



UNIVERSIDAD AUTONOMA DE CHIHUAHUA FACULTAD DE INGENIERÍA

enero-junio 2023

GUIA DE LABORATORIO #1
Nombre de la Practica: **Sistemas Numéricos**
Lugar de Ejecución: **Lab de Redes**
Tiempo Estimado: **2 horas y 30 minutos**
MATERIA: **Redes**

I. OBJETIVOS

- Identificar los diferentes sistemas numéricos a utilizar en la programación de dispositivos de redes locales.
- Realizar conversiones entre los diferentes sistemas (decimal-binario y viceversa, decimal hexadecimal y viceversa, hexadecimal-binario y viceversa).

II. INTRODUCCION TEORICA

Números utilizados en Electrónica Digital

Los sistemas de numeración (SN) utilizados en electrónica digital son los siguientes: sistema decimal, sistema binario, sistema octal y sistema hexadecimal.

1- SISTEMA DECIMAL

Este sistema consta de diez símbolos que van desde el numero 0 hasta el número 9, los cuales le dan la característica principal a este sistema conocido por todo el mundo.

Estos símbolos numéricos también forman unidades numéricas compuestas, al tomarlos como exponentes de un número que se encargará de regular el procedimiento, este número es llamado base. El numero base va a ser 10, por tal motivo también es conocido como "sistema de numeración en base 10".

2- SISTEMAS DE NÚMEROS BINARIOS

Este es el sistema numérico que utilizan los sistemas digitales para contar y es el código al que traduce todas las informaciones que recibe. Se dice "Binario" a todo aquello que tiene dos partes, dos aspectos, etc.

Muchas cosas en los sistemas digitales son binarias: Los impulsos eléctricos que circulan en los circuitos son de baja o de alta tensión, los interruptores están encendidos o apagados, abiertos o cerrados, etc.

A diferencia del sistema decimal al que estamos habituados, y que utiliza diez cifras, del 0 al 9, el sistema numérico binario utiliza solo dos cifras, el 0 y el 1. En el sistema binario las columnas no representan la unidad, la decena, la centena, como en el sistema decimal, sino la unidad (2^0), el doble (2^1), el cuádruple (2^2), etc. De modo que al sumar en la misma columna 1 y 1, dará como resultado 0, llevándonos 1 a la columna inmediatamente a la izquierda.

Para los sistemas digitales es fácil implementar el sistema binario, hasta el punto de que reduce todas las operaciones a sumas y restas de números binarios.

Imagen 1.1: Sistema binario y orden posicional de sus dígitos



Figura 1: Sistema binario



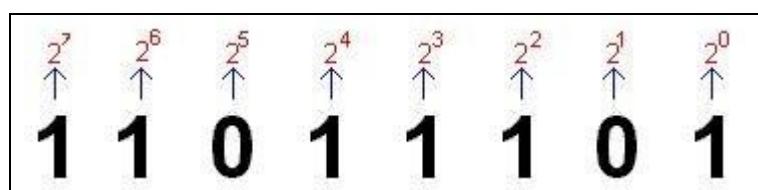
Figura 2: Números binarios

También las palabras, los números y los dibujos se traducen en el ordenador en secuencias de 1 y 0. De hecho toda letra, cifra o símbolo gráfico es codificado en una secuencia de 0 y 1. Si, por ejemplo, nuestro nombre tiene cinco letras, la representación para el ordenador constará de cinco bytes. La palabra bit deriva de las dos palabras inglesas "binary digit" cifra binaria, y designa a las dos cifras 0 y 1, que se utilizan en el sistema binario. Un bit es también, la porción más pequeña de información representable mediante un número, e indica si una cosa es verdadera o falsa, alta o baja, negra o blanca, etc.

Un byte es generalmente una secuencia de 8 bits. Ocho ceros y unos se pueden ordenar de 256 maneras diferentes ya que cada bit tiene un valor de posición diferente.

El bit número 1 le corresponderá un valor de posición de $2^0(1)$, el siguiente bit tendrá un valor de $2^1(2)$, el siguiente $2^2(4)$, el siguiente $2^3(8)$ y así sucesivamente hasta llegar la última posición, o último bit, en este caso el número 8, que también es llamado el **MSB (Bit Más Significativo)** y el **LSB (Bit Menos Significativo)** correspondiente a la primera posición o bit número 1. Observe un ejemplo de aplicación en la Imagen 1.2:

Imagen 1.2: Valores de las posiciones de los números binarios



3- SISTEMA DE NUMERACIÓN HEXADECIMAL

Este sistema consta de 16 símbolos donde desde el 0 hasta el 9 son números y del 10 hasta el 15 son letras, las cuales se encuentran distribuidas tal como se muestra en la Imagen 1.3.

La ventaja principal de este sistema de numeración es que se utiliza para convertir directamente números binarios de 4 bits, en donde un solo dígito hexadecimal puede representar 4 números binarios o también 4 bits.

Imagen 1.3: Símbolos utilizados en el sistema de numeración hexadecimal

Hexadecimal	Decimal	Hexadecimal	Decimal
0	0	8	8
1	1	9	9
2	2	A	10
3	3	B	11
4	4	C	12
5	5	D	13
6	6	E	14
7	7	F	15

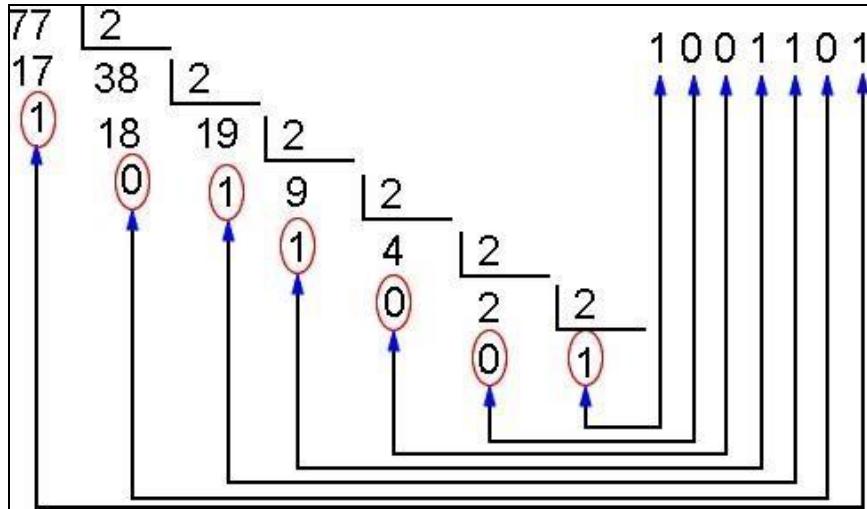
Conversión entre sistemas numéricos diferentes

Conversión de Decimal a Binario

Para hacer la conversión de decimal a binario, hay que ir dividiendo el número decimal entre dos y anotar en una columna a la derecha el resto. La lista de ceros y unos leídos de abajo a arriba es el resultado.

Ejemplo: Convertir 77(dec) a binario.

Imagen 1.4: Ejemplo de conversión de 77 decimal a binario



Conversión de Binario a Decimal

Para convertir las cifras que componen el número binario a decimal, cada uno de los dígitos se multiplican por las potencias de dos iniciado con la potencia de 0, es decir ($2^0, 2^1, 2^2, 2^3 \dots$ etc.), comenzando por el **LSB**, observa la Imagen 1.5

Imagen 1.5: Lista y posiciones de potencias de 2

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Ejemplo: Convertir 11001011 (bin) a decimal.

7	6	5	4	3	2	1	0	exponentes
1	1	0	0	1	0	1	1	

$$1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 128 + 64 + 8 + 2 + 1 = 203$$

Conversión de Hexadecimal a Binario

Para las conversiones de Hexadecimal a Binario y viceversa, se podrá hacer uso de la tabla de equivalencias descrita en la imagen 1.6.

Imagen 1.6: equivalencias entre SN binario y hexadecimal

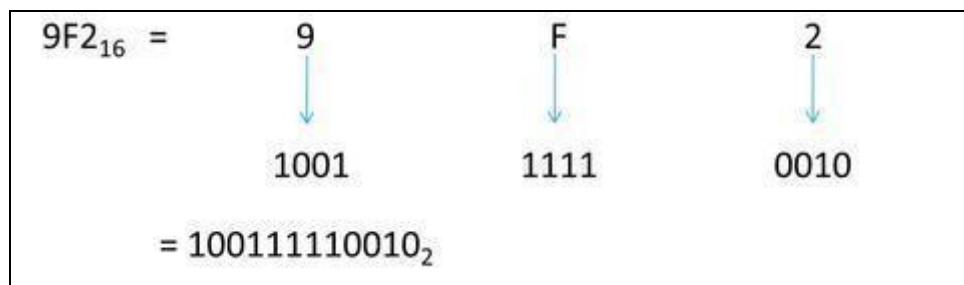
Binario	Hexadecimal	Binario	Hexadecimal
0000	0	1000	8
0001	1	1001	9
0010	2	1010	A
0011	3	1011	B
0100	4	1100	C
0101	5	1101	D
0110	6	1110	E
0111	7	1111	F

La conversión se obtiene al reemplazar cada cifra hexadecimal por su equivalente binario (formado de 4 bits) indicado en la Tabla 3.

A esta agrupación de 4 bits se le denomina **Nibble**, por lo que un byte en hexadecimal se compone de 2 nibbles.

Ejemplo: Convertir 9F2 (Hex) a binario:

Imagen 1.7: Conversión de numero hexadecimal a binario



Conversión de Binario a Hexadecimal

Para realizar las conversiones entre estos dos sistemas, se inicia agrupando a la secuencia binaria por nibbles (4 bits), comenzando por el LSB. Luego reemplaza cada nibble por su cifra hexadecimal correspondiente, haciendo uso de la Tabla 3. Ejemplo: Convertir 1110100110 (bin) a hexadecimal.

Imagen 1.8: Conversión de SN binario a Hexadecimal, por agrupación de bits

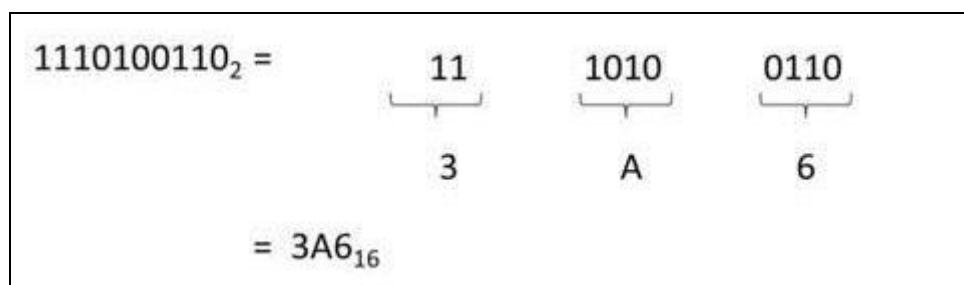


Tabla de referencia entre los tres sistemas numéricos

Existe una tabla (ver imagen 1.9) que muestra de manera general algún tipo de conversión rápida entre los 3 sistemas numéricos y contribuye a realizar dichos procesos.

Imagen 1.9: Tabla de equivalencias entre los sistemas más utilizados

Decimal	Binario	Hexadecimal	Octal	Decimal	Binario	Hexadecimal	Octal
0	0000	0	0	8	1000	8	10
1	0001	1	1	9	1001	9	11
2	0010	2	2	10	1010	A	12
3	0011	3	3	11	1011	B	13
4	0100	4	4	12	1100	C	14
5	0101	5	5	13	1101	D	15
6	0110	6	6	14	1110	E	16
7	0111	7	7	15	1111	F	17

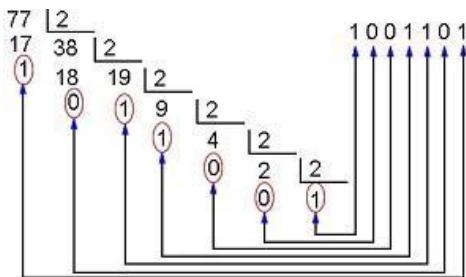
Redacción de cálculos de conversión del SN decimal a otro SN diferente

La redacción de las divisiones sucesivas requeridas para convertir un numero decimal a otro diferente, se puede facilitar si se elaboran en forma de una tabla, en la cual se resalten 2 resultados (cociente y residuo sucesivos) de las divisiones entre la nueva base del SN a convertir.

Analice los ejemplos descritos en las imágenes 1.10 y 1.11.

Ejemplo 1: Convertir 77(dec) a binario

Imagen 1.10: Redacción de cálculos para una conversión decimal-binaria



Método de conversión

Redacción de la conversión en forma de tabla

Numero	Cociente (entre 2)	Residuo
77	38	1
38	19	0
19	9	1
9	4	1
4	2	0
2	1	0
1	0	1

Resultado: Número en binario: **1001101**

Ejemplo 2: Convertir 110714 (dec) a hexadecimal (base 16)

Imagen 1.11: Redacción de conversión decimal-hexadecimal

Numero	Cociente (entre 16)	Residuo
110714	6919	10 (A)
6919	432	7
432	27	0
27	1	11 (B)
1	0	1

Resultado: Número 110714 en su formato hexadecimal es **1B07A hex**

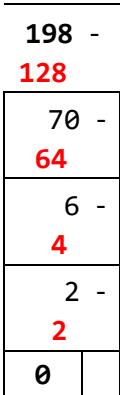
Conversión de un byte (en Decimal) a binario sugerida por Academia CISCO

Se le conoce como método de “resta sucesiva de potencias de 2” y consiste en restar al número a convertir la máxima potencia de 2 que puede contener. Al resultado se le resta la siguiente máxima potencia de 2 que aun contiene y así sucesivamente hasta que el resultado sea cero.

Tome en cuenta que debe recordar las potencias de 2:

2⁷	2⁶	2⁵	2⁴	2³	2²	2¹	2⁰
128	64	32	16	8	4	2	1

Luego, cada posición de las potencias de 2 que fue utilizada en las restas sucesivas se reemplaza por un bit (1) y se coloca bits (0) en el resto. Observe el siguiente ejemplo: Ejemplo: Convertir el byte 198 al sistema binario:

Paso 1: Resta sucesiva de potencias de 2: 	Paso 1 (en forma de tabla horizontal) Redacción equivalente de la misma resta de potencias de 2: <table border="1" data-bbox="845 475 1340 623"> <thead> <tr> <th>Numero</th><th>198</th><th>70</th><th>6</th><th>2</th></tr> </thead> <tbody> <tr> <td>Potencia 2</td><td>128 -</td><td>64 -</td><td>4 -</td><td>2 -</td></tr> <tr> <td>resta</td><td>70</td><td>6</td><td>2</td><td>0</td></tr> </tbody> </table>	Numero	198	70	6	2	Potencia 2	128 -	64 -	4 -	2 -	resta	70	6	2	0
Numero	198	70	6	2												
Potencia 2	128 -	64 -	4 -	2 -												
resta	70	6	2	0												

Paso 2: Redacción del Byte en binario:

1	1	0	0	0	1	1	0
128	64	32	16	8	4	2	1

Byte final (en binario) de 198 es **11000110(bin)**

III. MATERIALES Y EQUIPO

Para la realización de la guía de práctica se requerirá lo siguiente:

No.	Requerimientos	Cantidad
1	Guía de Laboratorio #1 de REC404	1
1	Calculadora básica	1

IV. PROCEDIMIENTO

1. En grupos de 2 o 3 integrantes, proceda a crear un documento de hoja de cálculo denominado REC_CARNET1_CARNET2_CARNET3.
2. En este archivo, proceda a desarrollar cada uno de los siguientes ejercicios, desarrollando cada parte en una hoja de cálculo diferente (nombrada como Parte 1, Parte 2, Parte 3...).

Utilice el método solicitado en cada parte. Resalte la respuesta y otros elementos del cálculo que crea necesario para demostrar la aplicación del método solicitado.

3. Una vez finalizada la hoja de cálculo con la resolución de los ejercicios, proceda a entregar el archivo a su instructor.

Ejercicios a resolver

PARTE I: CONVERSION DECIMAL A BINARIO

Redacte los cálculos de conversión en forma de tabla (ver Figura 7 de la introducción teórica).

a) 62	d) 436
b) 363	e) 153
c) 976	f) 547

PARTE II: CONVERSION DE BINARIO A DECIMAL

Para facilitar la conversión, debe convertir la secuencia binaria a hexadecimal y luego esta última en el valor decimal equivalente.

a) 10110	c) 1001101010001	e) 101011010
b) 111011	d) 110110011101	

PARTE III: CONVERSION HEXADECIMAL A BINARIO

1B2	EC1
16F8	DA5

PARTE IV: CONVERSION DE UN BYTE (DECIMAL) EN FORMATO BINARIO

En cada conversión, debe utilizar el método de restas sucesivas de potencias de 2.

(*) Para solucionar el ejercicio con este método, debe extender la tabla inicial de potencias de 2

32	185
293	2074 (*)
126	536 (*)

PARTE V: CONVERSION ENTRE SN HEXADECIMAL Y SN OCTAL

Investigue las reglas de escritura y valores posicionales de un número en el sistema numérico octal, así como el método usado para convertir un número binario en este sistema octal y viceversa.

Aplique su investigación, realizando las siguientes conversiones numéricas.

Tome en cuenta que en ningún momento debe utilizar conversiones al sistema decimal, pero si puede utilizar cualquier otro SN diferente para ejecutar la tarea.

13C hexadecimal al SN octal
615 octal a hexadecimal

1037 octal al SN hexadecimal

BACD hexadecimal al SN octal



UNIVERSIDAD AUTONOMA DE CHIHUAHUA FACULTAD DE INGENIERÍA

enero-junio 2023	GUIA DE LABORATORIO #2 Nombre de la Practica: Simulador Cisco Packet Tracer Lugar de Ejecución: Laboratorio de Redes Tiempo Estimado: 2 horas y 30 minutos MATERIA: Redes
------------------	---

I. OBJETIVOS

Al finalizar esta práctica, el estudiante podrá:

- Utilizar el entorno general de diseño de topologías de red y simulaciones bajo la aplicación Cisco Packet Tracer
- Seleccionar los dispositivos de red del cuadro de herramientas brindados en el entorno Lógico del simulador
- Realizar el cambio en las interfaces físicas utilizadas por los dispositivos de red configurables (switch, routers)

II. INTRODUCCION TEORICA

¿Qué es un simulador de red?

Es un software que permite reproducir tanto las sensaciones físicas (velocidad, aceleración, percepción del entorno) como el comportamiento lógico de las máquinas y dispositivos de red que conforman a una topología de red.

Estas aplicaciones permiten desde una interface gráfica, seleccionar diferentes periféricos e interconectarlos. Puede configurar a cada equipo (asignando IP, mascara, ip de punto de enlace, etc.) y/o modificar sus características como por ej.: cambiar el tipo de tarjetas de red (fibra óptica, Ethernet, inalámbrica, etc.), con sus respectivos parámetros de funcionamiento (velocidad, seguridad, direccionamiento, etc.).

Finalmente, puede realizar diferentes pruebas virtuales de la compatibilidad, funcionamiento y rendimiento de la topología de red.

Simulador de Redes Cisco Packet Tracer

Cisco Packet Tracer un software de simulación de Redes con entorno de aprendizaje, para que los diseñadores de redes puedan elaborar planos, vistas, configuraciones de protocolos y animaciones de sus Redes.

