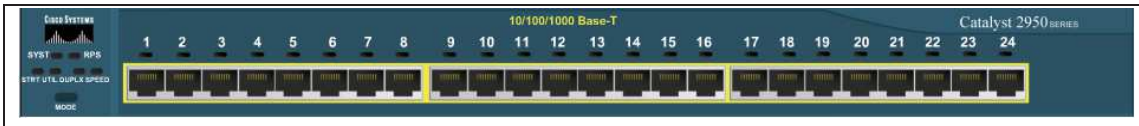

Figura 40. Switch Cisco 2950.
Tomado de Cisco Packet Tracer.

2.3. Computadores. Cantidad 4.

2.4. Impresora IP. Cantidad 1.

Figura 41. Ícono de impresora en Packet Tracer.
Tomado de Cisco Packet Tracer.

3) Realizar las configuraciones básicas en el nuevo enlace entre los *router*s de la red número 4 y 5, tal como en los demás *router*s. Llenar la Tabla 15, 16 y 17.

Tabla 16. Tabla de direccionamiento IP del *router* Red-3.

Red-3		
Interfaz	**Dirección IP**	**Longitud del prefijo**
S0/0/1	2001:db8:6::1/64	64

Tabla 17. Tabla de direccionamiento IP para el *router* Red-4.

Red-4		
Interfaz	**Dirección IPv6**	**Longitud del prefijo**
Fa0/0	2001:db8:7::1/64	64
S0/0/0	2001:db8:6::2/64	64
S0/0/1	2001:db8:8::1/64	64

Tabla 18. Tabla de direccionamiento IP para el *router* Red-5.

Red-5		
Interfaz	**Dirección IP**	**Longitud del prefijo**
Fa0/0	2001:db8:9:1/64	64
S0/0/0	2001:db8:8::2/64	64

4) Introducir el comando para permitir el envío de paquetes IPv6. Esta configuración se debe hacer en todos los *router*s.

```
RED-1(config)#ipv6 unicast-routing
```

5) Habilitar el protocolo de enrutamiento dinámico RIPng. Se debe introducir el siguiente comando en todos los *router*s, colocando al final el número/nombre de proceso del protocolo (puede ser cualquier número o palabra).

RED-1(config)#ipv6 *router* rip 1

6) Habilitar el protocolo RIPng en cada una de las interfaces de los *router*s mediante un comando que sigue la siguiente estructura:
ipv6 rip –*número/nombre de proceso*- enable

Ejemplo:
RED-1(config-if)#ipv6 rip 1 enable

7) Asignar direcciones IP a los Host. Llenar la tabla 18.

Tabla 19. Tabla de direcciones IP para computadores.

PC	**Dirección IP**	**Mascara de Subred**	**Puerta de Enlace**
Oficina 6			
Oficina 7			
Oficina 7			

8) Comprobar la conectividad ubicándose en cualquier host de la red 5 (*router* Red-5), y hacer ping a un host de la Red-1 (*router* Red-1). Ejemplo Figura 42.

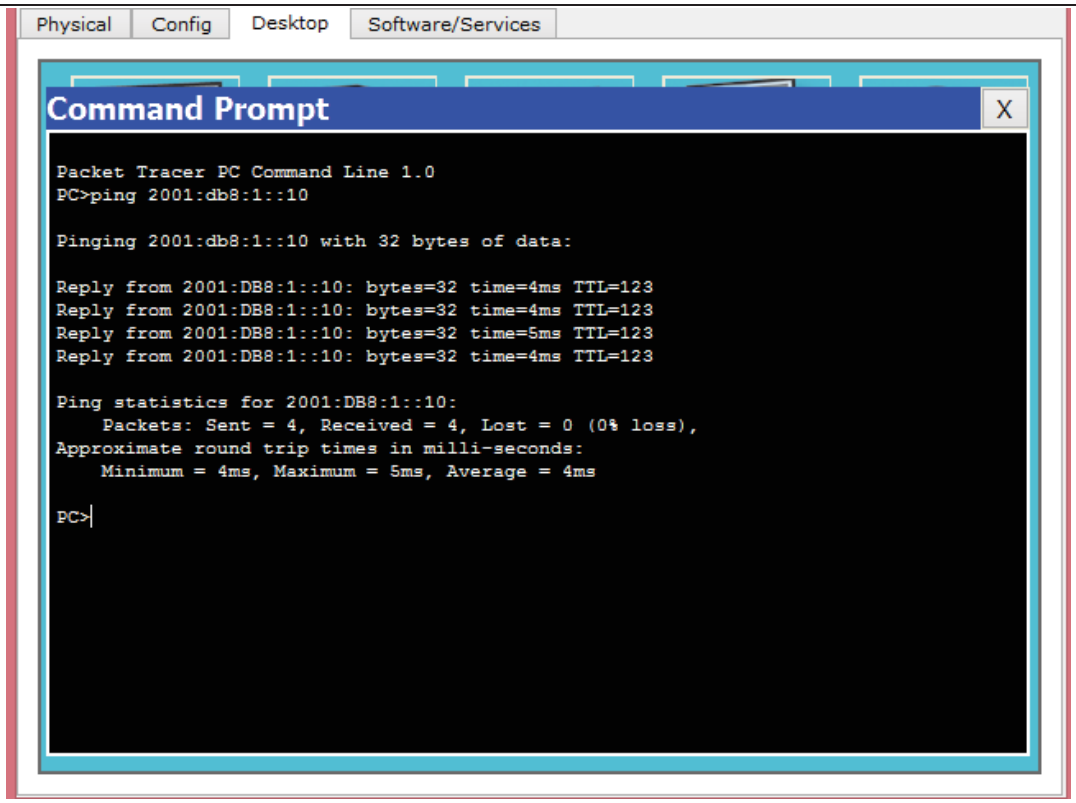

Figura 42. Ventana de un host de Packet Tracer que representa el CMD de Windows.