1 / 12

Después, los estudiantes pueden desarrollar pruebas (simulaciones) de funcionamiento.

Las simulaciones dan soporte a los protocolos mas utilizados, entre ellos::

- Internet Protocol versión 6 (IPv6)
- Modelos mejorados de Linksys, algoritmo WEP, mejoras en Cable y DSL
- Call Manager Express (soporte de VOIP)
- Servidores FTP en enrutadores y switches
- Sistema de Email (SMTP y POP3), cliente y servidor.
- Implementación limitada de Border Gateway Protocol (BGP)



Espacio de trabajo básico de Packet Tracer

Packet Tracer utiliza 2 esquemas de representaciones para implementar la simulación de su red:

- a) Espacio de trabajo lógico (**Logical**): Es donde usted construye la topología lógica de su red, sin tener en cuenta la escala física y limitaciones de construcciones
- b) Espacio de trabajo físico (**Physical**): modifica el arreglo de sus dispositivos físicos en el local, edificio, ciudad, etc. Debe tener en cuenta que las distancias/longitudes de cables y ubicaciones de dispositivos afectaran su diseño de red en el simulador (al igual que lo haría en la realidad).

En Packet Tracer, debe diseñar primero la topología lógica de la red y luego desarrollar el Espacio de trabajo físico respectivo.

Espacio de trabajo Lógico (Logical)

Es el entorno inicial de trabajo que muestra la simulación al iniciarla.

El área de trabajo lógico (ver la imagen 2.1), permite colocar cada uno de los dispositivos de red, para luego interconectarlos con el medio físico apropiado, de acuerdo a las topologías lógicas a implementar en el diseño de la red.

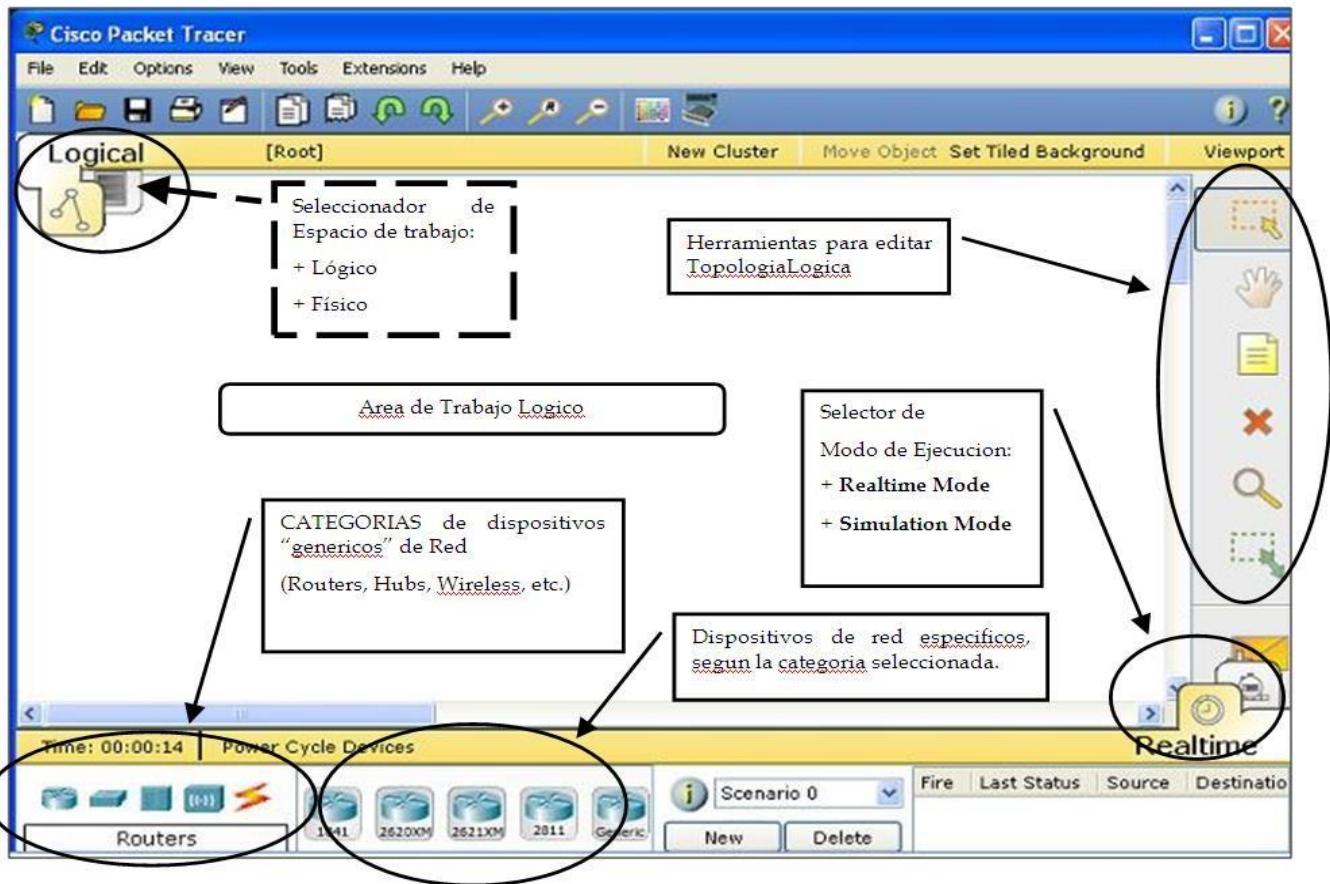
Las operaciones más importantes en este entorno Lógico ofrecido por Packet Tracer son las siguientes:

Selección y ubicación de los dispositivos de red

Para iniciar a construir una topología de red, se debe realizar lo siguiente:

1. Seleccionar de las herramientas de categorías y modelos al primer dispositivo requerido de su diseño de red. Ejemplos:
 - a) Para colocar una PC host:, dar clic en Categoría *End Device* y luego PC-PT
 - b) Para colocar un dispositivo repetidor: Categoría: Hubs y dispositivo Repeater-PT
2. Desplazar el cursor hasta la posición final en el área de trabajo lógico donde se colocara dispositivo y dar un clic. Se mostrara una imagen, la cual representa una copia del dispositivo seleccionado.
3. Repetir los pasos anteriores hasta colocar el resto de dispositivos de la topología a simular.

Imagen 2.1: Pantalla principal del software Cisco Packet Tracer.



MODOS DE OPERACIÓN del Espacio de Trabajo lógico

Los modos de operación (Operating Modes) de Packet Tracer reflejan el funcionamiento del esquema de red, los cuales pueden ser:

a) Modo tiempo real (**Realtime Mode**):

El simulador ejecuta su topología en tiempo real, limitando los protocolos a probar. La red responde a sus acciones inmediatamente, como lo haría un medio (device) de red en el momento que ocurra un suceso en la red.

b) Modo de Simulación (**Simulation Mode**):

El creador de la topología puede evaluar los tipos, tiempos y secuencias de PDU's generados en diversos "escenarios de prueba". Puede ver a su red, ya sea paso a paso o sino, evento por evento.

Espacio de trabajo físico (Physical)

El área de trabajo lógico permite colocar cada uno de los dispositivos de red, para luego interconectarlos con el medio físico apropiado, de acuerdo a las topologías lógicas que requiere el diseño de la red.

El espacio de trabajo físico permite dar las dimensiones físicas al diseño de la red. Usted define una escala y lugar (como su red se vería en un entorno real) para cada dispositivo utilizado en su diseño lógico de la red(es).

Analiza la colocación y distribución de todos los dispositivos de la red en un “área física de trabajo”, para así evaluar: calidad/marca de los dispositivos seleccionados, eficiencia, problemas de cobertura, etc., los cuales no se observan en el diseño lógico de la red.

Cambio en los puertos de conexión de un dispositivo de red

Se debe determinar la NIC apropiada para cada

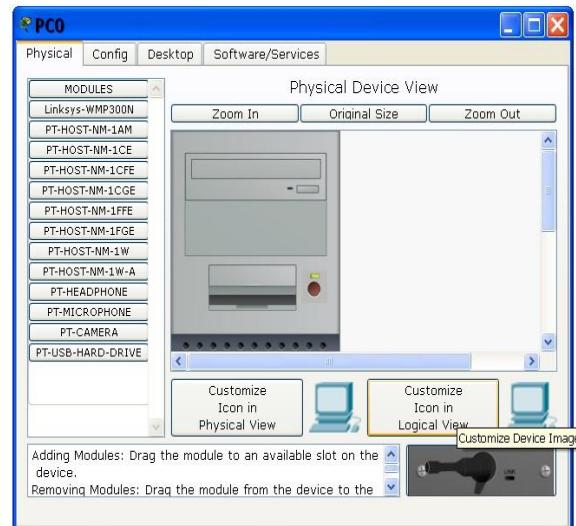
Imagen 2.2: Lista de Módulos para una PC-PT dispositivo a interconectar.

Packet Tracer consta de una serie de Módulos para definir la NIC a usar en un dispositivo. Por ejemplo, al dar un clic a un dispositivo PC-PT, se muestra (ver Imagen 2.2) el modulo instalado y los módulos disponibles se muestran en la columna izquierda.

Dando clic en los botones Zoom Out o Zoom In, se puede alejar/acercar la vista actual del dispositivo.

Para determinar el modulo instalado, colocar el cursor sobre la imagen de la NIC.

Las opciones para configuración de la NIC instalada y del resto del dispositivo, puede ser modificado con las fichas superiores (Config y Desktop).



Para cambiar el módulo de conexión del dispositivo:

1. Se localiza botón de encendido/apagado, que puede tomar la forma de un botón color verde (indica encendido) o un botón (1-0) (si es 1, está funcionando).
2. Da clic en el botón para apagar al dispositivo
3. Desconecta el modulo actual, arrastrando la imagen de su módulo ya instalada hacia la lista de módulos disponibles a la izquierda. Y si es necesario, se puede cambiar por otro modulo, seleccionando y arrastrando el módulo de la lista de módulos hacia la posición en el dispositivo.
4. Una vez instalado el módulo NIC apropiado, active nuevamente el botón de encendido.

Configuración de los parámetros de red

Para los dispositivos que requieran la configuración del protocolo IP, debe ejecutar los siguientes pasos:

1. De clic en el dispositivo a configurar y selecciona la ficha Escritorio (ver imagen 2.3). De las múltiples opciones, selecciona **IP Configuration**.
2. Ingresar el trío de parámetros básicos:

IP host

máscara de red

IP Gateway (opcional. cuando lo requiera).

DNS Server (opcional. cuando lo requiera).

Se repite los pasos anteriores por cada dispositivo que requiera IP.

Imagen 2.3: Opciones de configuración para una PC



III. MATERIALES Y EQUIPO

Para la realización de la guía de práctica se requerirá lo siguiente:

No.	Requerimiento	Cantidad
1	Guía # 2 de Redes	1
2	PC con el software de simulación “Cisco Packet Tracer 6.0.1” o superior	1

IV. PROCEDIMIENTO

Parte 1: iniciando Cisco Packet Tracer

1. Active su PC y acceda a la aplicación *Cisco Packet Tracer* instalada ahí
2. Guarde su primer archivo de simulación con el nombre **Simu1deCARNET.pkz**

3. En la Figura 1 se detalla las partes principales de la interfaz general de Cisco Packet Tracer, identifique cada una de ellas en el simulador.

Como podrá observar, en la esquina inferior izquierda de la ventana, aparecen una serie de dispositivos en una forma general (dispositivos genéricos de red).

4. Seleccione un dispositivo de esta área (por Ej. a un Router). En la parte de “dispositivos específicos” (a la derecha) aparecerán los modelos de los equipos pertenecientes al grupo general Router (Ej.: 1841, 2620XM, Generic, etc.)

5. De estos dispositivos, seleccione un router **2620XM**. Observe que el cursor cambia de una flecha a un signo más (+) dentro del área de trabajo de la simulación.

6. Haga clic en alguna parte del área de trabajo. Se mostrara una imagen que representa a un Router 2620XM, con el nombre por defecto: **Router0**.

7. De clic sobre el Router0. Se abre una ventana para definir los aspectos físicos y de configuración del dispositivo de red.

De clic en cada una de las 3 fichas superiores para reconocer las opciones que se definen en cada una.

8. Cierre la ventana de configuración de Router0.



9. Elimine el Router0 anterior, utilizando el botón que se encuentra en la barra de acceso común y luego seleccione el dispositivo a eliminar. Presione la tecla Esc (escape).

De esta manera, puede agregar/eliminar cuantos dispositivos desee a su simulación.

Parte 2: Networking con 2 host's (Red Punto a Punto)

10. Procederá a crear la red LAN más simple que existe.

Seleccione la categoría general (End Device) y coloque 2 dispositivos genéricos (**PC-PT**) en el espacio de trabajo.

11. De clic sobre la PC0 y dentro de la ventana emergente, presione al botón *Zoom Out*, para ver el CPU completo.

Localice en la parte inferior de esta vista del CPU al tipo de Modulo de NIC (tarjeta de red) usado por esta PC, ubique el ratón sobre esta NIC y anótelo aquí: _____ Cierre la ventana de configuración de PC0.

12. Proceda a crear la conexión física entre las NIC Ethernet de ambas PC's. Con este objetivo, de clic sobre categoría genérica **Connections**  , para ubicar y dar clic en el botón del cable (**Copper Cross Over**)

13. Mueva el ratón sobre área de trabajo, vera que ha cambiado de forma.

De clic sobre la PC0. En este momento se muestran todas las interfaces de red disponibles. Seleccione a la FastEthernet.

14. Mueva el ratón y vera que al ratón le sigue una línea en todo momento. Esto se debe a que está esperando que se le indique la interfaz de otro dispositivo al cual conectara el extremo de este cable.

15. De clic sobre PC1 y seleccione FastEthernet. Se mostrara un “cable” que une a las 2 PC’s y tiene un punto de color “verde” en cada extremos del cable de enlace.

Cuando use el simulador, tome en cuenta que los 2 extremos de una conexión física pueden tener uno de estos colores en sus extremos:

- Verde: representan actividad y/o conexión física correcta y activa.
- Rojo: El tipo de cable elegido para los puertos seleccionados es incorrecto. O también, el puerto de conexión del dispositivo de red esta deshabilitada de manera administrativa.
- Naranja: algún protocolo del dispositivo de red está configurando su puerto de conexión para activarse segundos después.

16. Borre el cable cruzado entre ambos host, seleccionando al botón  y haciendo clic sobre el cable.

17. Elija el tipo de cable (**Copper Straight-Through**) y conecta la interface FastEthernet de ambas PC. En este caso, el color rojo en ambos extremos significa que este tipo de cable no es el apropiado para enlazar ambas PC a través de este tipo de puertos FastEthernet.

18. Borre la conexión incorrecta y restaure la conexión entre ambos host, utilizando el cable cruzado (**Copper Cross-Over**).

19. Coloque el puntero del ratón sobre la PC0 pero no haga clic.

Se desplegará un recuadro con un resumen de parámetros de configuración de la NIC.

Parte 3: Configuración de los parámetros IP de una NIC

20. Ahora proceda a definir la configuración de red (Protocolo IP) del 1er host (PC0).

Revise la introducción teórica de esta práctica para configurar a este host una dirección IP **192.168.0.2**, dejando la Máscara predeterminada que ofrece el simulador.

Asigne al otro host la IP **192.168.0.3**.

21. Pruebe si la comunicación entre ambos host se realiza, dando clic en una de ellas, luego ingresa a la ficha Desktop y finalmente da clic en ícono *Command Prompt*.

22. Digite al comando **ipconfig** y presione tecla *Enter*.

Luego redacte **ping laIPdelOtroHost**. Reemplace el parámetro *laIPdelOtroHost* por la ip del otro equipo hacia el que envía el saludo.

23. Confirme si recibe respuesta de cada paquete de prueba generado por el protocolo.

24. Repita los 3 pasos anteriores pero desde la otra Terminal, utilizando la ip del 1er host como destino.

25. Ejecute nuevamente ping, pero dirigido a una IP desconocida (no asignada), por ejemplo, a la 195.0.2.35 ¿Cuál fue la diferencia entre este último resultado y los 2 anteriores? Analice
26. Guarde los cambios de su archivo de simulación.

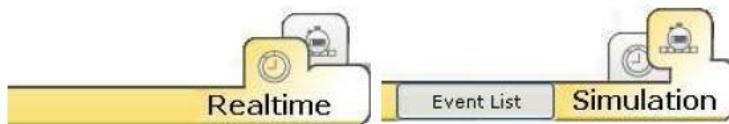
Parte 4: Uso de los Modos de Simulación de Packet tracer

MODO DE PRUEBA: Simulation

27. Cambie al modo de simulación

(**Simulation**) haciendo clic derecho **Imagen 2.3:** Botones para el cambio de Modo del en el cronometro que se encuentra Simulador. en la parte inferior derecha del área de trabajo lógica.

Observe la Imagen 2.3, aquí se visualiza el reloj (Realtime) y el cronometro (modo simulación).



Simulación del Concepto: Envío de tramas de bits.

28. Observe la figura 5. De clic en el botón **Add simple PDU** y con cuidado de clic en PC0 y luego en la PC1. Ha elegido que Terminal ORIGEN será PC0 y la Terminal DESTINO será PC1.

Vera que se agrega una fila en la tabla inferior derecha, con un evento que indica el estado y los nombres de PCorigen y la PCdestino.

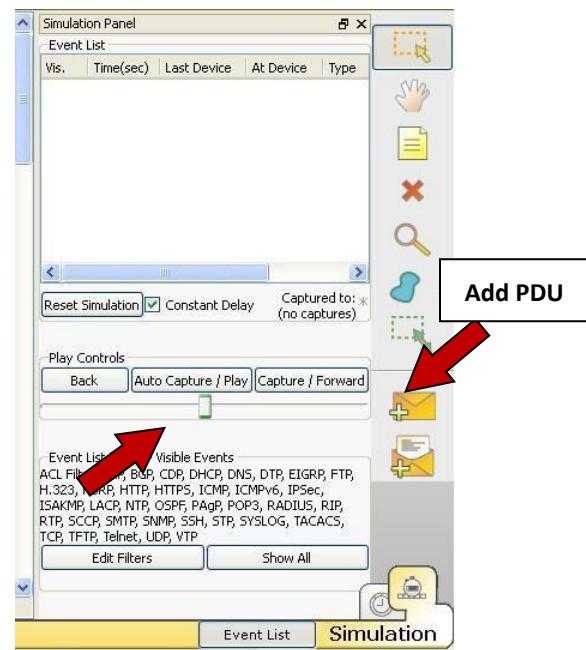
29. Se muestra la ventana *Lista de Eventos* (ver Imagen 2.4), que detalla el tipo y estado de ejecución de los PDU definidos para la Simulación a ejecutar.

Observe con mucho cuidado que: **Imagen 2.4:** Lista de eventos usados en Modo Simulación a) El color de la columna info coincide con el “Sobre PDU” colocado en el host

Origen del único evento hasta ahora

- b) El parámetro (constant Delay) está activado.
- c) Se posee una Lista de filtros (Lista de filtrado de eventos), con un listado de protocolos que la simulación del escenario puede generar.

30. Reduzca el tiempo de muestreo a un 10%, gracias a la barra debajo del botón **Auto Capture/Play** (que por defecto señala un 50% de la velocidad máxima de la simulación de eventos).



31. De un clic en el “Sobre” PDU ubicado en el equipo origen. Anote y analice la información mostrada aquí.

32. Presione el botón **Auto Capture/Play** para que Packet Tracer inicie las pruebas con su “evento” programado.

Observe que el “Sobre” (PDU formal) se desplaza (representando la comunicación de datos a través de un medio físico de red) desde el host origen hasta llegar al host destino.

33. Este atento a presionar el botón (Auto Capture /Play) antes que este Sobre llegue al equipo destino. La simulación es pausada. Observe el listado de eventos; se ha generado otro evento, pero vera que este evento tiene su destino (Last Device) y su origen (At Device) invertidos.

De clic en este nuevo Sobre que la PC destino ha generado. Ahora esta se convierte en el origen de este nuevo mensaje y lo dirige a la otra terminal que inicio la transmisión. Es una PDU de respuesta. Solicite a su docente una explicación sencilla de la ventana de detalle de la PDU!!

34. Cierre la ventana de información de la PDU a enviar y presione nuevamente botón (Auto Capture /Play) para continuar simulación del escenario y esté listo a pausarlo nuevamente cuando llegue a la PC que inicio la comunicación.

Se genera una señal en el Sobre, indicando que la solicitud de eco fue respondida por el otro equipo.

35. Retorne al modo de Tiempo Real (Realtime), guarde la simulación y cierre la simulación. Responda (Si) al cuadro de texto generado por el simulador.

Parte 5: Modificando la configuración física de un dispositivo de red

36. Prepare un nuevo archivo de simulación de red.

37. Agregue 2 router, de la serie 1841 y 2621XM, respectivamente. Coloque el ratón sobre cada dispositivo (sin dar clic) y observe la lista de puertos de conexión con lo que cuenta cada uno.
38. Lea la introducción teórica de esta práctica sobre la manera de cambiar los puertos de conexión de un dispositivo.

Luego, aplique estos pasos al router 1841 para modificarlo, agregando un módulo de conexión serial **WIC-2T**.

De igual forma, modifique el otro router.

39. Para la conexión de ambos router, utilizara un enlace/línea T1. Este tipo de cable requiere que cada dispositivo posea conectores seriales **WIC (WAN Interfaces Card)**, los cuales fueron agregados en el paso anterior.
40. Del listado de Conexiones, seleccione el tipo de cable (**Serial DCE**). Luego, conecte un puerto Serial del router 1841 con un puerto Serial del router 2621XM.

Observe que los extremos del cable serial están desactivados, porque es necesario configurar las interfaces en cada router para que la comunicación se establezca.

41. De clic en router 1841 y luego seleccione la ficha superior Config. Del listado de interfaces a la izquierda, ubique y de clic sobre el puerto Serial con el cual se conecta al otro router.

Observe el estado de funcionamiento de la interface (Port Status). Asigne la IP **10.0.0.1** y la máscara predeterminada **255.0.0.0** y active la interface (haga clic en opción **Activar/On**). Cierre la ventana de configuración del router.

42. Repita el paso anterior sobre el otro router para activar la interface Serial conectada con la ip **10.0.0.2**.

Los extremos del enlace se activaran.

43. Ingrese de nuevo al router 1841, seleccione la ficha superior CLI. Desde el cursor actual (Router>), digite el comando: **do ping 10.0.0.2**

Presione Enter y observe el resultado. Se generan 5 paquetes de saludo dirigidos por el puerto serial 0/1/1 a un host remoto que tenga asignada la ip 10.0.0.2.

Si la comunicación fue exitosa, obtendrá el siguiente mensaje:

```
.....
Success rate is 5 percent (5/5)
```

44. Envíe un ping a una ip no configurada en la topología (por ej. 10.0.0.26). Obtendrá una respuesta nula (0/5).

45. Incluya a una PC y a un Server-PT en el área de trabajo.

Utilice un cable cruzado para conectar el puerto FastEthernet de la PC al puerto FastEthernet 0/0 del Router0.

De igual manera, conecte el Server0 al puerto FastEthernet 0/1 del Router0.

46. Ahora proceda a configurar el protocolo IP de la PC0, Server0 y de las interfaces del Router0 con estos parámetros:

Configuración IP	PC0	Server0	Interface f0/0 de Router0	Interface f0/1 de Router0
IP	192.168.10.5	192.168.40.6	192.168.10.1	192.168.40.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.10.1	192.168.40.1		

Y finalmente active las interfaces modificadas en Router0

47. De clic en PC0. En la ventana de configuración, seleccione la ficha Desktop y de clic en botón Command Prompt. Haga la prueba de comunicación dirigido al Server0, digitando al comando: ping 192.168.40.6

Se generan 4 paquetes de prueba, de los cuales 1 se perderá y el resto obtendrán respuesta del Server0. Repita de nuevo el comando y se obtendrá respuesta completa del Server0.

48. Guarde la simulación y cierre el simulador. Muestre los resultados a su instructor.

V. ANALISIS DE RESULTADOS

Elaborar un nuevo archivo de simulación de red en "Packet Tracer. En esta simulación se debe desarrollar una topología de red que cumpla las siguientes políticas:

- Una red punto a punto formada por 2 router, conectados por medio de un cable de fibra óptica. El primer router se llamará **Cojute** y el otro enrutador **Morazan**.
- Red de área local conformada por 3 clientes, utilizando un Switch como dispositivo comutador. Utilice uno de sus puertos para conectarlo a uno de los puertos FastEthernet de Cojute.
- Una red local conformada por 2 servidores, la cual se conecta a una interface FastEthernet de Morazan.
- El esquema de direccionamiento ip a implementar será el siguiente:

Descripción de red	Ip de red	Mascara de subred	Ip Gateway
Red local de clientes	192.168.0.0	255.255.255.0	192.168.0.1
Red local de servidores	170.0.0.0	255.255.0.0	170.0.0.1
Red de Enlace entre router	10.0.0.0	255.0.0.0	

- Configure a los host y server con ip de la red de la cual formen parte.

- En router Cojute configure la interface de conexión a la red local de host con la ip Gateway correspondiente y luego, la interface de conexión de fibra con una ip de la red 10.0.0.0
- Ejecute un proceso similar en router Morazan, con las ip correspondientes a sus redes conectadas.

Ejecute pruebas de ping entre host de la red de cliente, entre ambos servers y por último, de un cliente hacia uno de los Server. Solamente funcionara la comunicación local interna. Los clientes no podrán comunicarse con los server.

Para comunicar un cliente con los server's, es necesario que el router Cojute publique las redes configuradas en sus interfaces al otro router y viceversa.

De clic en Cojute, luego en la ficha Config y del listado izquierdo elija la opción **RIP**. En el parámetro **Network** escriba la ip red de clientes y de clic en **Add**. Después agregue a la ip red de enlace entre ambos router.

De manera similar, repita el proceso de RIP en el otro router, pero agregue solo la ip red de servidores y de la red de enlace.

Ejecute nuevamente las pruebas de un cliente a un server. La comunicación será exitosa. Muestre la simulación final a su instructor para su respectiva evaluación.

VI. BIBLIOGRAFIA

- Cisco Systems/Networking Academy, (2011), Ayuda de software Cisco Packet Tracer, USA • Cisco Networking Academy, (2019), recuperado de: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html
- Técnicas de Configuración de Routers Cisco, Ernesto Ariganello, AlfaOmega- Ra-Ma 2008.

	UNIVERSIDAD AUTONOMA DE CHIHUAHUA FACULTAD DE INGENIERÍA
enero-junio 2023	<p style="text-align: center;">GUIA DE LABORATORIO #03</p> <p>Nombre de la Practica: Introducción al IOS Lugar de Ejecución: Laboratorio de Redes Tiempo Estimado: 2 horas y 30 minutos MATERIA: Redes</p>

I. OBJETIVOS

Que el estudiante:

- Implemente una topología lógica bajo la aplicación Cisco Packet Tracer.
- Conecte un dispositivo de red administrable a una PC utilizando un cable de consola.
- Acceda al IOS (Internetwork Operative System) de un dispositivo administrable de Cisco.
- Cree una sesión de consola con el IOS de un Switch, vía Hyperterminal.
- Realice una configuración básica de un dispositivo Switch Cisco administrable

II. INTRODUCCION TEORICA

INTRODUCCION AL (IOS) DE UN DISPOSITIVO DE RED

El sistema operativo Internetwork (IOS) de Cisco

Al igual que una computadora (PC), el hardware de un router o un switch no puede funcionar sin un sistema operativo.

El **sistema operativo Internetwork (IOS)** de Cisco es el software del sistema utilizado en los dispositivos administrables de Cisco, independientemente del tamaño o tipo de dispositivo. Se usa en routers, switches LAN, pequeños puntos de acceso inalámbricos, grandes routers con decenas de interfaces y muchos otros dispositivos.

Las operaciones realizadas por el IOS varían de acuerdo con los propósitos/funciones de los diferentes tipos de dispositivos de internetworking. Entre los servicios de red que el Cisco IOS provee a sus dispositivos están:

Seguridad y QoS de interfaces	Direccionamiento y Enrutamiento Manejo Calidad de servicios.
--	---

El archivo del IOS se encuentra en un área de memoria semipermanente llamada flash. La **memoria flash** provee almacenamiento no volátil, que hace que los contenidos de la memoria no se pierdan

cuando el dispositivo se apague, pero también se puedan modificar o sobrescribirse cuando sea necesario.

MODOS DE CONEXIÓN PARA LA ADMINISTRACIÓN DE LOS DISPOSITIVOS

Para establecer la conexión física entre PC del administrador y el dispositivo de red, existen varias formas de acceder al entorno de la CLI. Los métodos más comunes son:

- a) Consola
- b) Telnet o SSH

El método más común es conectar un equipo al puerto de Consola del dispositivo mediante el **método de Consola**. Este utiliza un **Cable de Consola**, para conectar la interfaz de un puerto serial EIA/TIA 232 disponible en la PC, con un conector DB-9 o RJ45 en el otro extremo, que es el que se conecta a un puerto de Consola (CONSOLE).

Conexión de administración vía Telnet y SSH

Otro de los métodos que sirve para acceder en forma remota a la sesión CLI es hacer vía telnet al dispositivo. A diferencia de la conexión de consola, las sesiones de Telnet requieren servicios de networking activos en el dispositivo de red. Este debe tener configurada por lo menos una interfaz activa con una dirección de Capa 3, por ej.: una dirección IPv4.

Los dispositivos Cisco IOS incluyen un proceso de servidor Telnet que se activa cuando se inicia el dispositivo. El IOS también contiene un cliente Telnet.

EMULADOR DE TERMINAL

Debido a que la mayoría de dispositivos de red administrables con IOS no tiene sus propias pantallas ni dispositivos de entrada (un teclado o ratón), el acceso para la configuración y administración de los mismos se realiza mediante una conexión lógica entre el dispositivo y una PC.

Para lograr esta conexión lógica, la PC debe contener un programa denominado emulador de terminal. Un **emulador de terminal** es un software que permite a una computadora acceder a las funciones de otro dispositivo, utilizando el teclado y pantalla de la PC.

El emulador genera una interfaz para el envío de comandos desde una PC hacia el dispositivo de red, así como, recibe y muestra los resultados de la ejecución de los mismos al Administrador de red.

Uno de los emuladores de terminal más utilizados bajo los SO Microsoft Windows es el **HyperTerminal**. Este programa puede encontrarse en el menú: *Todos los programas > Accesorios > Comunicaciones*. Ahí se selecciona HyperTerminal.

HyperTerminal solicita que para iniciar sesión remota con el dispositivo de red remoto, se confirma el número de puerto serial elegido y luego se configura el puerto. Un ejemplo de esta configuración es la siguiente>>>

Bits por segundo: 9600 bps
Bits de datos: 8
Paridad: Ninguna
Bits de parada: 1
Control de flujo: Ninguno

Si se realizan correctamente todas las configuraciones y conexiones de cables, podrá acceder al dispositivo al presionar la tecla Intro del teclado, desde la ventana del software emulador de terminal, mostrándose la **CLI**.

El Hyperterminal también lo incluye el Simulador de redes Cisco Packet Tracer en sus simulaciones de red.

INTERFAZ DE LÍNEA DE COMANDOS (CLI)

Accede a los servicios que proporciona el IOS, por medio de una serie de comandos, que invocan las diferentes funciones de administración del dispositivo. Las funciones accesibles a través de la CLI varían según la versión de IOS y el tipo de dispositivo.

Modos de configuración del IOS

Una vez se accede a la CLI, se consta de toda una serie de comandos clasificados por funciones. El Cisco IOS está diseñado como un sistema operativo modal. El término modal describe un sistema en el que hay distintos modos de operación, cada uno con su propio dominio de operación. La CLI utiliza una estructura jerárquica para diferenciar a los modos. Los modos de Cisco IOS para los switches y los routers son muy similares.

En orden jerárquico los modos principales, desde el más básico hasta el más especializado, son los siguientes:

- A. Modo de usuario (EXEC de usuario)
- B. Modo de ejecución privilegiado (EXEC privilegiado)
- C. Modo de configuración global
- D. Otros modos de configuración específicos

Cada modo consta de comandos orientados a realizar tareas determinadas, no disponibles en otro modo. Por ejemplo, el modo de configuración global permite configurar los parámetros generales del dispositivo, como la configuración del nombre de dispositivo.

Pero, se requiere un modo diferente para configurar los parámetros de seguridad en un puerto específico de un switch. En ese caso, debe ingresarse al modo específico de configuración de interfaz para ese puerto específico. Todas las configuraciones que se introducen en el modo de configuración de interfaz se aplican solamente a ese puerto.

Cada modo se distingue por una petición de entrada singular de línea de comandos que es exclusiva de ese modo denominado **Cursor**, tal como se muestra a continuación:

Modo	Cursor	Ejemplos de comandos disponibles
User EXEC	Nombredispositivo>	ping, enable, show
Privileged EXEC	Nombredispositivo#	Comandos de debug, reload, configure
Global Configuration	Nombredispositivo(config)#	enable password, hostname, ip route

Configuration específica	De acuerdo al elemento específico a configurar, algunos ejemplos: Nombredispositivo(config-if)# Nombredispositivo(config-router)# Nombredispositivo(config-line)#	
---------------------------------	---	--

El modo EXEC del usuario solo permite una cantidad limitada de comandos de control básicos. El siguiente modo, el modo EXEC privilegiado, permite hacer un examen detallado del dispositivo, incluyendo administración, depuración y pruebas.

Y los modos de configuración específicos acceden a configuraciones de interfaces o servicios.

Navegación entre los modos de IOS

Por defecto, la CLI accede al modo de usuario (nombredispositivo>). Si se desea ingresar al modo EXEC privilegiado, digita al comando **enable**.

Una vez en el modo EXEC privilegiado (nombredispositivo#), utilice el comando **configure terminal** para acceder al modo de configuración global (nombredispositivo(config)#). Para retornar a un modo previo, solamente basta ejecutar al comando **exit**

III. MATERIALES Y EQUIPO

Para la realización de la guía de práctica se requerirá lo siguiente:

No.	Requerimiento	Cantidad
1	Guía 3 de Redes de Comunicación	1
2	PC con el software “Simulador Packet Tracer 5.3.1 by Cisco Systems” o una versión superior	1

IV. PROCEDIMIENTO

PARTE 1: Diseñando una Topología de Red de área local Ethernet

- Crear una carpeta principal donde se guardaran las diferentes simulaciones del procedimiento a continuación.
- Acceda a la aplicación Packet Tracer y guarde su primer archivo de simulación con el nombre **Practica05_proc1**.
- Agregue el listado de equipos indicados en la **Imagen 3.1: Dispositivos de red a utilizar** Imagen 3.1.

Cambie los nombres de los dispositivos por los solicitados aquí, porque se hará referencia a los mismos en el resto del procedimiento

Hacer las conexiones de red entre estos equipos de tal forma que se generen **4 dominios de colisión**.

El server debe quedar aislado en un dominio



de

colisión propio.

Los host GLADIS y ALEX deben pertenecer a un dominio de colisión común.

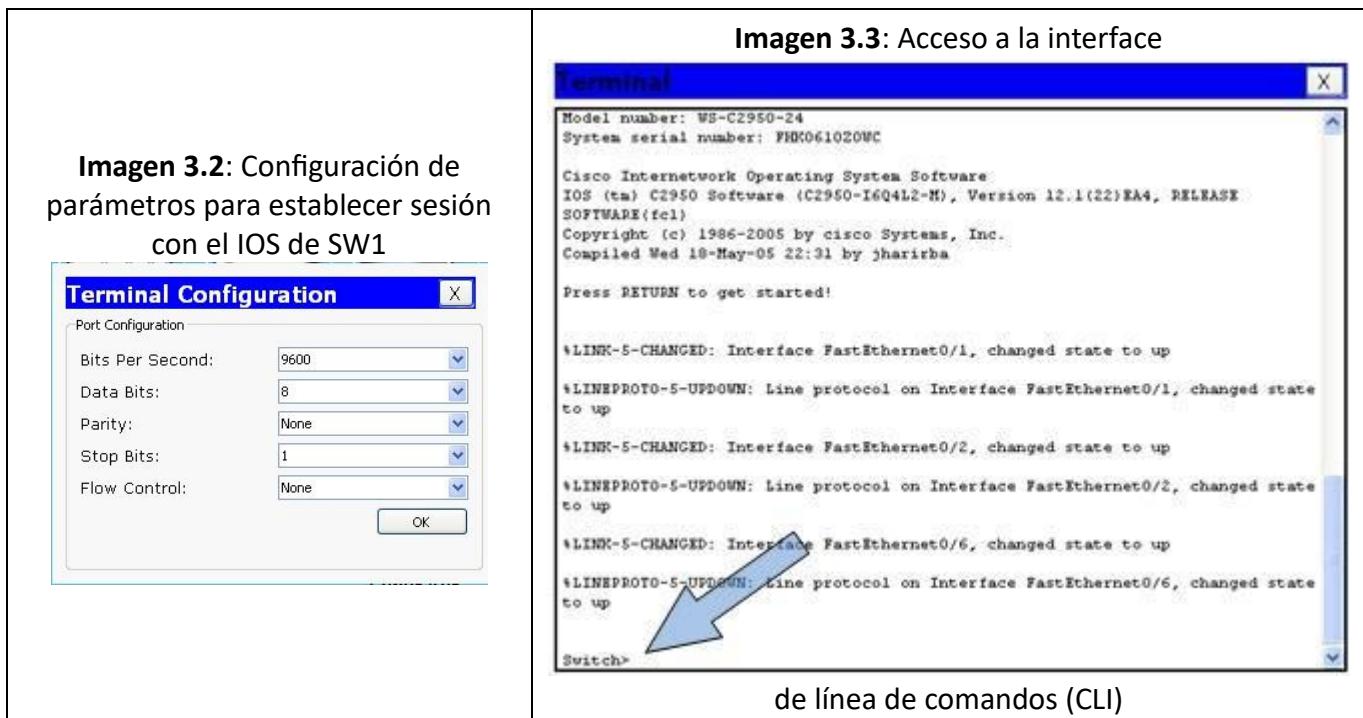
Todas las conexiones se harán con cables planos, excepto cuando se conecten dispositivos iguales o cuando sea una conexión entre el Switch y un Hub

4. Configurar al protocolo IP en cada uno de los Host y el Server bajo la red 10.0.0.X, en donde el byte X deberá ser diferente en cada equipo DTE. Y asigne la ip **10.0.0.1** en el parámetro Default Gateway en todos los host y el ServerFTP.
5. Desde el *Command Prompt* de ServerFTP, ejecutar un ping dirigido a la ip de GLADIS y otro ping hacia MIRIAM. En ambos caso deberá obtener respuesta.