Tomado de Cisco Packet Tracer.

8.6 Resultados de aprendizaje

- Emplear el protocolo de enrutamiento dinámico RIPng diseñado específicamente para IPv6.
- Adecuar una red anteriormente funcionando con IPv4, para que trabaje con el protocolo IPv6 y su protocolo de enrutamiento RIPng.

8.7 Conclusiones

- El protocolo de enrutamiento RIPng se implementa más rápido en comparación al RIPv2.
- En RIPng no es necesario especificar todas las redes que se conectan a este, sino que basta con activarlo en las interfaces.
- Las características de RIPv2 y RIPng son básicamente las mismas, por ejemplo el número de saltos máximos permitidos.

- Se pueden crear diferentes identificadores de proceso en la configuración de RIPng, tal como en el protocolo OSPF, no es necesario que se tenga el mismo nombre o número de proceso en todos los *router*s, de todas maneras los paquetes se encaminarán, tan solo es un identificador local.

8.8 Tiempo estimado de la práctica

Una sesión de clase.

8.9 Evaluación/ cuestionario

1. ¿Cuántos saltos tiene como máximo RIPng?
2. ¿Cuál es el comando para activar el envío de paquetes IPv6?
3. ¿Es necesario activar el protocolo RIPng en cada interfaz?

CAPÍTULO IX CONFIGURACIÓN DE UNA RED WAN CORPORATIVA

Materiales / herramientas
Descripción de los equipos/herramientas/*software* necesitados para la práctica.

- 1 Computador (laboratorio de redes)
- 1 Cisco Packet Tracer

9.1 Objetivo general

Incorporar el protocolo OSPFv3 en una red corporativa de acuerdo al requerimiento de un cliente supuesto, considerando la configuración de un doble *stack*, para que una red empresarial pueda usar los dos protocolos IPv4 e IPv6 simultáneamente.

9.2 Objetivos específicos

1. Configurar el protocolo de enrutamiento dinámico para IPv6, OSPFv3
2. Desarrollar la topología con el equipamiento y módulos correctos para cubrir las necesidades de un cliente.
3. Configurar los *router*s para que arranquen con una versión avanzada del IOS y de esa manera dar a los dispositivos las características necesarias que exige la configuración de esta red.
4. Configurar una red con doble *stack*.

9.3 Marco teórico

9.3.1 OSPFv3

Los protocolos de estado enlace se han convertido en una alternativa popular que los protocolos de vector distancia. OSPFv3 es la versión del protocolo OSPF compatible con IPv6, la métrica de OSPFv3 todavía se basa en el costo del enlace, es decir que considera la congestión en el enlace y el ancho de

banda del mismo. Los tipos de paquetes y los mecanismos de descubrimiento de vecinos son los mismos en la versión 2 y 3 del protocolo en cuestión.

> “Al comparar OSPF v2 y OSPF v3, muchos aspectos recuerdan las mismas características entre las dos versiones; tales como las reglas LSA, el mecanismo de asignación de LSA, y los tipos de difusión (broadcast, punto a punto, punto a multipunto, entre otros). Los formatos LSA de OSPF v3 difieren de la versión 2; específicamente OSPF v3 añade dos nuevos tipos de LSA, el 0x0008 usado para anunciar uno o más prefijos IPv6 en un enlace dado y el 0x2009 usado para publicar uno o más prefijos IPv6 asociados con el segmento del *router*, segmento de red o segmento de red de tránsito.” (Hogg, 2013).

“Los LSA (paquetes de estado enlace), son creados por todos los *router*s de una topología para describir su parte local del dominio de enrutamiento. Tomados juntos, los LSA se usan para los cálculos de enrutamiento.” (Moy, 2004, p. 74).

El proceso OSPF para IPv6 no requiere de una dirección IPv4 a ser configurada en el *router*, pero requiere de un valor de 32 bits para el *Router*-ID, el cual usa una notación similar a las direcciones IPv4; el *router* ID se define usando el comando “*router* ID”. Si el *router* ID no es configurado, el sistema intentará asignarlo dinámicamente escogiendo un ID de acuerdo a la dirección IPv4 activa de mayor valor, si no hay direcciones IPv4 configuradas, el proceso fallará al iniciar. Para activar el proceso OSPF IPv6 en una interfaz y asignar esa interfaz a un área se usa el comando “ipv6 ospf *proceso-ospf* area *area-id*“. Las áreas en el protocolo OSPF vienen a ser una serie de escalafones en el enrutamiento, donde el área cero es el área principal que abarca las demás áreas; las áreas se pueden intercomunicar entre sí independientemente del número que se les asigne.

La selección del *router* ID sigue una secuencia, primeramente considera el mismo *router* ID configurado, luego la dirección *loopback* y por último las interfaces físicas configuradas, tomando siempre la más alta en cada caso.

OSPF se puede configurar con áreas múltiples siempre y cuando el área cero esté en el centro de todas las áreas, ya que a esta área se le considera como el *backbone* por el cual se lleva a cabo el enrutamiento de los paquetes hacia el internet. Figura 43.