PARTE 2: Configuración del (IOS) de un Dispositivo Administrable de Red

Sección 2.A: Estableciendo una sesión vía Consola con Switch SW1

6. Ubique al host GLADIS. Desde aquí iniciara una sesión directa de consola con el Switch SW1 de la topología de red.
7. Para comenzar, haga la conexión física de GLADIS a SW1. Seleccione un cable para conexión de Consola (Console).
Hacer clic sobre GLADIS y marque su interfaz serial de conexión (**RS-232**).
Luego dar clic en el Switch0 y seleccionar su interfaz de administración (**Console**).
8. Ahora, utilizará el software del **Emulador de Terminal** instalado en GLADIS para ingresar al IOS de SW1.
De clic sobre GLADIS, localice la ficha superior **Escritorio/Desktop** y luego seleccione al botón **Terminal**.



9. Observe la Imagen 3.2. Aquí se simula la ventana de configuración de parámetros para establecer una “Configuración de la terminal”.
 10. Confirme al dar clic en Aceptar/Ok.
 11. Ha ingresado a la ventana del emulador de terminal (ver la Imagen 3.3). Desde aquí hará la administración del IOS del Switch, ejecutando comandos desde una **Interface de línea de comandos (CLI: Command Line Interface)**.
 12. Presione Intro para ingresar al Modo de Ejecución del Usuario (o **Modo EXEC del usuario**) del IOS del Switch0.
- Sabrá que se encuentra en el mismo, gracias al tipo de cursor presentado: **Switch>**
- Este modo EXEC usuario permite ejecutar sólo una cantidad limitada de comandos de monitoreo básicos y de visualización solamente.

Sección 2.B: Ayuda contextual de la CLI

13. En el cursor del modo usuario actual, digite el símbolo (?). Vera el listado de comandos disponibles a este nivel de acceso de la CLI, junto a una descripción general de la acción y/o resultado que mostraría cada uno al ser invocado.
- Este es uno de los métodos de ayuda proporcionado al administrador, la cual se le denominada **“ayuda contextual”**.

14. Localice la descripción simple

Imagen 3.4: escritura incorrecta de un comando brindada sobre el comando **connect**.

15. Luego escríbalo en el cursor, pero escrito de manera incorrecta, por ej.: **conect** y presione Intro para ejecutarlo.

Tal como muestra la imagen 3.4, la CLI mostrara el siguiente mensaje:

Translating "conect"...domain server
(255.255.255.255)

The screenshot shows a terminal window titled 'Terminal'. The command 'Switch>?' is entered, followed by 'Exec commands:'. A list of commands is displayed, with 'connect' highlighted. Below the list, the command 'Switch>conect' is entered, followed by the message 'Translating "conect"...domain server (255.255.255.255)'.

```

Switch>?
Exec commands:
connect      Open a terminal connection
disable       Turn off privileged commands
disconnect    Disconnect an existing network connection
enable        Turn on privileged commands
exit         Exit from the EXEC
logout       Exit from the EXEC
ping          Send echo messages
resume       Resume an active network connection
show          Show running system information
telnet        Open a telnet connection
terminal     Set terminal line parameters
traceroute   Trace route to destination
Switch>conect
Translating "conect"...domain server (255.255.255.255)
  
```

Y no se mostrara nuevamente el cursor hasta que transcurran unos 40 seg.

Finalmente, se mostrara el siguiente mensaje:

% Unknown command or computer name, or unable to find computer address

16. Con el 1er mensaje, el IOS informa que se ha escrito un *comando no reconocido* y que intenta conectarse a un servidor de nombres de dominio (DNS) para obtener información del mismo. Luego del periodo de consulta, no hay servidor que le responda y el IOS informa al administrador con el 2do mensaje.

Por lo tanto, cuidar la escritura correcta de cada nombre de comando a ejecutar o esta suspensión por consulta de información se repetirá continuamente, restándole a usted tiempo valioso de configuración como administrador del dispositivo.

17. Nuevamente ejecute la ayuda contextual, ejecutando **?** Localice a la descripción del comando **show**. Este comando al igual que muchos disponibles en la CLI, puede usar *parámetros* que le especifican exactamente la operación realizar. Para ver las opciones disponibles para show, digite esta orden: **show ?**

18. Se muestra un listado de cada uno de los parámetros que puede ejecutar este comando show y una descripción del resultado que se obtiene al agregarlo a este comando.

Importante:

Si al final de un resultado de ayuda se muestra al texto **--More--**, significa que aún faltan mas parámetros disponibles.

Puede presionar Intro varias veces hasta ver el resto de parámetros del comando o sino, presionar cualquier otra tecla para retornar al Cursor (>) sin ver resto de parámetros.

19. Ejecute el comando show con su parámetro **clock**, de esta forma: **show clock** Este retornara la fecha-hora actual del sistema.

20. Obtenga las características de la versión del IOS activo, al ejecutar comando **show version**. Presione tecla Enter continuamente hasta que se muestre nuevamente el cursor del modo Usuario (**Switch>**)

De las líneas de resultado, localice el número de la Versión del IOS del dispositivo y el total de la memoria de la NVRAM (flash-simulated non-volatile configuration memory).

21. Luego digite el comando **show history** y deduzca el significado del resultado devuelto.
22. Proceda a ejecutar **enable** y vera que el cursor cambia a **Switch#**
23. Ahora se encuentra en el **modo de usuario privilegiado (Modo EXEC privilegiado)** de la CLI del Switch.
En este modo EXEC privilegiado, puede ejecutar comandos de configuración general del IOS.
24. Genere la descripción sobre los comandos disponibles en este modo. Presione continuamente tecla Enter para ver el listado completo de comandos disponibles.
25. Del listado de comandos, ubique la descripción del comando **disable**, y luego, proceda a ejecutarlo. ¿Cuál fue el resultado?
26. Retorne al modo EXEC privilegiado. Después ejecute el comando **clock ?** y analice la ayuda devuelta.
27. Con el parámetro set, se puede establecer/definir una nueva fecha-hora para el sistema. Escriba **clock** con el parámetro set y la ayuda contextual: **clock set ?**
28. Proceda a cambiar la hora del sistema del switch, ejecutando comando **clock set 16:30:23 17 february 2023**
Confirme si cambio la hora, ejecutando comando **show clock**

29. Ejecute nuevamente a clock pero con los parámetros incorrectos, ej.: **clock set 16:30:23 40 february 2017**

Observe como el CLI responde al ingresar incorrectamente el nombre y/o valor de los parámetros de un comando.

PARTE 3: Configurando la seguridad de acceso al IOS del Dispositivo de red Administrable

30. Proceda a ingresar al *modo de configuración global*. Para ello digite el comando **configure terminal**. Observe el cambio en la forma del cursor: **Switch(config)#**
31. Desde este Modo de Configuración Global se ejecutara el esquema de seguridad de acceso básico, para permitir acceso a los diferentes modos de administración del Switch solamente al personal autorizado.
32. Ejecute el comando **hostname SW1** para cambiar el nombre interno del equipo. Observe los cambios en el cursor activo.
33. Ingrese el comando **enable secret gatito**, y luego **enable password pajarito**. Estos asignan contraseñas de acceso a los diferentes modos de configuración del dispositivo.

<p>34. Con el siguiente comando de este grupo (ver a la derecha), ingresara a un <i>Modo de Configuración Específico</i>, en este caso al modo de configuración específico de línea de acceso de consola.</p>	<pre>line console 0 password perrito login exit</pre>
<p>35. Asigna la contraseña perrito, y la activa con login. Y retorna al modo configuración global.</p>	
<p>36. De manera similar a como configuro la seguridad de la línea de consola, ahora configurara a la línea de control de acceso remoto telnet.</p> <p>37. Con el carácter ayuda (?), observe que tiene 16 líneas (de la 0 a la 15) de sesiones telnet disponibles simultáneamente. De estas, selecciona a la 1era línea (vty 0)</p> <p>38. Luego, asigna contraseña cisco y la activa. Retorna al modo de configuración global.</p>	<pre>line vty ? line vty 0 password cisco login exit</pre>

39. Ejecute comando **banner motd \$Que tal administrador... bienvenido a switch SW1\$**

40. Ahora vera las consecuencias de la restricción de acceso a los diferentes modos y el acceso por línea de consola que configuro en pasos anteriores.

41. Digite comando **end** y luego cualquier tecla. Ahora digite **exit**. Se cierra la sesión de consola.

42. Presione Enter para ingresar nuevamente al modo EXEC usuario. Le solicitara una contraseña. Pruebe una a una las contraseñas asignadas (gatito, pajarito y perrito).

Importante:

Al ingresar contraseñas, estas nunca se mostraran, ni siquiera vera caracteres de confirmación de presión de teclas. Escriba la contraseña con la cual logro ingresar: _____

43. Ejecute los comandos necesarios para ingresar al modo de Configuración Global (cursor **SW1(config)#**). Identifique ¿En cuál de los Modos le solicita contraseña? y ¿Cuál de las 3 contraseñas fue la aceptada?

44. Ahora configurara al Switch SW1 un direccionamiento IP de host (dirección IP, máscara de subred y una gateway predeterminada), con el fin de manejarlo en forma remota mediante TCP/IP, desde una PC.

45. Ejecute el comando **interface vlan 1**

Ingrasa a otro modo de configuración específico, denominado “**modo de configuración de la interface de la VLAN 1**”. Observe que el cursor de entrada cambia a: **SW1(config-if)#**

46. Con los siguientes comandos, asigna al Switch una ip de host disponible de la red, activa la Vlan 1 (este concepto se verá en detalle en una práctica posterior) y retorna al modo configuración global.

```
ip address 10.0.0.200 255.0.0.0 no
shutdown
exit
```

<p>47. Luego, asigna al dispositivo una ip de puerta de enlace. Retorne al Modo EXEC privilegiado. Presione Enter para confirmar la orden. El cursor resultante será SW1# Y guardara todos los cambios efectuados hasta ahora hacia el archivo de configuración de inicio (startupconfig) del IOS.</p>	<pre>ip default-gateway 10.0.0.1 exit copy running-config startup-config</pre>
--	--

48. Ahora evalúe el listado de configuraciones realizadas al IOS del dispositivo SW1. Ejecute comando **show running-config**, para ver el archivo de configuración de ejecución actual. Observe desde la línea Building configuration... en adelante. Presione Enter de manera continua para ir retornando las líneas de configuraciones almacenadas.
49. Localice A CADA UNO DE LOS PARAMETROS QUE SE HAN ALTERADO EN LOS PASOS ANTERIORES, así como otros parámetros, entre ellos el nombre de las interfaces FastEthernet del dispositivo. Presione Enter hasta que se muestre nuevamente el cursor del modo actual.
50. Ejecutar **exit** para cerrar la sesión desde el Terminal del host GLADIS. Cierre la ventana de GLADIS.

PARTE 4: Estableciendo una sesión remota TELNET para la administración de un Switch

51. Seleccione a un host que esté conectado en alguno de los Hub, es decir, no esté conectado directamente a ninguno de los puertos del switch SW1. Ingrese al Command Prompt de esta PC seleccionada.
52. Envié un ping a la ip asignada a la VLan1 del switch SW1. Si no recuerda la IP asignada a SW1, ubique el cursor sobre este switch y localice a la IP asignada a vlan1.
Asegúrese que SW1 le responde como un DTE más dentro de la Networking, de lo contrario llame a su instructor para solucionar el problema.
53. Ejecute al comando telnet con la ip utilizada en el paso anterior, escribiendo lo siguiente: **telnet IPdeSW1**
En donde reemplazara **IPdeSW1** por la ip asignada a la vlan 1 del switch SW1.
54. Se intenta ingresar al CLI del IOS de SW1 de manera remota. Ingrese la contraseña **cisco**.
Vera que ingresa al modo EXEC usuario, tal como si estuviera desde el Emulador de Terminal.
55. Ejecute los comandos necesarios para acceder al modo de Configuración Global de la CLI, ingresando las contraseñas adecuadas.
56. Para demostrar que se está desarrollando una administración remota del dispositivo, se hará una configuración del switch SW1.
57. Desde el modo global, ejecute el siguiente comando. **no ip domain-lookup**
Retorne al software Terminal de GLADYS, para ingresa al modo EXEC privilegiado. Escriba cualquier palabra e inténtelo ejecutar.

Esta vez, no se pausara la ejecución ante un comando desconocido, debido a que se deshabilito la búsqueda a un servidor de nombres DNS desde la sesión remota.

58. Retorne al host donde inicio la sesión Telnet y luego, ejecute **exit** para cerrar la sesión telnet.

PARTE 5: Acceso a modos de configuración específicos

59. Para poder continuar, agregue a 2 host más a la topología de red, cada uno debe ser conectado a un dominio de colisión diferente. Configure el protocolo IP de cada uno con el direccionamiento apropiado.
60. Hará uso de los modos de configuración específicos, modificando a una interface o a conjunto de interfaces específicas.
61. Retorne al software Terminal del host GLADYS e ingrese al modo Global de SW1.
62. Identifique el número de puerto (interface) del SW1 al cual se conecta el ServerFTP.
63. Luego, se cambiara al modo de configuración especifica de esta interface con el siguiente comando (reemplace el **0/21** por el número del puerto que identifico en el paso anterior): **interface fastEthernet 0/21**
64. Use la ayuda contextual de comandos disponibles para esta interface, escribiendo (**?**). Luego, ejecute los siguientes comandos:

```
SW1(config-if)#description Acceso al ServerFTP
SW1(config-if)#speed 100
```

65. Ejecute **exit** para retornar al modo global. Ahora, ejecutara una acción sobre un rango específico de interfaces.
 66. Ejecute el siguiente comando:
- ```
SW1(config)#interface range fastEthernet 0/12-24 SW1(config-if-range)#shutdown
```
- De esta forma, desconecta administrativamente a cada una de las interfaces de la mitad de las interfaces del dispositivo, en lugar de ir modificando a cada una.
67. Desconecte alguno de los demás host existentes y conéctelos a uno de los puertos del rango de puertos del rango deshabilitado. Observe el resultado en el área de trabajo de su simulación.
  68. Para volver a reactivar el rango de las interfaces anterior, solamente debe “negar” al comando anterior. Ejecute comando: **no shutdown**

69. Llame a su instructor para confirmar el funcionamiento apropiado de su simulación hasta este momento.
70. Guarde la configuración de comandos del switch SW1, ejecutando el comando: **do copy running-config startup-config**
71. Guarde y cierre la simulación.

## V. DISCUSION DE RESULTADOS

### EJERCICIO COMPLEMENTARIO

Haga una copia de la simulación final del procedimiento, para luego hacer una copia del archivo bajo el nombre: **Practica05\_analisis**

En esta nueva simulación, realice los siguientes cambios:

Desde el software Terminal de cualquiera de los host, ingrese al IOS del SW1 y desactive administrativamente a todos sus puertos que aun no estén siendo utilizados.

Luego, desde MIRIAM:

Haga una conexión vía consola con el router YUPI y desde el software Terminal, desarrolle la siguiente configuración en el IOS de YUPI:

**Hostname: YUPI Esquema de contraseñas**

acceso:

**Banner de presentación:**

Intentando acceder a enrutador YUPI

**Fecha/Hora:**

*14:00h de este dia del año en curso*

| Modo                | Contraseñas                                      |
|---------------------|--------------------------------------------------|
| Privilegiado        | <i>su número de carnet en minúscula ni guion</i> |
| Consola             | Consolayupi                                      |
| telnet, línea vty 0 | linea1yupi                                       |
| telnet, línea vty1  | liínea2yupi                                      |

**Interface de conexión utilizada de YUPI:** asignarle la dirección ip **10.0.0.1 255.0.0.0** y activar (no shutdown)

Finalmente, enviar a su instructor una copia de la carpeta con la resolución de las simulaciones realizadas durante todo el procedimiento de esta practica



**UNIVERSIDAD AUTONOMA DE  
CHIHUAHUA  
FACULTAD DE INGENIERIA**

**enero-junio  
2023**

**GUÍA DE LABORATORIO #04**

**Nombre de la Practica:** Cableado de topologías de red  
**Lugar de Ejecución:** Laboratorio de redes  
**Tiempo Estimado:** 2 horas y 30 minutos  
**MATERIA:** Redes

**I. OBJETIVOS**

Que el estudiante:

- Compare los diferentes estándares para la elaboración del Cableado de una LAN.
- Seleccione la norma de elaboración de cableados de red según estándares internacionales.
- Adquiera las destrezas motrices para utilizar las herramientas de construcción del Cableado de una LAN.
- Fabrique cables de red aplicando las normas EIA/TIA 568A y EIA/TIA 568B
- Elabore el cable necesario para conectar dos dispositivos (host) del mismo tipo (cable directo).
- Elabore el cable necesario para conectar dos dispositivos (host) diferentes (crossover).
- Compruebe el funcionamiento del cableado que permite la comunicación entre los hosts.

**II. INTRODUCCION TEORICA**

**¿Por qué es tan importante un cableado óptimo dentro de la red?**

Una red LAN está limitada por distancias geográficas relativamente pequeñas y en su diseño incluye dispositivos tales como computadoras, hub, switches y otros.

Dentro de la jerarquía de las siete capas del modelo OSI, la **Capa Física (nivel1)** es el pilar de la transferencia de la información y uno de los principales factores que influyen en el óptimo funcionamiento de una Red.

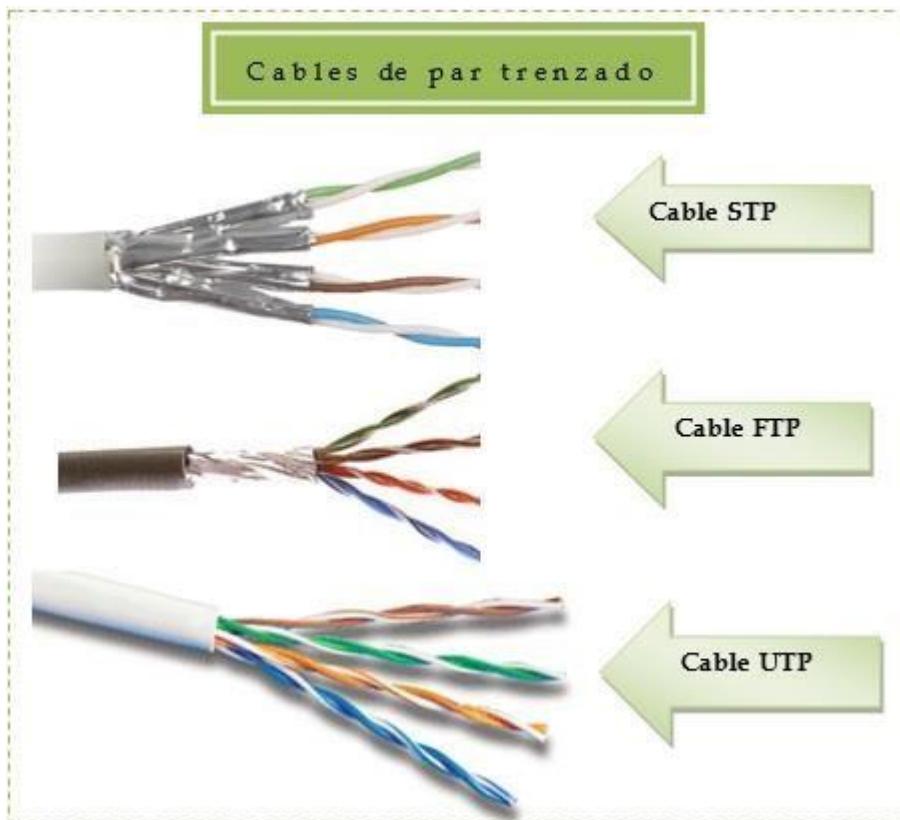
Un mal cableado es uno de los factores que puede causar pérdidas de paquetes de datos, al sobrecargar la red y disminuir su desempeño, hasta causar altos costos y por lo tanto pérdidas en el presupuesto de una empresa.

## Los medios de cobre

Los cables de **cobre** más utilizados son los cables de par trenzado (ver imagen 4.1), que en sus inicios fueron utilizados para las comunicaciones telefónicas.

1 / 13

**Imagen 4.1:** Tipos de cables de Par Trenzado



### Cable de par trenzado apantallado STP (Shielded Twisted Pair)

En este tipo de cable, cada par va recubierto por una malla conductora que actúa de apantalla frente a interferencias y ruido eléctrico. Su impedancia es de 150 Ohm.

El nivel de protección del STP ante perturbaciones externas es mayor al ofrecido por UTP. Sin embargo es más costoso y requiere más instalación. La pantalla del STP, para que sea más eficaz, requiere una configuración de interconexión con tierra (dotada de continuidad hasta el terminal), con el STP se suele utilizar conectores RJ49.

Es utilizado generalmente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, pero el inconveniente es que es un cable robusto, caro y difícil de instalar.

### Cable de par trenzado con pantalla global (FTP)

En este tipo de cable como en el UTP, sus pares no están apantallados, pero sí dispone de una pantalla global para mejorar su nivel de protección ante interferencias externas.

Su impedancia característica típica es de 120 ohmios y sus propiedades de transmisión son más parecidas a las del UTP. Además, puede utilizar los mismos conectores RJ45. Tiene un precio intermedio entre el UTP y STP.

### **Cable par trenzado no apantallado (UTP)**

UTP (del inglés: Unshielded Twisted Pair, par trenzado no apantallado) es un cable de par trenzado más simple y el más empleado, sin ningún tipo de pantalla adicional y con una impedancia característica de 100 Ohmios.

El conector más frecuente con el UTP es el RJ45, aunque también puede usarse otro (RJ11, DB25, DB11, etc.), dependiendo del adaptador de red.

Es sin duda el que hasta ahora ha sido mejor aceptado, por su costo accesibilidad y fácil instalación. Sus dos alambres de cobre torcidos aislados con plástico PVC han demostrado un buen desempeño en las aplicaciones de hoy. Sin embargo, a altas velocidades puede resultar vulnerable a las interferencias electromagnéticas del medio ambiente.

#### **Características del cable Unshielded Twister Pair (UTP) Categoría 5 Formato de cables**

Según los recursos con que se cuente para administrar Hubs, Switches, Routers, o simplemente dos PCs, la construcción del cableado comienzan con identificar los recursos a conectar entre sí. Sin embargo existen estándares para unir los alambres del cable UTP lo cual facilita dichas tareas.

#### **Seleccionando Categoría del Cable**

La categoría especifica las ventajas que se tendrán con el cable, por ejemplo el nivel de aislamiento del ruido exterior, longitudes máximas a cubrir, etc. Actualmente el cableado de Categoría 5 es el más usado por su relación costo y eficiencia.

El cable que trataremos en esta guía será el UTP Categoría 5, al que nos referiremos como **UTPC5** en adelante.

#### **Número de alambres y pares del UTPC5**

Este contiene 8 hilos de cobre en donde se tienen dos de estos hilos trenzados en sí mismo, dos trenzas de estos hilos se les conoce como un par en total se tienen 4 pares de cables trenzados contenidos en un forro de PVC.

#### **Ordenando los pares**

Los pares de cables dentro del cable UTP tienen colores para poder identificar fácilmente cada cable en ambas puntas.

Cada par de cables tiene un código de color.

**Imagen 4.2:** Orden de los pares de cables dentro de un cable UTP

Los códigos de los cuatro pares están constituidos por un color sólido y otro del mismo color, pero con fondo blanco, tal como se observa en la imagen 4.2. La tabla muestra el orden normal de los pares de cables, “**no su forma de conectarse**”.

|                |                               |  |
|----------------|-------------------------------|--|
| <b>Par # 1</b> | <b>Blanco/Azul Azul</b>       |  |
| <b>Par # 2</b> | <b>Blanco/Naranja Naranja</b> |  |
| <b>Par # 3</b> | <b>Blanco/Verde Verde</b>     |  |
| <b>Par # 4</b> | <b>Blanco/Café Café</b>       |  |

### Conectores para el cableado UTP

Los conectores y jacks de uso común para cable UTPC5 son los **RJ45**. El conector es una pieza de plástico transparente en donde se inserta el cable y tienen identificado un número de pin, según su forma física. Esta ubicación del pin es importante respetarla para óptimos resultados.

En la imagen 4.3 se muestra al *conector RJ45 macho* y al *conector Jack* para su uso en los extremos de conexión de un cable UTP.

**Imagen 4.3:** Conector RJ-45 macho y hembra (Jack) para el Cable UTP CAT 5



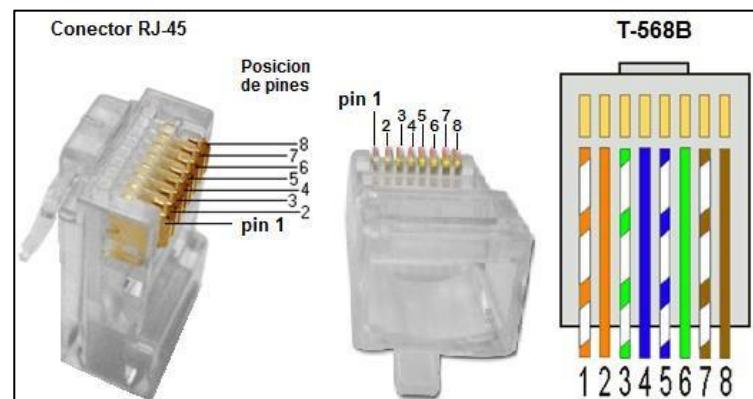
Este conector reduce el ruido, y los

**Imagen 4.4:** Ubicación de pines del Conector RJ45 macho problemas de estabilidad mecánica y se asemeja al enchufe telefónico, con la diferencia de que tiene ocho conductores en lugar de cuatro.

Se considera como un *componente de networking pasivo* ya que sólo sirve como un camino conductor de corriente eléctrica entre los cuatro pares del cable trenzado de Categoría 5 y las patas de la toma RJ-45.

El cable se inserta en el conector por la parte trasera (Ver la imagen 4.4).

Una vez el cable tiene un conector en cada extremo, cada conector se conecta al Jack que puede estar en la pared, o en la tarjeta de red de la computadora o en el concentrador.



### Jacks RJ-45

Los enchufes o conectores RJ-45 se insertan en **jacks o receptáculos RJ-45**. Los jacks RJ-45 tienen 8 conductores, que se ajustan a los del conector RJ-45. En la parte posterior del Jack RJ-45 hay un bloque de inserción donde los hilos individuales se separan y se introducen en ranuras mediante una herramienta similar a un tenedor denominada **herramienta de punción**. Esto suministra un camino conductor de cobre para los bits. El Jack RJ-45 es un componente de la Capa 1.

### Paneles de Conexión (Path Panel)

Los paneles de conexión son una serie de jacks RJ-45 agrupados de forma conveniente en una sola pieza. Esta viene con configuraciones de 12, 24 o 48 puertos y normalmente están montados en un bastidor, como se muestra en la Imagen 4.5.

Las partes delanteras son jacks RJ-45 y las partes traseras son bloques de punción que proporcionan conectividad o caminos conductores. Se clasifican como dispositivos de la Capa física.

**Imagen 4.5:** Un panel de Conexión (Path Panel)



### Cables de conexión de Red: Normas EIA/TIA 568-A y TIA 568-B CABLE PLANO

Es el estándar para conectar una PC a un Hub. Se le llama **cable plano**, porque se conecta uno a uno cada pin de ambos extremos del cable UTP, es decir el pin 1 al pin 1 de ambos extremos de un cable de cobre, luego al cable del pin 2 a pin 2, pin 3 a pin 3, y así sucesivamente, observe la Tabla de la imagen 4.6.

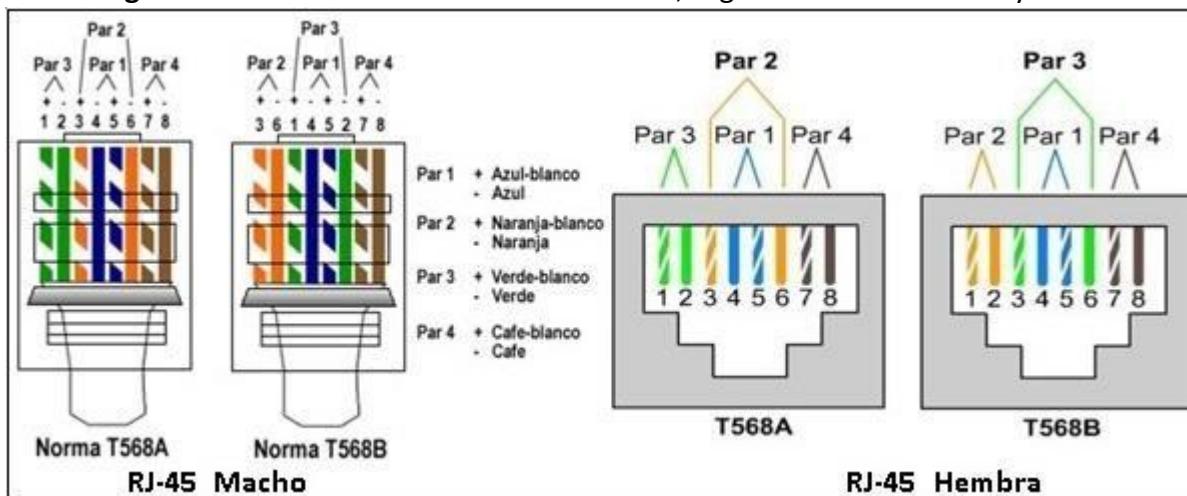
**Imagen 4.6:** Orden de secuencia de los pines de un Cable UTP CAT5 para un cable “Plano”

| <b>COMBINACIÓN DE COLORES POR PINES (Cable Plano: UTP CAT5)</b> |                             |
|-----------------------------------------------------------------|-----------------------------|
| <b>RJ45 Izquierdo</b>                                           | <b>RJ45 Derecho</b>         |
| Pin 1 color: Blanco/Naranja                                     | Pin 1 color: Blanco/Naranja |
| Pin 2 color: Naranja                                            | Pin 2 color: Naranja        |

|                           |                           |
|---------------------------|---------------------------|
| Pin 3 color: Blanco/Verde | Pin 3 color: Blanco/Verde |
| Pin 4 color: Azul         | Pin 4 color: Azul         |
| Pin 5 color: Blanco/Azul  | Pin 5 color: Blanco/Azul  |
| Pin 6 color: Verde        | Pin 6 color: Verde        |
| Pin 7 color: Blanco/Café  | Pin 7 color: Blanco/Café  |
| Pin 8 color: Café         | Pin 8 color: Café         |

Tal como se muestra en la imagen 4.7, existen 2 normas (T568-A y T568-B) que sugieren la secuencia de colores de los pares de cables que debe implementarse en ambos extremos del cable. Lo importante es que se aplique la misma norma en ambos extremos.

**Imagen 4.7:** Orden de cables en conector RJ45, según las normas T568A y T568B



### CABLE CROSSOVER/CRUZADO (PUNTO A PUNTO)

Este cable se utiliza solamente cuando se dispone de 2 computadoras (que es la manera más sencilla para conectar dos PCs entre sí).

Se debe tener cuidado con la distancia a cubrir con el cable, pues al no tener un reforzador de señal estamos limitados a las distancias que limitan al cable UTP CAT5.

En la imagen 4.8, se indica el orden de conexión entre los pines de un cable UTP de tipo Cruzado.

**Imagen 4.8:** Secuencia de colores en los extremos de un cable UTP “Cruzado”.

| EXTREMO IZQUIERDO DEL CABLE |                | EXTREMO DERECHO DEL CABLE |                |
|-----------------------------|----------------|---------------------------|----------------|
| Pin 1                       | Blanco/Naranja | Pin 1                     | Blanco/Verde   |
| Pin 2                       | Naranja        | Pin 2                     | Verde          |
| Pin 3                       | Blanco/Verde   | Pin 3                     | Blanco/Naranja |

|              |             |              |             |
|--------------|-------------|--------------|-------------|
| <b>Pin 4</b> | Azul        | <b>Pin 4</b> | Azul        |
| <b>Pin 5</b> | Blanco/Azul | <b>Pin 5</b> | Blanco/Azul |
| <b>Pin 6</b> | Verde       | <b>Pin 6</b> | Naranja     |
| <b>Pin 7</b> | Blanco/Café | <b>Pin 7</b> | Blanco/Café |
| <b>Pin 8</b> | Café        | <b>Pin 8</b> | Café        |

### Concentrador (Hub)

El propósito de un hub es regenerar y re temporizar las señales de red. Esto se realiza a nivel de los bits para un gran número de hosts (por ejemplo: 4, 8 o incluso 24 PC) utilizando un **proceso denominado Concentración**.



Podrá observar que esta definición es muy similar a la del repetidor, es por ello que al **Hub** también se le denomina **Repetidor Multipuerto**. La diferencia es la cantidad de cables que se conectan al dispositivo.

Las razones por las que se usan los hubs son: a) crear un **punto de conexión central** para los medios de cableado y b) aumentar la **confiabilidad de la red**.

La confiabilidad de la red se ve aumentada al permitir que cualquier cable falle sin provocar una interrupción en toda la red.

### III. MATERIALES Y EQUIPO

Para la realización de la guía de práctica se requerirá lo siguiente:

| No. | Requerimiento                                 | Cantidad |
|-----|-----------------------------------------------|----------|
| 1   | Guía de Laboratorio #4 de Redes               | 1        |
| 3   | Segmento de 2 metros de Cable UTP categoría 5 | 1        |
| 4   | Conecotor RJ45 macho                          | 3        |
| 5   | Conecotor Jack RJ45                           | 1        |
| 5   | Tenazas Prensadoras RJ45                      | 1        |
| 6   | Cortador de alambre                           | 1        |
| 7   | Multitester                                   | 1        |
| 8   | (*) Panel de Conexión                         | 1        |
| 9   | (*) Herramienta de Punción                    | 2        |

|    |                  |   |
|----|------------------|---|
| 10 | (*) Switch o Hub | 1 |
|----|------------------|---|

## IV. PROCEDIMIENTO

### INICIO: Entrega de materiales

1. Forme grupos de 3 estudiantes y soliciten a su instructor los materiales descritos en los requerimientos para esta práctica.
2. Además, cada estudiante llenara sus datos personales en la hoja de evaluación de la práctica. La calificación la hará su instructor de acuerdo al desempeño y habilidades alcanzadas por c/alumno en el resto del procedimiento a continuación.

#### PARTE 1: Elaboración de Cable Cruzado (Crossover)

3. Tome la herramienta cortadora de cable (ver **Imagen 4.9:** Herramienta cortadora Imagen 4.9) y retire un aproximado de **1 ½ cm** del de cable UTP forro PVC en ambos extremos del segmento de cable UTP proporcionado.
4. Alinee los alambres de cada extremo del cable y ordenarlos por colores (de acuerdo a las normas de código de colores) para crear un cable “cruzado”.



Llene la Tabla de la Imagen 4.10 con la secuencia de colores de los alambres que usara en cada extremo.

**Imagen 4.10:** Llene los colores de cables en los pines de cada extremo de un cable UTP cruzado

| Pin | Extremo 1 | Extremo 2 | Pin | Extremo 1 | Extremo 2 |
|-----|-----------|-----------|-----|-----------|-----------|
| 1   |           |           | 5   |           |           |
| 2   |           |           | 6   |           |           |
| 3   |           |           | 7   |           |           |
| 4   |           |           | 8   |           |           |

5. Cada estudiante debe seleccionar un extremo de cable, para introducir lentamente los 8 alambres dentro de un conector RJ45.

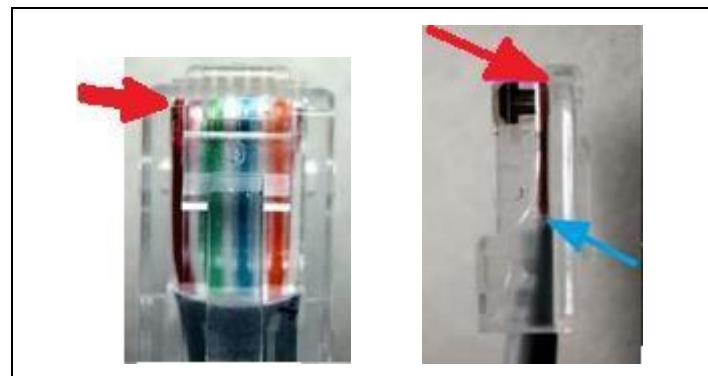
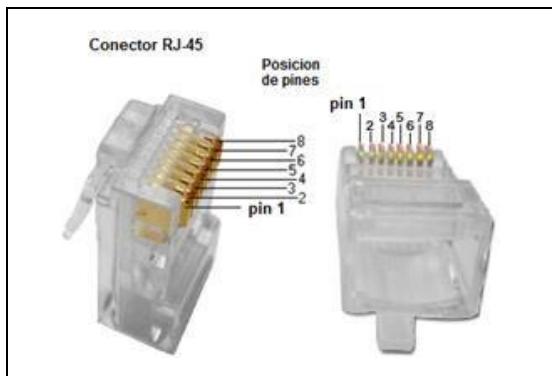
En este momento, verifique de cumplir cada uno de los siguientes aspectos:

- A. Seleccione el alambre 1 de la secuencia de colores a implementar en su extremo, para ubicar el alambre 1 de la secuencia de colores en el **pin 1** en cada conector, observe la imagen 4.11.

- B. Los alambres deben ir quedando a la misma altura (ver flecha roja en imagen 4.12), de lo contrario, los alambres más cortos no harán contacto con su pin del conector y el funcionamiento del cable será deficiente o quedará inservible.
- C. El forro debe introducirse hasta la mitad del interior del conector (ver flecha azul en imagen 4.12).

**Imagen 4.11:** Ubicación de pin 1 en**Imagen 4.12:** Vista frontal y laterales del RJ-45 con conector

RJ-45 los alambres dentro del forro.



6. Realice un reconocimiento “visual lateral” sobre el conector RJ45, para confirmar que cada alambre del UTP queda al mismo nivel y alcanza el final del conector.
7. Una vez verificada la colocación correcta de cada alambre y norma en el conector de cada, llame a su instructor para que haga una última confirmación y que ambos conectores están listos para ser prensados.
8. Seleccione la herramienta de Crimpar (ver Imagen 4.13) e introduzca uno de los conectores ya preparados en la abertura apropiada para RJ-45.