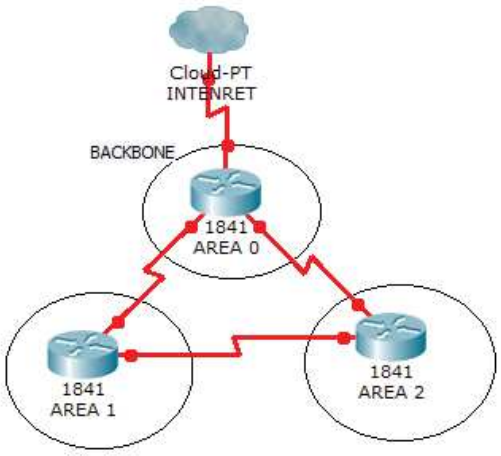

Figura 43. Diagrama de áreas en OSPF v3.
Adaptada de Cisco Packet Tracer.

9.4 Trabajo preparatorio

Conseguir Packet Tracer versión 6.0.1 (mínimo).

Disponer de un computador de laboratorio o propio con características como sistema operativo Windows (7, 8, 8.1), Linux (Ubuntu, Fedora), procesador 200 MHz o superior, 64 MB RAM o superior.

9.5 Desarrollo de la práctica

Pasos a seguir:

1) Revisar el requerimiento del cliente:

1.1. Una entidad bancaria requiere la conexión de 3 sucursales que se encuentran en la misma ciudad pero en lugares remotos de la misma. Figura 44.

Figura 44. Mapa geográfico representativo del tipo de red a realizar.
Adaptado de google maps.

1.2. El departamento técnico especifica la necesidad de implementar un router para cada una de las sucursales y se conectarán 2 *switches* a cada una. A continuación se muestra la cantidad de equipos y su distribución. Figura 45.

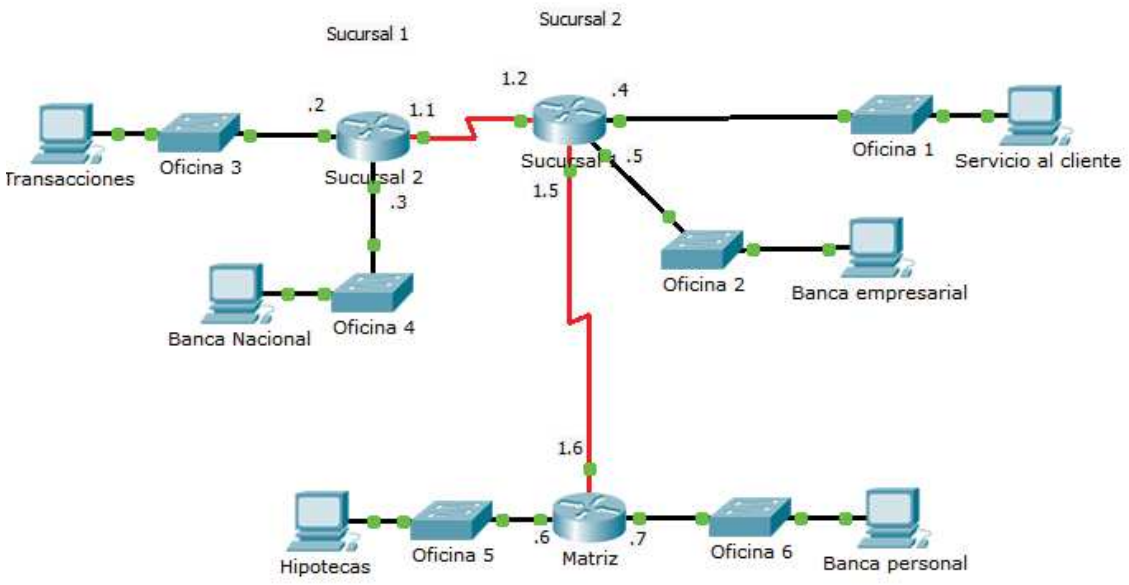

Figura 45. Topología física de red.
Tomado de Cisco Packet Trace.

1.3. Los *switches* deberán tener 24 puertos para la conexión de las computadoras y futuro crecimiento. Los *router*s deben ser de tipo modular, es decir, que permita el aumento de módulos de forma que la red sea escalable y facilite el crecimiento de la red, deberán dejar al menos 2 ranuras libres.

2) Considerar los siguientes equipos de red para la implementación de la red con sus respectivos módulos adicionales:

2.1. *Router* 2620XM con interfaces WIC-2T y NM-2FE2W.

*Figura 46.*Router Cisco 2620XM.
Tomado de Cisco Packet Tracer.

Figura 47. Interfaz serial WIC-2T.
Tomado de Cisco Packet Tracer.

Figura 48. Interfaz serial NM-2FE2W.
Tomado de Cisco Packet Tracer.

De forma que el *router* quede de la siguiente manera:

Figura 49. Router Cisco 2620XM con todos sus módulos instalados.
Tomado de Cisco Packet Tracer.

2.2. *Switch* 2950 de 24 puertos 10/100/1000 Mbps. Cantidad 6.

Figura 50. Switch Cisco 2950.
Tomado de Cisco Packet Tracer.

2.3. Computadores. Cantidad 6.

3) Reemplazar el IOS con el que funciona un *router* para poder configurar IPv6.

3.1. Conectar un servidor a la interfaz libre del *router*. Configurar una dirección IPv4 en el servidor. Figura 51.

Figura 51. Diagrama de conexión del servidor TFTP para cambiar IOS.
Tomado de Cisco Packet Tracer.

3.2. Introducir los siguientes comandos en el *router*:

router**#copy tftp: flash:**

Address or name of remote host []? **192.168.0.10**

Source filename []? **c2600-advipservicesk9-mz.124-15.T1.bin**
Destination filename [c2600-advipservicesk9-mz.124-15.T1.bin]? ***presionar-enter***

3.3. Activar la imagen IOS copiada y reiniciar para que el *router* funcione con la nueva versión configurada.
router#config terminal
router(config)#boot system flash:/c2600-advipservicesk9-mz.124-15.T1.bin
router(config)#end
router#wr
router#reload

3.4. Realizar los mismos pasos con los otros dos *router*s y borrar el servidor utilizado al finalizar.

4) Configurar las interfaces del *router* “Sucursal 1” con IPv6. Llenar la Tabla 19.

Tabla 20. Tabla de direccionamiento IP del *router* “Sucursal 1”.

Sucursal 1			
Interfaz	Dirección IP	Longitud del prefijo	Clock Rate
Fa1/0			
Fa1/1			
S0/0			
S0/1			

5) Configurar las interfaces del *router* “Sucursal 2” con IPv6. Llenar la Tabla 20.

Tabla 21. Tabla de direccionamiento IP del *router* “Sucursal 2”.

Sucursal 2			
Interfaz	Dirección IP	Longitud del prefijo	Clock Rate
Fa1/0			
Fa1/1			
S0/0			

6) Configurar las interfaces del *router* “Matriz” con IPv6. Llenar la Tabla 21.

Tabla 22. Tabla de direccionamiento IP del *router* “Matriz”.

Matriz			
Interfaz	Dirección IP	Longitud del prefijo	Clock Rate
Fa1/0			
Fa1/1			
S0/0			

7) Asignar direcciones IP a los Host con IPv6. Tabla 22.

Tabla 23. Tabla de direccionamiento IP para computadores.

PC	Dirección IP	Longitud del prefijo	Puerta de Enlace
Servicio al cliente			
Banca empresarial			
Transacciones			
Banca Nacional			
Hipotecas			
Banca personal			

8) Configurar el protocolo de enrutamiento dinámico OSPFv3, para lo cual es necesario introducir los comandos en cada interfaz, ejemplo:
Sucursal1(config)#ipv6 unicast-routing

```
Sucursal1(config)#ipv6 router ospf 1
Sucursal1(config)#interface fa1/0
Sucursal1(config-if)#ipv6 ospf 1 area 0
Sucursal1(config-if)#exit
Sucursal1(config)#int fa1/1
Sucursal1(config-if)#ipv6 ospf 1 area 0
Sucursal1(config-if)#exit
```

9) Realizar las mismas configuraciones en todos los *router*s y en todas sus interfaces.

10) Designar al router “Sep1” como router-id.

```
Sucursal1(config)# ipv6 router ospf 1
Sucursal1(config)#router-id 1.1.1.1
```

11) Configurar direcciones IPv4 en las interfaces de los *router*s y en los host, tomar las direcciones del bloque 192.168.1.0/24

12) Establecer rutas estáticas IPv4 entre las diferentes redes.

13) Introducir los siguientes comandos

```
Sucursal2# ping 2001:DB8:2::1
Sucursal2# show ipv6 interface
Sucursal2# show ipv6 route ospf
```

9.6 Resultados de aprendizaje

- Adecuar un *router* para que funcione con una versión superior de software para poder realizar configuraciones avanzadas.
- Emplear OSPFv3 para redes IPv6.
- Seleccionar el *router*-id para elegir el *router* encargado de las actualizaciones de topología mediante paquetes LSA.

9.7 Conclusiones

- Los comandos que se pueden ingresar en un dispositivo de red depende de la versión de sistema que tenga instalado, en el caso de cisco este sistema se llama IOS.
- Cada dispositivo de red ofrece diferentes capacidades y debe ser elegido según los requerimientos del cliente, siempre que sean coherentes o de acuerdo a las características necesarias para que la topología funcione.
- El protocolo de enrutamiento OSPFv3 no requiere de la especificación de las rutas que contiene el *router*, sino solo de la activación en cada interfaz, al igual que RIPng. Lo cual permite un tiempo de configuración menor en comparación a la versión anterior de OSPF.
- La dirección IP más alta es la 255.255.255.255 y la más baja es la 1.1.1.1, tomando esta consideración se puede asignar un valor a un *router* para la elección del *router* ID.

9.8 Tiempo estimado de la práctica

Una sesión de clase.

9.9 Evaluación/ cuestionario

1. ¿Cuál es el resultado de los comando del paso 13 de la práctica?
2. ¿Cuál es el área OSPF hacia la cual deben dirigirse todas las demás?
3. ¿Para qué sirve el *Router*-ID, es necesario y qué sucede si no se configura?
4. ¿Qué se debe hacer luego de cambiar de IOS en un *router* Cisco, para que tenga vigencia la nueva versión configurada?

CAPÍTULO X CONFIGURACIÓN DE UNA RED DE COMUNICACIÓN INTERNACIONAL

Materiales / herramientas

Descripción de los equipos/herramientas/*software* necesitados para la práctica.

- 1 Computador (laboratorio de redes)
- 1 Cisco Packet Tracer

10.1 Objetivo general

Incorporar el protocolo de enrutamiento EGP para lograr una comunicación entre dos sistemas autónomos.

10.2 Objetivos específicos

1. Configurar el protocolo BGP para unir sistemas autónomos diferentes.
2. Desarrollar una configuración considerando el método más acertado de enrutamiento de paquetes para la red propuesta.
3. Configurar una red de tipo internacional considerando los dispositivos y módulos necesarios.
4. Analizar el requerimiento del cliente, de forma que las especificaciones de los dispositivos propuestos igualen o superen la petición hecha inicialmente.

10.3 Marco teórico

10.3.1 IGP y EGP

Existen dos tipos de protocolos de enrutamiento dinámico, están divididos en los grupos IGP (Interior Gateway Protocol) y EGP (Exteriro gatewaay protocol).