**MUY IMPORTANTE:**

Bajo ningún motivo prense el conector con la crimpadora si no está seguro de haber aplicado correctamente alguno de los pasos mencionados, pues una vez prensado no se podrá retornar para corregir descuidos, y debe sustituirse por otro conector RJ45.



9. Con la tenaza, prense con fuerza al conector hasta se escuche un **leve Clic** en la tenaza, lo que asegura que las placas del conector han penetrado los pines. Libere la herramienta.
  10. Repita el paso anterior para el conector del otro extremo del cable UTP que está preparando.
  11. Llame a su instructor, para comprobar por medio de un Tester (probador de cables de red) si se ha “cruzado” correctamente los pares de colores en el cable.
- Finalmente, comprobar que cada pin esta eléctricamente conectado.

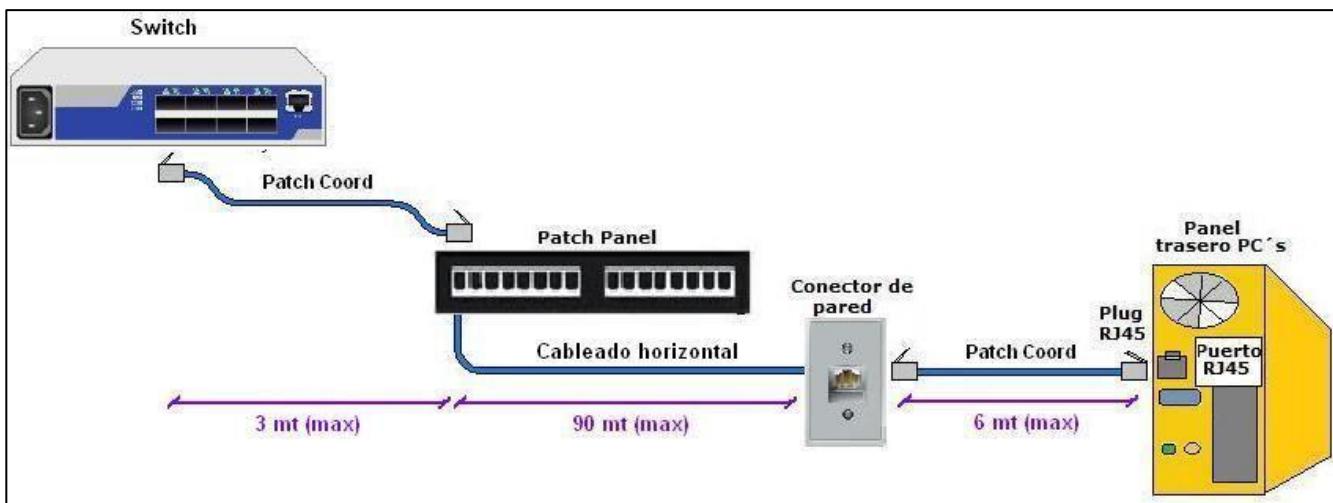
## **PARTE 2: ELABORACION DE UN CABLE PLANO**

12. Para elaborar el cable plano, proceda a cortar exactamente por la mitad a su cable UTP cruzado desarrollado en el procedimiento de la parte anterior.
13. Ahora se cuenta con 2 segmentos de cable UTP y cada uno con un conector macho en uno de sus extremos.
14. Seleccione a uno de los 2 segmentos de cable obtenidos al cortar el cable cruzado del paso anterior.
15. Del segmento elegido, identifique la norma aplicada en el conector RJ45 ya existente.  
Luego, separe los 8 alambres del extremo libre de este segmento de cable con la misma secuencia de colores de la norma usada en el conector RJ-45 de su otro extremo.
16. Tome el último conector RJ-45 proporcionado y complete la conexión del extremo libre del segmento de cable analizado en el paso anterior. De esta manera, creara un “Cable Plano”, porque ambos extremos tendrán aplicada la misma norma de colores en sus pines.
17. Llame a su instructor para que evalúe con un **Tester** que su cable “**plano**” elaborado es correcto y funcional.
18. Conecte su cable plano entre la tarjeta de red (NIC) de una de las PC utilizadas con el conector RJ45 hembra (**módulo RJ-45**) ubicado en las placas de conexión de red atrás de las mesas del laboratorio.  
Confirmar que funciona, gracias a que la luz de la NIC se enciende al fijar ambos extremos de c/cable y que se mantiene la conexión a internet desde un navegador web.
19. Desconecte el cable plano elaborado.

## **PARTE 3: ELABORACION DE UN CABLEADO ESTRUCTURADO DE RED**

20. Ahora procederá a elaborar un Cableado Estructurado UTP, basado en el diagrama de conexión física mostrada en la imagen 4.14.

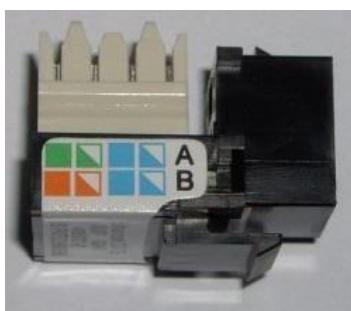
**Imagen 4.14:** Topología física del Cableado Estructurado de Red a implementar.



- Cada uno de los 3 segmentos de cable son de tipo plano (utilizando la misma norma TIA en ambos extremos) y el cable que hace falta elaborar es el del “Cableado horizontal”.

21. Solicite a su instructor el material restante indicado en la tabla de requerimientos (Jack RJ-45, Patch Panel, herramienta de punción y un Switch).
22. Tome el 2do segmento de cable UTP, que tiene un conector RJ-45 macho ya preparado en uno de sus extremos y el otro aun libre.
23. Seleccione la herramienta para cortar cable UTP y corte el conector RJ45 macho de este segmento. Así obtendrá un nuevo segmento UTP sin conectores en sus extremos.
24. Retire 1.5 cm del forro PVC en cada uno de los extremos de este segmento de cable UTP.
25. Seleccione el Jack RJ-45 y ubique a cada lado a los colores de las normas de colores A o B, observe un ejemplo en la Imagen 4.15.

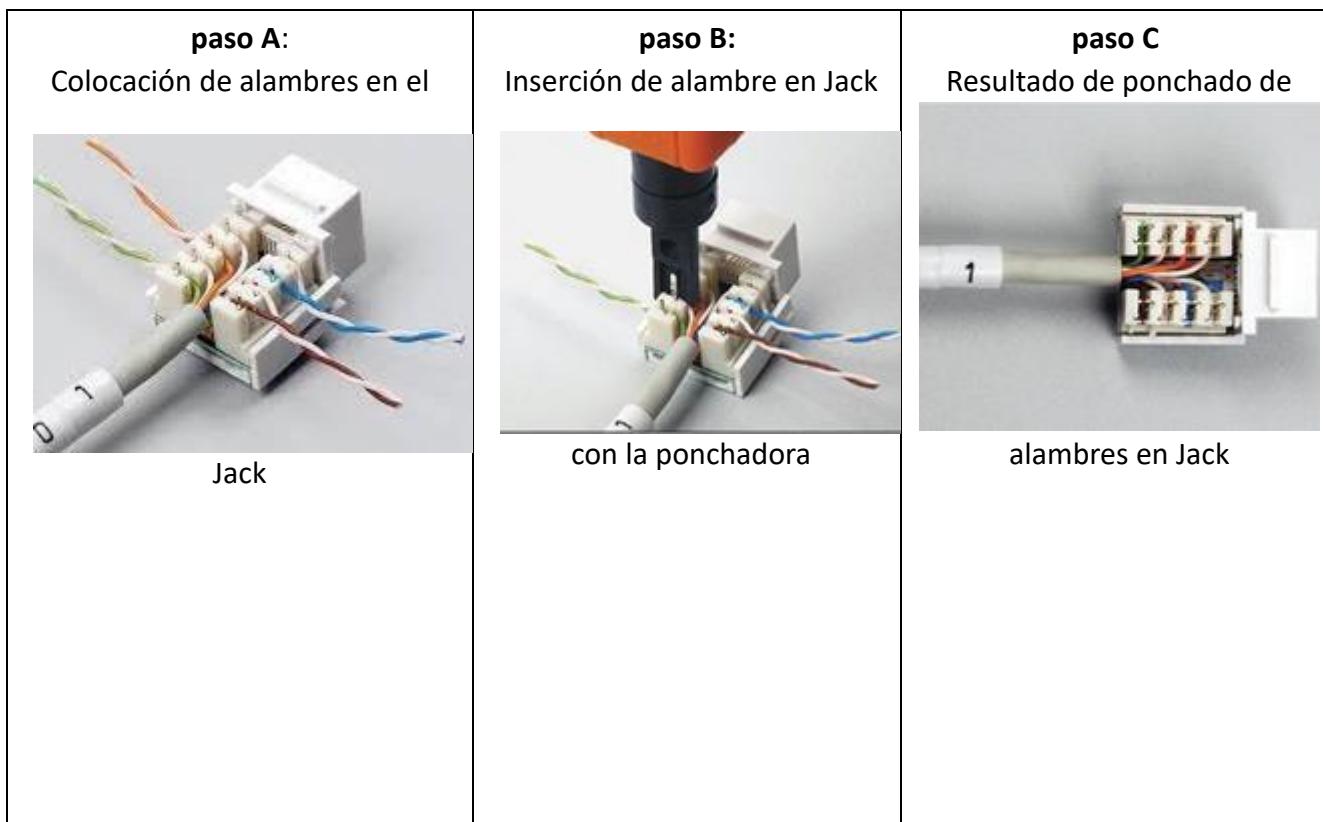
**Imagen 4.15:** Vista lateral  
Ponchadora de cables



**Imagen 4.16:** Herramienta del Jack RJ-45



26. De las hendiduras de los 2 lados del Jack RJ-45, identifique la secuencia de colores que corresponda a la **norma A (TIA 568-A)**.

**Imagen 4.17:** Preparación de alambres en el conector Jack RJ45

27. Proceda a ordenar y alinear a los alambres de uno de los extremos del segmento de cable UTP a cada lado del Jack RJ-45 (observe el **paso A** de la imagen 4.17) e inserte cada alambre en la hendidura apropiada del conector.
28. Tal como muestra el **Paso B** de la imagen 4.17, coloque el Jack RJ-45 en una superficie firme, tome la herramienta ponchadora y ubique su punta sobre una de las hendiduras del Jack, con el extremo de filo hacia afuera del Jack.
29. Con esta herramienta, haga una presión vertical rápida sobre la hendidura elegida, para fijar el alambre en la hendidura del conector.
30. Repita el paso anterior, para insertar uno por uno al resto de alambres en las hendiduras del Jack.
31. Remueva el exceso de cada alambre en las hendiduras del Jack. En el **Paso C** de la imagen 4.17, muestra el resultado de cómo deben quedar distribuidos los 8 alambres del cable UTP dentro del Jack RJ-45.
32. Ahora, creara el otro extremo de su cable horizontal.
33. Alinee los 8 alambres del otro extremo del cable.
34. Tome el Patch Panel. Ubique el lado de entradas Jack y seleccione un puerto de conexión libre, no utilizado por otro equipo de compañeros.

Luego, ubique en la parte de atrás (denominada *Bloque de Punción*) al bloque de hendiduras correspondiente al puerto seleccionado en el paso anterior, como se muestra la Imagen 4.18.

35. Coloque al patch panel con su lado **Imagen 4.18: bloque de punción** de entradas Jack en un lugar plano y un puerto del Patch Panel firme, de modo que observe el *bloque de punción* elegido del dispositivo. Este bloque de punción es del mismo tipo que se compone un conector Jack RJ-45 individual.

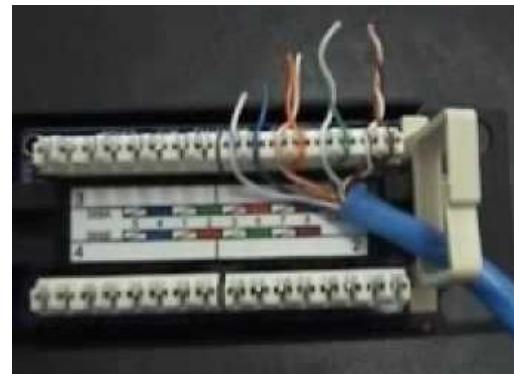


36. Ubique el patrón de colores 568-A en el bloque de punción del puerto seleccionado, para luego, colocar el forro del extremo del cable en el canal interior del patch panel.

Coloque cada alambre en la hendidura correspondiente del bloque, según los colores de la norma indicada en este paso, en dirección hacia afuera del dispositivo. Observe un ejemplo en la imagen 4.19.

37. Finalmente, utilice la herramienta de **Imagen 4.19: Ubicación de alambres en la punción** para hacer presión a cada alambre hendidura de conexión del puerto dentro de la hendidura correspondiente.

38. Compruebe que el segmento de cable horizontal está correcto, haciendo la conexión de un cable plano, en el Jack individual y puerto del patch panel.



39. Con un tester, utilice los extremos de ambos cables planos para comprobar si el circuito de conexiones está correcto.

El Tester debe indicar que hay una conexión de tipo plana (misma norma en c/extremo de la conexión) y debe haber conexión en cada uno de los 8 alambres del cableado.

40. Seleccione otra pareja de compañeros que hayan desarrollado correctamente todos los pasos anteriores sobre el mismo Patch Panel asignado a ambos grupos.

41. Encienda el dispositivo (Switch o Hub) proporcionado para este procedimiento.

Cada grupo haga su respectiva conexión hacia un puerto diferente del switch y en el otro extremo hacia la NIC de su respectiva PC.

Confirme que el indicador de uso cada puerto del switch se enciende, confirmando que ha detectado un equipo terminal en ese puerto conectado.

42. Llamen a su instructor para comprobar que ambos puertos del switch (de los 2 grupos de estudiantes) están activados.
43. Demuestre que hay envío de mensajes entre ambas PC conectadas al switch, gracias al cableado implementado en el Patch Panel.
44. Pana finalizar, reconecte la NIC de cada PC utilizada en las pruebas, hacia el cableado de red fijo del laboratorio y restaure el acceso a internet.
45. Desconectar el switch/hub utilizado y de una manera ordenada, entregue los diferentes materiales y dispositivos a su instructor.
46. Luego de confirmar que el equipo entregado es devuelto en orden, este le mostrara la evaluación individual y grupal de su desempeño alcanzado a lo largo de toda la práctica.
47. Apague las diferentes PC's utilizadas.

## VI. INVESTIGACION COMPLEMENTARIA

- ¿Cuál es la función específica de cada par dentro de un cable UTPCAT5?
- ¿Cómo se hace un **cable para la administración directa** de un Dispositivo Switch o Router?  
¿Cuál es la función y como se le conoce en el medio de los técnicos de redes?  
Describa en detalle su elaboración (**teoría e imágenes**)

## VII. BIBLIOGRAFIA

- Shaughnessy, Tom. Manual de Cisco. MCGRAW HILL 2000



## UNIVERSIDAD AUTONOMA DE CHIHUAHUA FACULTAD DE INGENIERÍA

enero-junio  
2023

### GUIA DE LABORATORIO # 5

Práctica: Configuración de Spanning Tree Protocol (STP)  
Lugar de Ejecución: Laboratorio de Redes  
Tiempo Estimado: 2 horas, 30 minutos  
Materia: Redes

#### I. OBJETIVOS

- Analice las consecuencias negativas de los bucles de capa 2 dentro de una red commutada
- Evaluar el funcionamiento del algoritmo Spanning tree (STA), utilizado por el protocolo STP.
- Personalice los parámetros de STP para establecer a un Puente Raíz y a un Puente Secundario.
- Diseñe una topología de red en base al modelo jerárquico, utilizando STP para bloquear lógicamente a enlaces redundantes de capa 2.

#### II. MATERIALES Y EQUIPO

| No | Requerimiento                                                     | Cantidad |
|----|-------------------------------------------------------------------|----------|
| 1  | Estación de trabajo PC.                                           | 1        |
| 2  | Simulador de Red (Cisco Packet Tracer 5.3.1 o superior) instalado | 1        |
| 3  | Guía de laboratorio #5                                            | 1        |
|    |                                                                   |          |

#### III. PROCEDIMIENTO

1. Cree una carpeta denoma **RECpractica5\_CARNET**, en la cual guardara las diferentes simulaciones solicitadas en el procedimiento a continuación.

### Parte I: Bucle de capa 2 al crear un enlace redundante entre switch

2. Abrir el software Cisco Packet Tracer y guardar la simulación bajo el nombre **Parte1\_Switch\_sinSTP**. Agregar 1 switch de la serie 2950-24 y cambiarle su nombre por **S1**.
3. Ingresar al modo de configuración global de switch S1 y cambiar su hostname por S1. Luego, ejecute los siguientes comandos:

| comando                                                                                                                    | acción                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no cdp run<br>no ip domain-lookup                                                                                          | Deshabilita protocolo cdp<br>Deshabilita búsqueda con servidor dns por comandos mal escritos                                                                         |
| no spanning-tree vlan 1<br>interface range fastEthernet 0/1-20<br>switchport mode access<br>switchport nonegotiate<br>exit | Desactiva STP para vlan 1 predeterminada<br>Selecciona puertos de acceso<br>Modo de acceso a la vlan 1 predeterminada<br>Deshabilita la negociación de protocolo DTP |
| interface range fastEthernet 0/21-24<br>switchport mode trunk end<br>write                                                 | Selecciona puertos en modo troncal<br>Retorna directamente al Modo Privilegiado<br>Guarda cambios en archivo startup-config                                          |

Estos comandos deshabilitan a los protocolos CDP, STP y DTP; definen los puertos de acceso (a la vlan 1 predeterminada) y define los puertos troncales.

4. Guarde la configuración de S1. Luego, seleccione S1 con el puntero del ratón y proceda a duplicarlo 2 veces, para crear 2 switch más con la misma configuración de S1.
5. Cambie el nombre de la nueva pareja de switch por S2 y S3; además, ingrese a la CLI de cada uno y cambiar sus hostname por S2 y S3, respectivamente. Y guarde la configuración de ejecución de los nuevos switch
6. Agregue una PC y conéctela a un puerto de acceso de S1.  
Observe que el puerto del switch S1 se coloca directamente en modo acceso (color Verde en extremo de cable). Ya no negocia su Estado de conexión como antes (extremo de conexión en color Naranja).
7. Agregue 2 PC más, luego configure el protocolo ip de los 3 host para formar parte de la red 195.0.0.0
8. Conecte a PC1 a un puerto de acceso de S2.  
Y conecte con un cable cruzado a un puerto troncal de S1 con un puerto troncal de S2.