> “Los protocolos IGP son aquellos usados dentro de un sistema autónomo, entendiéndose por sistema autónomo un grupo de redes que

> están regidos por una sola política de enrutamiento, es decir un mismo IGP. Su tarea es la de intercambiar información de enrutamiento entre *router*s pertenecientes a un mismo sistema autónomo. Entre los protocolos de Gateway interno más conocidos están RIP, RIPv2, EIGRP y OSPF.
>
> EGP se refiere a los protocolos de Gateway externo que se usan para la interconexión de diferentes sistemas autónomos, el protocolo más conocido para esta configuración es el BGP. La utilización de este protocolo es vital pues permite la comunicación de redes con diferentes políticas de enrutamiento de paquetes, es decir, disímiles protocolos de enrutamiento; ya que la única forma de intercomunicar redes con distintos protocolos IGP sería mediante un protocolo intermediario entre estos el cual viene a ser BGP. De esta manera es como se logra el intercambio de paquetes sin importar el IGP configurado en las demás redes." (Held, 2003, p. 158).

"Para la interconexión de sistemas autónomos que usualmente tiene configurados distintos tipos de IGP, es necesario un protocolo que sirva de intermediario entre los mismos, ya que la función de un EGP con un IGP no son las mismas." (Tanenbaum, 2003, p. 459).

> "El protocolo BGP está diseñado de tal manera que no se produzcan bucles y no importen las políticas de enrutamiento de cada sistema autónomo. La métrica que utiliza es conocida como vector ruta y su forma de funcionamiento consiste en que todos los *router*s conectados directamente al destino le envían sus rutas de recorrido desde el origen hasta el destino, para finalmente examinar, seleccionar y recordar la mejor ruta de entre todas. Si algún enlace deja de estar activo simplemente no se lo considera y si la mejor ruta hacia el destino resulta afectada, se vuelve a reconsiderar la mejor ruta." (Clark, 2003, p. 259).

10.4 Trabajo preparatorio

Conseguir Packet Tracer versión 6.0.1 (mínimo).

Disponer de un computador de laboratorio o propio con características como sistema operativo Windows (7, 8, 8.1), Linux (Ubuntu, Fedora), procesador 200 MHz o superior, 64 MB RAM o superior.

Realizar con anticipación la topología de este laboratorio y Llenar anticipadamente las bases técnicas para switches y routers presentadas por el cliente según el paso 1 y todos sus literales. La información se puede encontrar en hojas técnicas (datasheet) en la página del fabricante. Los modelos a considerar son los del packet tracert.

10.5 Desarrollo de la práctica

Pasos a seguir:

a) Revisar el requerimiento del cliente:

a.1. Una corporación farmacéutica nacional quiere comunicarse con todas las sucursales ubicadas en el país y además con su nueva sucursal en Perú.

a.2. El equipo técnico de la corporación ve la necesidad de implementar *router*s para cada una de las ciudades y conectarán en cada uno de ellos 3 *switches* (Oficinas) con al menos 24 puertos cada *switch* para la conexión de las computadoras que conformaran los laboratorios y oficinas. Los *router*s se llamarán Loja, Cuenca, Ambato, Quito, Carchi y Perú. Se muestra a continuación la cantidad de equipos, su distribución y la clase de red la determina el usuario. (Figura 52).

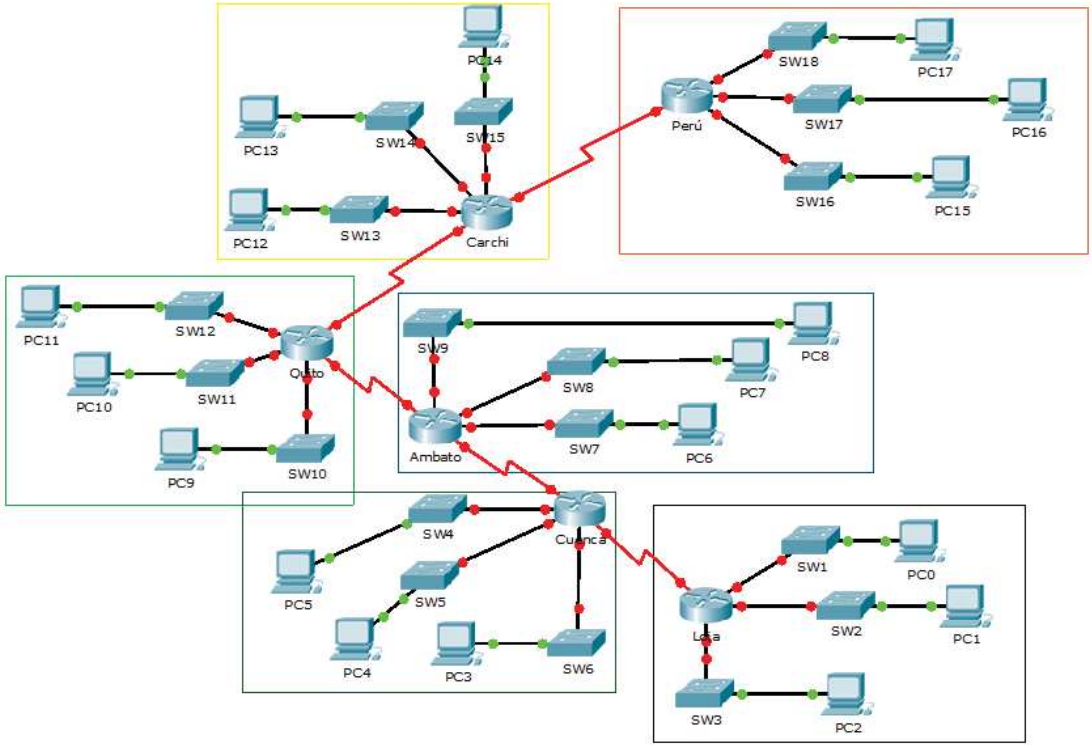

Figura 52. Topología física de red.
Tomado de Cisco Packet Tracer.

a.3. Cada *router* deberá tener un módulo que contenga dos líneas serial asincrónica para realizar la comunicación entre cada red y suficientes interfaces *Fast Ehternet* para la conectar los swtiches. Los *router*s (Tabla 23) y *switches* (Tabla 24) deberán cumplir con las bases técnicas entregadas por el cliente; estas bases se deben considerar como requerimientos mínimos, los cuales se pueden igualar o superar.

Tabla 24. Bases técnicas del *Router*.

Router	
Funcionalidad	**Cumplimiento del oferente**
Marca: a porponer por el oferente	
Modelo: a porponer por el oferente	
Router Modular	
Módulos de red: 1	
Capacidad de tarjetas WAN: 2	
Puertos *Fast ethernet*: 1	
Paquetes por segundo: 30 Kpps	
DRAM: 256 MB	
Flash memory: 32MB	
Versión IOS Software IP Base	

Tabla 25. Bases técnicas del *switch*.

Switch	
Funcionalidad	**Cumplimiento del proveedor**
Marca: a porponer por el oferente	
Modelo: a porponer por el oferente	
24 puertos 10/100/1000	
DRAM: 128MB	
Flash: 64MB	
Ancho de banda de reenvío (Forwarding bandwidth): 88Gbps	
Capacidad de *switch*ing (*switch*ing bandwith): 176 Gbps	
MTU: 9198 bytes	
Jumbo frame: 9216 bytes	
IOS LAN base	

2. Configurar direcciones IPv4 e IPv6 en el *router* "Loja". Ejemplo:

```
LOJA(config)#int fa1/1
LOJA(config-if)#ip addr 192.168.3.1 255.255.255.0
LOJA(config-if)#ipv6 enable
LOJA(config-if)#ipv6 addr 2001:db8:8::1/64
LOJA(config-if)#exit
```

Tabla 26. Tabla de direccionamiento IP para el *router* Loja. Llenar la tabla.

Loja			
Interfaz	Dirección de red	Mascara subred	Clock Rate
Fa1/0			
Fa1/1			
Fa0/0			
S0/0			
S0/1			

3. Configurar direcciones IPv4 e IPv6 en el *router* "Cuenca".

Tabla 27. Tabla de direccionamiento IP para el *router* Cuenca. Llenar la tabla.

Cuenca			
Interfaz	Dirección de red	Mascara subred	Clock Rate
Fa1/0			
Fa1/1			
Fa0/0			
S0/0			
S0/1			

4. Configurar direcciones IPv4 e IPv6 en el *router* "Ambato".

Tabla 28. Tabla de direccionamiento IP para el *router* Ambato. Llenar la tabla.

Ambato			
Interfaz	Dirección de red	Mascara subred	Clock Rate
Fa1/0			
Fa1/1			
Fa0/0			
S0/0			
S0/1			

5. Configurar direcciones IPv4 e IPv6 en el *router* “Quito”.

Tabla 29. Tabla de direccionamiento IP para el *router* Quito. Llenar la tabla.

Quito			
Interfaz	Dirección de red	Mascara subred	Clock Rate
Fa1/0			
Fa1/1			
Fa0/0			
S0/0			
S0/1			

6. Configurar direcciones IPv4 e IPv6 en el *router* “Carchi”.

Tabla 30. Tabla de direccionamiento IP para el *router* Carchi. Llenar la tabla.

Carchi			
Interfaz	Dirección de red	Mascara subred	Clock Rate
Fa1/0			
Fa1/1			
Fa0/0			
S0/0			
S0/1			

7. Configurar direcciones IPv4 e IPv6 en el *router* “Perú”.

Tabla 31. Tabla de direccionamiento IP para el *router* Perú. Llenar la tabla.

Perú			
Interfaz	Dirección de red	Mascara subred	Clock Rate
Fa1/0			
Fa1/1			
Fa0/0			
S0/0			
S0/1			

8. Asignar direcciones IP a los host.

9. Configurar un protocolo de enrutamiento que mejor se ajuste con la topología de red, ya sea IGP o ruta estática. Justificar en la sección de preguntas.

10. Configurar el protocolo BGP en los *router*s de borde de cada sistema autónomo, donde el *router* Carchi corresponde al *router* de borde del sistema autónomo 100, y el *router* Perú pertenece al sistema autónomo 200. La configuración deberá realizarse con las direcciones de red que se encuentren dentro de cada sistema autónomo, como en el siguiente ejemplo:

    CARCHI(config)#router bgp 100
    CARCHI(config-router)#neighbor 192.168.0.18 remote-as 200
    CARCHI(config-router)#network 192.168.0.0 mask 255.255.255.252
    CARCHI(config-router)#network 192.168.0.4 mask 255.255.255.252
    CARCHI(config-router)#network 192.168.0.8 mask 255.255.255.252
    CARCHI(config-router)#network 192.168.0.12 mask 255.255.255.252
    CARCHI(config-router)#network 192.168.1.0 mask 255.255.255.0
    CARCHI(config-router)#network 192.168.2.0 mask 255.255.255.0
    CARCHI(config-router)#network 192.168.3.0 mask 255.255.255.0
    CARCHI(config-router)#network 192.168.4.0 mask 255.255.255.0