9. Desde la ventana de comandos (command prompt) del host PC0, envíe un ping hacia PC1, conectado a S2. Comprobar que hay comunicación entre ambos host.
10. Desde PC0, ejecute comando arp -d, para limpiar su tabla de ARP.
11. Agregar otro cable de conexión entre puertos troncales de S1 y S2. **Esto creara una redundancia de conexión entre ambos dispositivos.**
12. Retornar a PC0 y enviar nuevamente el ping hacia el host conectado a S2.  
¿Se logró la comunicación?, ¿Que está sucediendo entre ambos switch y entre los host?
13. Se ha generado un **bucle de capa 2**, debido a que la trama de broadcast ARP de host emisor se retransmite indefinidamente entre ambos switch continuamente, no permitiendo determinar la ubicación del host destino y ocasionando la caída de la comunicación en la red.
14. Elimine uno de los cables troncales y vera que finaliza el bucle capa 2.
15. Otra situación que desencadena un bucle de capa 2 es la descrita a continuación.
16. Crear un enlace redundante entre S2 y S3, conectando 2 parejas de puertos troncales entre ambos dispositivos.
17. Conecte al último host (PC2) hacia un puerto de acceso de S3.  
De nuevo, ocurre un bucle de capa 2 entre S2 y S3; incluso afecta a S1, bloqueando finalmente a toda la red.  
¿Pero quién ha generado la trama de difusión inicial para que se desencadenara este bucle?
18. El host PC2 ha sido el responsable del envío automático de tramas ARP, porque “envía solicitudes de eco dirigidos a otro host de la red con su propia IP asignada”. A este se llama **“Descubrimiento de host”**.
19. El principio de “descubrimiento automático de host” permite a cualquier equipo de red con capacidad de configuración de IP, determinar si la IP de Host que se le esta asignando, ya está siendo utilizada por otro equipo en la red a la cual se conecta físicamente, evitando direcciones duplicadas en el dominio de broadcast.
20. Finalice el bucle infinito de reenvío de capa 2, quitando uno de los cables troncales entre S2 y S3.
21. Restaurar el enlace troncal redundante entre S1 y S2, así como entre S2 y S3.