CARCHI(config-router)#network 192.168.5.0 mask 255.255.255.0
CARCHI(config-router)#network 192.168.6.0 mask 255.255.255.0
CARCHI(config-router)#network 192.168.7.0 mask 255.255.255.0
CARCHI(config-router)#network 192.168.8.0 mask 255.255.255.0
CARCHI(config-router)#network 192.168.9.0 mask 255.255.255.0
CARCHI(config-router)#network 192.168.10.0 mask 255.255.255.0
CARCHI(config-router)#network 192.168.11.0 mask 255.255.255.0
CARCHI(config-router)#network 192.168.12.0 mask 255.255.255.0
CARCHI(config-router)#network 192.168.13.0 mask 255.255.255.0
CARCHI(config-router)#network 192.168.14.0 mask 255.255.255.0
CARCHI(config-router)#network 192.168.15.0 mask 255.255.255.0

Al momento de configurar el *router* Perú, se mostrará un mensaje que manifieste el establecimiento de comunicaciones entre los dos *router*s, tal como en la siguiente configuración:
PERU(config)#*router* bgp 200
PERU(config-*router*)#neighbor 192.168.0.17 remote-as 100
PERU(config-*router*)#%BGP-5-ADJCHANGE: neighbor 192.168.0.17 Up

PERU(config-*router*)#network 192.168.16.0 mask 255.255.255.0
PERU(config-*router*)#network 192.168.17.0 mask 255.255.255.0
PERU(config-*router*)#network 192.168.18.0 mask 255.255.255.0

10.6 Resultados de aprendizaje

- Solucionar el requerimiento técnico de un cliente, cumpliendo con sus bases técnicas y dimensionando el equipamiento activo necesario para la implementación de una red tomando en cuenta que las especificaciones dadas son el mínimo sugerido.
- Identificar el tipo de enrutamiento adecuado con el cual encaminar los paquetes.
- Emplear el protocolo BGP para intercomunicar sistemas autónomos.
- Distinguir entre un protocolo IGP y EGP.

10.7 Conclusiones

- Para intercomunicar redes con diferentes políticas de enrutamiento, es necesaria la configuración de BGP.
- Hay casos en los que para realizar una implementación, se debe cumplir con el requerimiento de un cliente.
- Es importante respaldarse en información técnica provista por el fabricante de los equipos, que justifique el cumplimiento con las bases técnicas.
- El método de enrutamiento que se implemente en una red debe considerar el ancho de banda de los enlaces para que no se saturen con los paquetes propios de un protocolo IGP, como es el caso del protocolo OSPF que requiere de mayor ancho de banda en comparación respecto a RIP y el que menor ancho de banda requiere serían las rutas estáticas. La elección debe ser considerada también de acuerdo al requerimiento del cliente en caso que para las configuraciones se especifique un protocolo dinámico o estático, sus diferencias en tiempo de administración y facilidad en la escalabilidad para el crecimiento de la red.

10.8 Tiempo estimado de la práctica

Dos sesiones de clase.

10.9 Evaluación/ cuestionario

1. ¿Qué método de enrutamiento uso para la red interna y por qué?
2. ¿Al momento de llenar bases técnicas, se puede proponer equipamiento de características menores a las pedidas?

Conclusiones y recomendaciones

11.1 Conclusiones

Cada laboratorio forma parte del entendimiento necesario para comunicar redes distintas, lo cual conlleva varios aspectos, tales como dimensionamiento del equipamiento a usarse y configuraciones.

En la implementación de una topología intervienen equipos activos de diferentes capas del modelo OSI los cuales necesitan tener capacidades adecuadas para el funcionamiento de la red, tales como la versión del software de los equipos activos y de ser el caso, los módulos que se le puedan añadir o los puertos con los que ya cuenten los dispositivos de red.

Las prácticas presentes en este documento tratan de dar un enfoque básico de una implementación real, en la cual interviene el requerimiento de un cliente y la topología que se quiere construir o extender según el caso.

El protocolo de red que se use depende de la cantidad de *routers* que contenga la red. Se debe considerar que el tráfico que el protocolo de enrutamiento puede afectar al rendimiento de la red, por lo cual en redes pequeñas lo más recomendable es el uso de rutas estáticas.

El simulador *Packet Tracer* es una herramienta útil para el aprendizaje de la forma como se arman topologías y configuran redes.

11.2 Recomendaciones

Analizar los resultados de una configuración realizada, mediante la simulación de envío de paquetes que ofrece *Packet Tracer.* Esta también puede ser una forma de saber en dónde se pierde un paquete en caso que exista alguna

configuración errónea o faltante y de esta manera tener una base de experiencias que se pueden aplicar en una implementación.

Cabe señalar que en una implementación real, la mayoría de veces habrá un requerimiento de un cliente, el cual tendrá que ser el punto de partida básico para la implementación, siendo posible superar las especificaciones requeridas por el cliente, pero nunca lo contrario.

Con el fin de aprovechar las características del simulador *Packet Tracer* y si el estudiante lo cree necesario, capacitarse en las características del software mencionado.

Revisar con anticipación cada práctica antes de clases para agilizar y entender el procedimiento que se va a realizar.

Referencias

Cisco. (2006). *Understanding and Tuning Spanning Tree Protocol Timers*. Recuperado de http://www.cisco.com/c/en/us/support/docs/lan-*switch*ing/spanning-tree-protocol/19120-122.pdf

Cisco. (2012). *Cisco IOS Software Configuration Guide Release 12.2(33)SXH and later releases*. California, Estados Unidos: Cisco Press.

Clark, M. (2003). *Data Networks, IP and the Internet.* West Sussex, Inglaterra: Wiley.

Collado, E. (2009). *Fundamentos de routing*. Recuperado de https://books.google.com.ec/books?id=zfaN9k840xsC&pg=PA20&dq=rutas+est%C3%A1ticas&hl=es-419&sa=X&ei=zrioVIXCAcOVNuqbgZgH&ved=0CCUQ6AEwAg#v=onepage&q=rutas%20est%C3%A1ticas&f=false

Donabue, G., A. (2011). *Network warrior*. (2ª Ed.). California, Estados Unidos: O'Reilly Media Inc.

Duarte, E. (2013). *Cisco CCNA – Todo sobre IPv6 – Espacio de direccionamiento*. Recuperado el 10 de enero de 2015 de http://blog.capacityacademy.com/2013/04/13/cisco-ccna-todo-sobre-ipv6-espacio-de-direccionamiento/

Gerometta O. (2007). *Administración de tráfico de broadcast excesivo con switches Cisco*. Recuperado el 20 de diciembre de 2014 de http://librosnetworking.blogspot.com/2007/03/administracin-de-trfico-de-broadcast.html

Gil, P., Pomares, J. y Candelas, F. (2010). *Redes y transmisión de datos*. Alicante, España: Publicaciones de la Universidad de Alicante.

Hagen, S. (2014). *IPv6 Essentials.* California, Estados Unidos: O'Reilly Media Inc.

Held, G. (2003). *The ABCs of TCP/IP*. Florida, Estados Unidos: CRC Press LLC.

Hogg, S. (2013). *OSPFv3 for IPv4 and IPv6*. Recuperado el 14 de febrero de 2015 de http://www.networkworld.com/article/2225270/cisco-subnet/ospfv3-for-ipv4-and-ipv6.html

Kennedy, C. y Hamilton, K. (2001). *Cisco LAN switching.* Indianápolis, Estados Unidos: Cisco Press.

Kioskea. (2014). *Equipos de red – El conmutador.* Recuperado el 27 de diciembre de 2014 de http://es.kioskea.net/contents/pdf/291-equipos-de-red-el-conmutador

Kioskea. (2014). *Equipos de red – Router.* Recuperado el 27 de diciembre de 2014 de http://static.ccm2.net/es.kioskea.net/contents/pdf/equipos-de-red-*router*-299-k8u3gh.pdf

Lammle, T. (2007). *CCNA Cisco Certifier Network Associate Study Guide*. Indianapolis, Estados Unidos: Wiley Publishing Inc.

Martínez, G. (2011). *Puentes Raíz*. Recuperado el 1 de enero de 2014 de http://siistemasgeral.blogspot.com/2011/02/puentes-raiz.html

Milla, R. (s.f.). *El protocolo IPv6 (I)*. Recuperado el 10 de enero de 2015 de http://www.ramonmillan.com/tutoriales/ipv6_parte1.php

Moy, J. (2004). *OSPF Anatomy of an Internet Routing Protocol*. Indianapolis, Estados Unidos: Pearson Education Corporate Sales Division.

Mun, Y. y Lee, H. (2005). *Understanding IPv6*. New York, Estados Unidos: Springer Science+Business Media Inc.

Ochoa Correa, V. A. (2010). Uso del packet tracer y aplicaciones resueltas. Recuperado el 20 de diciembre de 2014 de http://vochoa84.files.wordpress.com/2010/08/tutorial-uso-packet-tracer-y-aplicaciones-resueltas-corpocides.pdf

Odom, W. (2004). *CCNA ICND Exam Certification Guide.* Indianapolis, Estados Unidos: Cisco Press.

Rueda, G. (2001). *Técnico en redes y comunicaciones para computadores*. Bogotá, Colombia: Comercializadora editorial y sistemas Ltda.

Tanenbaum, A. (2003). *Redes de computadoras*. (4ª Ed.). Naucalpan de Juárez,
México: Pearson Educación.

Valencia, F. (2011). *Manual básico de configuración de redes Cisco*. Recuperado de https://books.google.com.ec/books?id=0gpdAgAAQBAJ&pg=PA52&dq=vtp&hl=es-419&sa=X&ei=snudVMPTG4axggTK7oLwDA&ved=0CBsQ6AEwAA#v=onepage&q=vtp&f=false

Wikipedia. (2014). *Host*. Recuperado el 27 de diciembre de 2014 de http://es.wikipedia.org/wiki/Host

ANEXOS

Anexo 1

Configuraciones del segundo ejercicio del laboratorio 7.

R1#sh run

```
Building configuration...
Current configuration : 718 bytes
!
version 12.4
!
hostname R1
!
no ip domain-lookup
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 192.168.0.117 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 192.168.0.113 255.255.255.252
 clock rate 64000
```

```
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.0.0
!
ip classless
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
End
```

R2#sh run

```
Building configuration...
Current configuration : 677 bytes
!
version 12.4
!
hostname R2
!
interface FastEthernet0/0
 ip address 192.168.0.1 255.255.255.192
 duplex auto
```

```
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 192.168.0.118 255.255.255.252
!
interface Serial0/0/1
 ip address 192.168.0.121 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.0.0
!
ip classless
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
End
```

R3#sh run

```
Building configuration...
Current configuration : 714 bytes
!
version 12.4
!
hostname R3
!
interface FastEthernet0/0
 ip address 192.168.0.65 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 192.168.0.122 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 192.168.0.125 255.255.255.252
 clock rate 64000
!
interface Vlan1
 no ip address
 shutdown
```

```
!
router rip
 version 2
 network 192.168.0.0
!
ip classless
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
End
```

R4#sh run

```
Building configuration...
Current configuration : 678 bytes
!
version 12.4
!
hostname R4
!
interface FastEthernet0/0
 ip address 192.168.0.97 255.255.255.240
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
```

```
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 192.168.0.114 255.255.255.252
!
interface Serial0/0/1
 ip address 192.168.0.126 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.0.0
!
ip classless
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
End
```