## Parte I: Utilizando protocolo STP para administrar enlaces redundantes entre switch

22. Hacer una copia de la simulación bajo el nombre **Parte2\_Switch\_conSTP**
23. Reinicie a todos los dispositivos de la red, dando clic en botón “Power Cycle Devices” (ubicado sobre la lista de los nuevos dispositivos a incluir en la simulación).
24. Observe que se produce el bucle de capa 2 justamente luego del reinicio del IOS de los Switch, ocasionado por las pruebas de “descubrimiento de host” que hace cada PC para saber si posee una dirección IP duplicada en la red.
25. Desconecte solamente a todos los diferentes enlaces troncales entre los switch. No desconecte a ninguno de los host!!
26. Ahora comenzara el análisis de funcionamiento del protocolo STP
27. Ingresar al modo privilegiado de S1 y observe el estado del protocolo STP con el comando: **show spanning-tree active**
28. Este indicara que no hay ninguna instancia de STP existente funcionando en este switch y en el resto de switch.
29. Ingresar al Modo Global de S1 y levantar una instancia del protocolo STP para la vlan 1 (predeterminada), ejecutando al comando: **spanning-tree vlan 1**
30. Retorne al modo privilegiado y ejecute al comando: do show spanning-tree active.  
Confirme los parámetros de la instancia STP activada. Observe un ejemplo de un resultado devuelto a continuación:

```
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0030.F2AA.CA02
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0030.F2AA.CA02
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 |
|-------|------|--------|-------|-----|

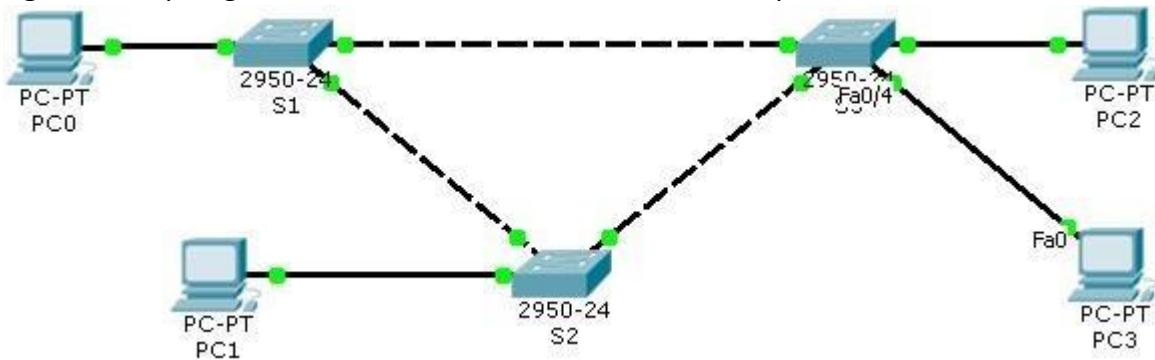
31. Compare el ejemplo anterior con los resultados devueltos por STP en su switch S1, específicamente en los datos resaltados en el ejemplo anterior. Observar que:
- STP ha definido 2 identificadores, el **Root ID** (el Id de puente Raíz) y el **Bridge ID**.
  - Cada uno de los identificadores está formado por un id de prioridad (con valor predeterminado de **32769**) y una dirección MAC (en este resultado, la MAC **0030.F2AA.CA02**)
  - El Root ID indica cual switch es el "Puente raíz". Como ambos identificadores valen exactamente lo mismo, STP indica que "este mismo switch es el Puente Raíz": **This bridge is the root**.
32. Ejecute al comando `show interface vlan 1`. Vera las configuraciones de esta interfaz lógica de la vlan 1.
33. Localice el parámetro (address is) y compare esta MAC con el parámetro Address asignado tanto al Root ID como a Bridge ID de STP.
34. Ingrese al modo configuración global de S2 y levante una instancia de STP para la vlan 1. Luego ejecutar comando `do show spanning-tree active`, para observar los valores de sus identificadores Raíz y de Puente.
35. Repetir el paso anterior para S3.
36. Finalmente, anote de cada switch a los parámetros Root ID y Bridge ID de STP en la Tabla 1

**Tabla 1:** Lista de ID de puentes raíz e ID puente de los 3 switch con STP (sin conectar aun)

| Switch con STP                | S1 | S2 | S3 |
|-------------------------------|----|----|----|
| ID Root                       |    |    |    |
| Prioridad                     |    |    |    |
| MAC de switch                 |    |    |    |
| ¿Es el puente Raíz? (si / no) |    |    |    |
| Bridge ID                     |    |    |    |
| Prioridad                     |    |    |    |
| MAC de switch                 |    |    |    |

37. Conectar a los switch entre si según la topología de red descrita en la Imagen 5.1.  
 Guarde los cambios de configuración en el archivo `startup-config` de cada switch y reinicie la topología completa de la red.

**Imagen 5.1:** Topología con conexión redundante entre Switch por medio de enlaces troncales



38. Observe que esta vez, ya no se genera un bucle infinito, debido a que los switch tienen configurado STP y ellos iniciaran el intercambiando de tramas BPDU para elegir al Switch Puente Raíz (Root bridge).

39. Luego de unos 40-50 seg., el STA habrá elegido al switch que funcionara como Puente Raíz.

40. Para continuar, evalúe el funcionamiento del algoritmo STA usado por STP para elegir al puente Raíz de una topología.

41. El algoritmo STA establece 2 criterios/reglas para seleccionar a puente raíz entre todos 2 o más switch con STP:

1. El switch con prioridad menor se convierte en raíz
2. Ante 2 Switch con igual prioridad en su Bridge ID, se selecciona como Puente raíz al switch que posea la MAC con menor valor.

42. Con base a las reglas definidas en el paso anterior, analice cuidadosamente los datos recopilados en la Tabla 1 y determine:

¿Cuál de los 3 switch (S1, S2, S3) de esta topología se ha convertido en Puente raíz?

43. Ejecute el comando show spanning-tree en el switch que usted eligió en el paso anterior y confirme si es el puente raíz elegido bajo el algoritmo STA.

44. Ejecute el comando del paso anterior en el resto de switch.

45. Evalúe los resultados en cada switch para determinar las funciones (roles) de c/u de los puertos troncales conectados, mostrados al final.

+ La función (**Role**) de un puerto puede ser:

Puerto Raíz (**Root**), Puerto Designado (**Desg**), Puerto no designado (también llamado Alternativo: **Altn**)

+ Luego, según el rol asignado a cada puerto, determine su estado (**Sts**), que puede ser reenvío (**FWD**) o bloqueado (**BLK**)

46. Solamente los puertos en estado de reenvío (FWD) permitirán la transmisión de tramas, permitiendo así bloquear lógicamente los enlaces redundantes y evitar los bucles de capa 2.
47. Guardar los cambios en la configuración de inicio de cada switch.

### **Parte III: Alterando la selección de puente raíz dentro del algoritmo STA**

48. Guarde los últimos cambios y luego realice una copia de la simulación actual bajo el nombre **Parte3\_EleccionPuenteRaiz**.
49. Se procederá a la alteración sobre la selección del puente raíz por medio de 2 métodos diferentes:

#### **Método 1: Ejecutando comando spanning-tree vlan numvlan priority ValorPrioridad**

50. En este ejemplo, hará que S3 siempre sea elegido como Puente raíz y a S2 como puente secundario.
51. Ingresar a modo configuración global de S3 y asignar una prioridad de 4096 con comando: **spanning-tree vlan 1 priority 4096**
52. Luego, desde modo configuración global, ejecutar en S2 al comando: **spanning-tree vlan 1 priority 8192**

Y desde S1, ejecute al comando **spanning-tree vlan 1 priority 20480**.

53. Observe el cambio de funcionamiento de los puertos troncales (reenvío o bloqueo) entre los switch cuando nuevamente determinan entre ellos al nuevo Puente raíz de acuerdo a la modificación de las prioridades anteriores.
54. Luego de unos 35 seg. , visualice el estado de STP en S3, ejecutando el comando **show spanningtree active**  
Confirme que este switch S3 sea el nuevo puente raíz.
55. Guarde las últimas configuraciones de comandos en cada switch y luego, cierre el archivo de simulación actual.

## Método 2: Uso comando: **spanning-tree vlan numvaln root primary/secondary**

56. Vuelva a cargar el archivo final de la parte 2 (Parte2\_Switch\_conSTP) y haga una copia del mismo, bajo el nombre **Parte3\_Eleccion2PuenteRaiz**

57. El 2do método de alterar la prioridad para elegir al puente raíz de STP es con los comandos:

**spanning-tree vlan 1 root primary**

**spanning-tree vlan 1 root secondary**

58. Ahora se establecerá nuevamente que switch S3 de la topología sea elegido como puente raíz

59. Para ello, desde modo configuración global de S3 ejecute comando **spanning-tree vlan 1 root primary**

60. Y luego S2 será el puente raíz alternativo ejecutando en el mismo al comando: **spanning-tree vlan 1 root secondary**

61. Espere 40 seg. , para que se dé por finalizado otro proceso de elección entre los switch y sea elegido S3 como Puente raíz.

62. Confirme la elección desde el modo privilegiado de S3, ejecutando el comando **show spanningtree active**

63. Guardar cambios en la configuración y cerrar la simulación.

## IV. ANALISIS DE RESULTADOS

1. Prepare una nueva simulación de red.
2. En esta nueva simulación, ubique un total de 5 switch **2950-24**. Seleccione a 2 de ellos, para cambiar sus nombres por **raiz1** y **raiz2**, respectivamente. El resto de switch se llamaran **acceso1**, **acceso2** y **acceso3**.
3. Haga las conexiones necesarias para que **raíz1** se conecte al resto de switch, utilizando un puerto diferente. Haga lo mismo con **raíz2**.
4. A cada switch de acceso, agregue y conecte un total de 2 host diferentes. Configúrelos bajo la red ip **172.16.0.0 /24-**
5. Finalmente, haga las configuraciones necesarias (con el método de modificar prioridades) para que bajo STP, el switch **raíz1** sea elegido como root y el switch **raíz2** debe ser el switch designado (de respaldo).

6. Guarde los cambios de configuración en el IOS de cada switch y reinicie la simulación.
7. Realice pruebas de comunicación entre los diferentes host.



## UNIVERSIDAD AUTONOMA DE CHIHUAHUA FACULTAD DE INGENIERÍA

**enero-junio  
2023**

### **GUIA DE LABORATORIO #6**

**Nombre de la Practica:** Subneteo y VLSM  
**Lugar de Ejecución:** Laboratorio de Redes  
**Tiempo Estimado:** 2 horas y 30 minutos  
**MATERIA:** Redes

### **I. OBJETIVOS**

Que el estudiante:

- Desarrolle los cálculos del Subneteo IP requerido en una topología de red lógica
- Ejecute las configuraciones de direccionamiento ip (gateway) en un Router • Ejecute las conexiones de routers y configuraciones de los IOS con equipo real.

### **II. INTRODUCCION TEORICA**

#### **¿Qué es Subneteo de red?**

Es un procedimiento que permite dividir a una red primaria IPv4 en una serie de subredes, de tal forma que cada una de ellas funcione a nivel de envío y recepción de paquetes, como una red individual, aunque todas pertenezcan a la misma red principal y, por lo tanto, al mismo dominio de difusión original.

#### **¿Por qué realizar un Subneteo?**

Cuando trabajamos con una red pequeña no encontramos muchos problemas para configurar el rango de direcciones IPv4 para conseguir un rendimiento óptimo.

Pero a medida que se van agregando Host a la red, el desempeño empieza a verse afectado. Esto puede ser corregido, en parte, segmentando la red con switches, reduciendo los Dominios de colisión (host que comparten el mismo medio) enviando las tramas solo al segmento correcto.

Pero aunque se reducen las colisiones con tomar estas medidas, si se continúa aumentando el número de host, aumentan también los envíos de broadcast (Envío de paquetes a todos los dispositivos de la

red). Lo que afecta considerablemente el desempeño de la red. Esto se debe a que los Switches solo segmentan a nivel de MAC Address y los envíos de broadcast son a nivel de red 255.255.255.255. ¡¡Es aquí donde el Subneteo nos ayuda!!

1 / 13

Subneteando la red tendremos, en su conjunto, una sola IP address dividida en varias subredes más pequeñas perfectamente diferenciadas, consiguiendo un mayor control y reduciendo el congestionamiento por los broadcasts. A continuación, se ofrecen una serie de conceptos relacionados a este proceso de Subneteo.

### **Subred**

Es la agrupación física o lógica de dispositivos de red que conforman a una sección de un sistema autónomo o como tal puede ser un sistema autónomo.

### **Máscara de red**

Denominado también **Prefijo de red extendida**, es el número que acompaña a una dirección IP, indicando los bits totales ocupados para la parte de red, que deben ser comunes para todos los clientes de una Red IP.

### **Subneteo IP**

La función del Subneteo o Subnetting es dividir una red IP física en subredes lógicas (redes más pequeñas) para que cada una de estas trabaje a nivel envío y recepción de paquetes como una red individual, aunque todas pertenezcan a la misma red física y al mismo dominio.

El Subneteo permite una mejor administración, control del tráfico y seguridad I segmentar la red por función. También, mejora la performance de la red al reducir el tráfico de broadcast de nuestra red. Como desventaja, su implementación desperdicia muchas direcciones, sobre todo en los enlaces seriales entre routers.

### **Calcular la Cantidad de Subredes y Hosts por Subred**

La **Cantidad de Subredes** es igual a  $2^N$ , donde "N" es el número de bits "robados" a la porción de Host.

Y la Cantidad de Hosts x Subred es igual a  $2^M - 2$ , en donde "M" es el número de bits disponible en la porción de host y "-2" es debido a que toda subred debe tener una ip reservada para su ID de red y otra ip para su propia dirección de broadcast.

### Convertir Bits en Números Decimales

Como sería casi imposible trabajar con direcciones de 32 bits, es necesario convertirlas en números decimales.

En el proceso de conversión cada bit (en un intervalo de 8 bits) de una dirección IP, cuando este vale "1" tiene un valor de "2" elevado a la posición que ocupa ese bit en el octeto y finalmente se suman los resultados.

En la Tabla 1 se muestra el valor posicional de cada bit dentro de un Byte y 3 ejemplos diferentes para poder aplicar este método de conversión rápida de binario a decimal.

La combinación de 8 bits permite un total de 256 combinaciones posibles que cubre todo el rango de numeración decimal desde el 0 (00000000) hasta el 255 (11111111).

**Tabla 1:** Posiciones binarias y su valor decimal.

| Posición y Valor de los Bits |       |       |       |       |       |       |       |       |
|------------------------------|-------|-------|-------|-------|-------|-------|-------|-------|
|                              | $2^7$ | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |
| Binario                      | 1     | 0     | 0     | 0     | 0     | 0     | 0     | 0     |
| Decimal                      | 128   | 0     | 0     | 0     | 0     | 0     | 0     | 0     |
| Binario                      | 0     | 1     | 0     | 0     | 0     | 0     | 0     | 0     |
| Decimal                      | 0     | 64    | 0     | 0     | 0     | 0     | 0     | 0     |
| Binario                      | 0     | 0     | 1     | 0     | 0     | 0     | 0     | 0     |
| Decimal                      | 0     | 0     | 32    | 0     | 0     | 0     | 0     | 0     |
| Binario                      | 0     | 0     | 0     | 1     | 0     | 0     | 0     | 0     |
| Decimal                      | 0     | 0     | 0     | 16    | 0     | 0     | 0     | 0     |
| Binario                      | 0     | 0     | 0     | 0     | 1     | 0     | 0     | 0     |
| Decimal                      | 0     | 0     | 0     | 0     | 8     | 0     | 0     | 0     |
| Binario                      | 0     | 0     | 0     | 0     | 0     | 1     | 0     | 0     |
| Decimal                      | 0     | 0     | 0     | 0     | 0     | 4     | 0     | 0     |
| Binario                      | 0     | 0     | 0     | 0     | 0     | 0     | 1     | 0     |
| Decimal                      | 0     | 0     | 0     | 0     | 0     | 0     | 2     | 0     |
| Binario                      | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 1     |
| Decimal                      | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 1     |

|       |       |       |       |       |       |       |       |   |
|-------|-------|-------|-------|-------|-------|-------|-------|---|
| 1     | 1     | 1     | 1     | 1     | 1     | 1     | 1     | 1 |
| $2^7$ | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |   |
| 128   | +     | 64    | +     | 32    | +     | 16    | +     | 8 |
| = 128 |       |       |       |       |       |       |       |   |
| + 64  |       |       |       |       |       |       |       |   |
| = 192 |       |       |       |       |       |       |       |   |
| 1     | 1     | 0     | 0     | 0     | 0     | 0     | 0     | 0 |
| $2^7$ | $2^6$ |       |       |       |       |       |       |   |
| 128   | +     | 64    |       |       |       |       |       |   |
| = 192 |       |       |       |       |       |       |       |   |
| 1     | 0     | 1     | 0     | 1     | 1     | 0     | 0     | 0 |
| $2^7$ | $2^6$ |       | $2^5$ | $2^4$ | $2^3$ | $2^2$ |       |   |
| 128   | +     | 32    | +     | 8     | +     | 4     |       |   |
| = 172 |       |       |       |       |       |       |       |   |

Ejemplos de uso método sumas de potencias de 2  
Para convertir byte de binario a decimal

### Ejemplos de aplicación de Subneteo

#### 1. Ejemplo de Subneteo de IP CLASE B

Dada la red Clase B 132.18.0.0/16 se nos pide que mediante Subneteo obtengamos un mínimo de 50 subredes y 1000 hosts por subred. El Subneteo se realizará en 3 pasos:

**Paso 1:** Adaptar la Máscara de Red por Defecto a la cantidad de Subredes.

La máscara por defecto para la red 132.18.0.0 es >>

Usando la fórmula  $2^N - 2$ , donde N es la cantidad de bits que debe prestar a la porción de host, se adapta la máscara de red por defecto a la máscara de subred.

En este caso particular  $2^N = 50$ , ya que se requieren crear 50 subredes. Este cálculo indica que se prestan 6 bits (los más significativos) a la porción de host para hacer 50 subredes o más y que el total de subredes útiles va a ser de 64, es decir que van a quedar 14 para uso futuro.

|       |       | Porción de Red  |   | Porción de Host |   |                 |   |          |                     |
|-------|-------|-----------------|---|-----------------|---|-----------------|---|----------|---------------------|
|       |       | 255             | . | 255             | . | 0               | . | 0        |                     |
|       |       | 11111111        | . | 11111111        | . | 00000000        | . | 00000000 | = /16               |
| $2^N$ | Redes | Máscara Binario |   |                 |   | Máscara Decimal |   |          |                     |
| $2^5$ | 32    | 1111111         | . | 1111111         | . | 11111000        | . | 00000000 | 255 . 255 . 248 . 0 |
| $2^6$ | 64    | 1111111         | . | 1111111         | . | 1111100         | . | 00000000 | 255 . 255 . 252 . 0 |
| $2^7$ | 128   | 1111111         | . | 1111111         | . | 1111110         | . | 00000000 | 255 . 255 . 254 . 0 |

|  |  | Porción de Red |     | Porción de Host |     |          |   |          |       |
|--|--|----------------|-----|-----------------|-----|----------|---|----------|-------|
|  |  | 255            | 255 | .               | 252 | .        | 0 |          |       |
|  |  | 11111111       | .   | 11111111        | .   | 11111100 | . | 00000000 | = /22 |
|  |  |                |     |                 |     | 4        |   |          |       |
|  |  |                |     |                 |     | 8        |   |          |       |
|  |  |                |     |                 |     | 16       |   |          |       |
|  |  |                |     |                 |     | 32       |   |          |       |
|  |  |                |     |                 |     | 64       |   |          |       |
|  |  |                |     |                 |     | 128      |   |          |       |
|  |  |                |     |                 |     | 252      |   |          |       |

Entonces a la máscara Clase B por defecto se le agregan los 6 bits prestados, reemplazándolos por "1" y obtiene la máscara adaptada **255.255.252.0** o en notación de red: **/22**

**Paso 2:** Obtener Cantidad de Hosts por Subred (2) Una vez que determina la máscara de subred, se trabajara con la dirección IP de la red.

En este caso con la porción de host (fondo gris)

|          |  | Porción de Red |   | Porción de Host |   |          |   |          |  |
|----------|--|----------------|---|-----------------|---|----------|---|----------|--|
|          |  | 132            | . | 18              | . | 0        | . | 0        |  |
|          |  | 10000100       | . | 00010010        | . | 00000000 | . | 00000000 |  |
| Subredes |  |                |   |                 |   |          |   |          |  |

El ejercicio solicita una cantidad específica de 1000 hosts por subred. Para verificar que sea posible obtenerlos con la nueva máscara, se utiliza la fórmula  $2^M - 2$ , donde M es el número de bits "0" disponibles en la porción de host y - 2 es debido a que la primer y última dirección IP de la subred no son utilizables por ser la dirección de la subred y broadcast respectivamente.  $2^{10} - 2 = 1022$  Hosts por subred.

Los 10 bits "0" de la porción de host (fondo gris) son los que más adelante se modifican según se vaya asignando los hosts a las subredes.

**Paso 3:** Obtener Rango de Subredes

Para obtener las subredes se trabaja con la porción de red de la dirección IP de la red, más específicamente con la parte de la porción de red que se modifica en la máscara de red, pero esta vez en la dirección IP.

|          |  | Porción de Red |   | Porción de Host |   |          |   |          |  |
|----------|--|----------------|---|-----------------|---|----------|---|----------|--|
|          |  | 132            | . | 18              | . | 0        | . | 0        |  |
|          |  | 10000100       | . | 00010010        | . | 00000000 | . | 00000000 |  |
| Subredes |  |                |   |                 |   |          |   |          |  |

Recuerde que a la máscara de red con anterioridad se le agregaron 6 bits en el tercer octeto, entonces van a tener que modificar esos mismos bits pero en la dirección IP de la red (fondo negro).

Para obtener el rango de subredes (llamado también el “salto” que habrá entre las ip de subred) existen varios métodos.

El método más sencillo para determinar el “salto” es restarle a 256 el número de la máscara de subred. En este caso sería:  $256 - 252 = 4$ , entonces 4 va a ser el rango entre cada subred.

En el gráfico solo muestran las primeras 10 subredes y las últimas 5 subredes posibles del rango.

| Nº de Subred | Rango IP *   |                | Hosts Asignables x Subred |
|--------------|--------------|----------------|---------------------------|
|              | Desde        | Hasta          |                           |
| 1            | 132.18.0.0   | 132.18.3.255   | 1.022                     |
| 2            | 132.18.4.0   | 132.18.7.255   | 1.022                     |
| 3            | 132.18.8.0   | 132.18.11.255  | 1.022                     |
| 4            | 132.18.12.0  | 132.18.15.255  | 1.022                     |
| 5            | 132.18.16.0  | 132.18.19.255  | 1.022                     |
| ...          |              |                |                           |
| 60           | 132.18.236.0 | 132.18.239.255 | 1.022                     |
| 61           | 132.18.240.0 | 132.18.243.255 | 1.022                     |
| 62           | 132.18.244.0 | 132.18.247.255 | 1.022                     |
| 63           | 132.18.248.0 | 132.18.251.255 | 1.022                     |
| 64           | 132.18.252.0 | 132.18.255.255 | 1.022                     |

\* La primera y la última dirección IP de cada Subred no se asignan ya que contienen la dirección de red y broadcast de la Subred.

### Subneteo de máscara de subred de longitud variable (VLSM)

El Subneteo normal (CIDR) visto anteriormente es apropiado cuando las capacidades de host de las subredes requeridas son casi constantes o no interesa cuánto espacio de direccionamiento se debe de usar en cada subred.

Las deficiencias de este Subneteo CIDR comienzan a detectarse cuando se presenta una varianza en la capacidad de host de las subredes solicitadas para una topología.

Como respuesta a este problema se propone una variación del método, que consiste en “**dividir a una subred en otras subredes y cualquiera de estas nuevas subredes en otras y así sucesivamente... para lograr un mejor aprovechamiento del espacio de direccionamiento de host por subred**”.

A este nuevo método se le conoce como **Subneteo con Máscara de subred de longitud variable (VLSM)**.

Observe su aplicación en el siguiente ejemplo.

### Ejemplo de aplicación de VLSM

Elabore los cálculos de subneteo ip con la red inicial **200.0.0.0 / 24** para cubrir apropiadamente el siguiente Esquema de direccionamiento de redes:

| #Red                                                          | Total host mínimos     |
|---------------------------------------------------------------|------------------------|
| Red A                                                         | 16 host                |
| Red B                                                         | 35 host                |
| Red C                                                         | 20 host                |
| Enlace 1, Enlace 2, Enlace 3<br>(Para enlaces entre router's) | 2 host por cada enlace |

1. Se ordena el esquema direccionamiento de redes anterior por cantidad de host requerida, calculando los bits de host que necesitaría cada subred cuando se implemente:

| #Red     | Total host mínimos | Bit para host requeridos |
|----------|--------------------|--------------------------|
| Red B    | $35+3 = 33$ host   | 6                        |
| Red C    | $20+3 = 23$ host   | 5                        |
| Red A    | $16+3 = 19$ host   | 5                        |
| Enlace 1 | $2+2 = 4$ host     | 2                        |
| Enlace 2 | $2+2 = 4$ host     | 2                        |
| Enlace 3 | $2+2 = 4$ host     | 2                        |

**Muy importante:**

- Observe que se ha sumado 3 direcciones ip a cada red de host, porque se cuenta las ip reservadas: id de red, id de broadcast e ip de puerta de enlace/ Gateway.
  - En cambio, a las redes de enlace solo se suman 2 direcciones, porque aquí no se requiere ip de gateway
2. Inicia el **subneteo 1**, dividiendo la ip red inicial (**200.0.0.0 / 24**) en subredes para cubrir a las redes que requieren mayor cantidad de host (la Red B) según la tabla anterior.
3. Calcula la máscara de subred, de la siguiente forma. Compare a la derecha la forma matemática equivalente más rápida para calcular este valor:

|                                                                                                                                                                          |                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br><b>Máscara de subred:</b><br><b>11111111. 11111111. 11111111. 11000000</b><br><b>255.255.255.192 (notación de octetos)</b> O<br>también <b>/26 (notación de red)</b> | <b>Máscara de subred</b><br>$= /32 \text{ bits} - (\text{total bit host por subred})$<br>$= /32 - 6$<br>$/26 \text{ (notación de red)}$<br>O también en notación de octetos<br>$/26 = /8./8./8./2$<br><b>255.255.255.192 (notación de octetos)</b> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

4. Determina los límites de cada subred ip, gracias al “Salto o cambio entre subredes”. Para ello, extrae de la máscara de subred (255.255.255.**192**) al byte donde finalizan los bits de subred, en este caso a **192**. El salto se obtendrá de restar este byte a 256, así: **Salto entre subredes = 256 – 192 = +64**

5. Dado que 2 bits de host se convirtieron a bits de subred, se obtendrán ( $2^2 = 4$  subredes), las cuales se obtienen aplicando el “Salto” anterior (**+64**). Y además, se indica la red que se asignara c/u.

| #subred | Subneteo 1 Ip red    | Asignada a   |
|---------|----------------------|--------------|
| 1       | <b>200.0.0.0 /26</b> | <b>Red B</b> |
| 2       | 200.0.0.64 /26       | Sin Asignar  |
| 3       | 200.0.0.128 /26      | Sin Asignar  |
| 4       | 200.0.0.192 /26      | Sin Asignar  |

6. La red original se segmento en 4 bloques de direcciones, de las cuales se reservó la subred #1 a la Red B.
7. **Subneteo 2:** para continuar, se requieren 2 subredes para cubrir a las redes C y A (de **5 bits** de host c/subred). Se tomara la subred #1 (**200.0.0.64 / 26**) para volver a subnetear.
8. Primero se calcula la máscara de subred 2 con la fórmula:

$$\begin{aligned} \text{Mascara2} &= /32 \text{ bits} - (\text{total bit host de subneteo2}) \\ &= /32 - 5 \end{aligned}$$

$$\text{Mascara2} = /27 \text{ o también } 255.255.255.\textcolor{red}{224}$$

9. Determina el “salto 2” de este nuevo subneteo, tomando el byte de la nueva mascara, así: **Salto2 = 256 – 224 = +32**
10. De la máscara del subneteo 1 (**/26**) a la máscara del subneteo 2 (**/27**), solo un bit se convierte en bit de subred, por lo que solo se generan ( $2^1 = 2$  subredes). Observe el nuevo subneteo en la tabla de direccionamiento:

| #subred | Subneteo 1 Ip red    | Subneteo 2 Ip red     | Asignada a   |
|---------|----------------------|-----------------------|--------------|
| 1       | <b>200.0.0.0 /26</b> |                       | <b>Red B</b> |
| 2       | 200.0.0.64 /26       | <b>200.0.0.64 /27</b> | <b>Red C</b> |
|         |                      | <b>200.0.0.96 /27</b> | <b>Red A</b> |
| 3       | 200.0.0.128 /26      |                       | Sin Asignar  |
| 4       | 200.0.0.192 /26      |                       | Sin Asignar  |

11. Ya solo quedan 2 espacios de direcciones disponibles. Utilizará el espacio de la subred (**200.0.0.128 /26**) para cubrir las 3 subredes para enlaces entre los router.

12. **Subneteo 3:** Calcula la máscara de subred 3, así:

$$\begin{aligned} \text{Máscara subred } 3 &= /32 - 2 \\ &= /30 \text{ (notación de red)} \text{ o también } 255.255.255.\textcolor{red}{252} \text{ (notación de bytes)} \end{aligned}$$

13. Calcula el Salto 3, con la fórmula:

$$\text{Salto3} = 256 - \textcolor{red}{252} = +4$$

14. De la máscara (/26) a la máscara (/30), hay 4 bit convertidos a bit de subred, por lo que se generaran ( $2^4 = 16$  subredes), de las cuales, solo se asignaran a 3 de ellas, dejando al resto en reserva, así:

| #subred | Subneteo 1 Ip red    | Subneteo 2 Ip red     | Subneteo 3 Ip red      | Asignada a      |
|---------|----------------------|-----------------------|------------------------|-----------------|
| 1       | <b>200.0.0.0 /26</b> |                       |                        | <i>Red B</i>    |
| 2       | 200.0.0.64 /26       | <b>200.0.0.64 /27</b> |                        | <i>Red C</i>    |
|         |                      | <b>200.0.0.96 /27</b> |                        | <i>Red A</i>    |
| 3       | 200.0.0.128 /26      |                       | <b>200.0.0.128 /30</b> | <i>Enlace 1</i> |
|         |                      |                       | <b>200.0.0.132 /30</b> | <i>Enlace 2</i> |
|         |                      |                       | <b>200.0.0.136 /30</b> | <i>Enlace 3</i> |
|         |                      |                       | 200.0.0.140 /30        | Sin Asignar     |
|         |                      |                       | ...                    |                 |
|         |                      |                       | 200.0.0.188 /30        | Sin Asignar     |
| 4       | 200.0.0.192 /26      |                       |                        | Sin Asignar     |

15. Observe que del espacio de direccionamiento ip inicial (200.0.0.0 /24), ya solamente quedan disponibles 5 bloques de ip para enlace entre router (de la 200.0.0.140/30 a la 200.0.0.188/30) y un bloque (200.0.0.192 /26); este último podría ser dividido en el futuro gracias al VLSM.

### **III. MATERIALES Y EQUIPO**

Para la realización de la guía de práctica se requerirá lo siguiente:

| No. | Requerimiento                                           | Cantidad |
|-----|---------------------------------------------------------|----------|
| 1   | Guía #06 de Redes                                       | 1        |
| 2   | Software “Simulador Packet Tracer 6.2 by Cisco Systems” | 1        |
|     |                                                         |          |



## IV. PROCEDIMIENTO

### **Parte 1: Desarrollando proceso de Subneteo**

1. Desarrolle junto a su instructor el siguiente ejercicio de Subneteo ip.

Seleccione una ip base de clase C para el cálculo.

“Divida su espacio de direccionamiento en 3 segmentos, para configurar una red de 20 host, otra red de 25 host y una más de 16 host”

2. Luego, de igual forma, solucione el siguiente ejercicio de Subneteo ip. Seleccione una ip base de clase C para el cálculo.

“Divida su espacio de direccionamiento en 3 segmentos, para configurar una red de 50 host, otra red de 24 host y una más de 80 host”

### **Parte 2: Definiendo un Dominios de Broadcast**

3. Seleccione una IP de red Clase B y anótela a continuación:

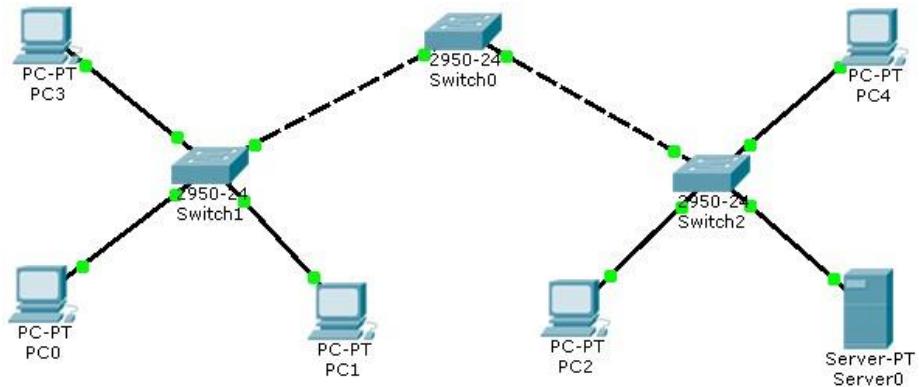
De esta IP seleccionada, determine y anote los parámetros solicitados en la Tabla 2.

**Tabla 2:** Parámetros de la ip red seleccionada

| IP de red base =           |   | <i>Rango de IP para host</i> |  |
|----------------------------|---|------------------------------|--|
| <i>Mascara de subred</i>   |   | <i>IP inicial =</i>          |  |
| <i>Notación de octeto=</i> |   | <i>IP final =</i>            |  |
| <i>Notación de red =</i>   | / |                              |  |
|                            |   | <i>IP broadcast =</i>        |  |

4. Ejecute la aplicación Cisco Packet Tracer, para luego crear la topología lógica inicial mostrada en la figura 6.1.

**Figura 6.1:** Topología lógica (un único dominio de difusión)



5. Ahora configurada un único dominio de difusión/broadcast. Para cada cliente y servidor, seleccione ip de host aleatorias dentro del rango de ip's calculado en la Tabla 2. No altere la máscara predeterminada y no asigne aun la ip de gateway.
6. Haga pruebas de comunicación entre 2 parejas de host aleatorios y confirme que se logra exitosamente.
7. Expanda la topología, incluyendo otro switch, así como otras 2 PC y un nuevo Server. Conecte un puerto de este switch al switch principal (el switch que actualmente conecta a los otros 2 switch). Configure el protocolo ip de estos 3 nuevos equipos.

### Parte 3: Dividiendo a un dominio de Broadcast (Subneteo IP)

8. Guarde la simulación bajo el nombre **Guia4\_subneteo**.
9. A continuación, hará los cálculos para dividir a la ip red en subredes ip y dividir el dominio de difusión en segmentos más pequeños.
10. Solicite a su instructor el criterio (A o B) y la cantidad (de subredes o de host/subred, respectivamente) que usted deberá aplicar sobre su ip red para los cálculos de Subneteo:

| Criterio                | descripción              | Total a calcular |
|-------------------------|--------------------------|------------------|
| <input type="radio"/> A | Total de subredes        |                  |
| <input type="radio"/> B | Total de host por subred |                  |

**Tabla 2:** Esquema de Subneteo a utilizar en procedimiento

11. De acuerdo al criterio asignado por su instructor, proceda a realizar los cálculos de Subneteo apropiados y luego llene la Tabla 3 con los parámetros de las IP-red solicitadas ahí.
12. Modifique el direccionamiento ip (ip y mascara de red) de los host conectados al primer switch con direcciones de host de la Subred A (Ver Tabla 3).
13. Repita el paso anterior, pero con los host y server del 2do switch, asignando direcciones de la Subred B.
14. Y de igual, asigne direcciones de la Subred C a los host y server del ultimo switch
15. Con las herramientas de dibujo de Packet tracer, documente su topología, con elipses limitando a los host de cada subred diferente, indicando también la ip red y mascara de red.
16. Elija aleatoriamente a un host y desde el mismo, haga pruebas de ping a un host de su misma subred y a otros de otras subredes configuradas en la topología.  
De acuerdo a las pruebas, ¿Cuáles comunicaciones resultaron exitosas y cuáles fallaron?, justifica tu respuesta.
17. Compruebe sus conclusiones, haciendo pruebas desde un server hacia host de la misma y de diferente subred.

**Subneteo general:**

IP Red inicial: \_\_\_\_\_

Criterio seleccionado (A o B) : \_\_\_\_\_ Total de(subredes o totalhostxSubred): \_\_\_\_\_ Total

bit red: \_\_\_\_\_ Total bit subred: \_\_\_\_\_ Total bit de host: \_\_\_\_\_

Mascara subred en formato ...

... decimal: \_\_\_\_\_ ... de Notación de barra / \_\_\_\_\_ Salto

entre subredes: \_\_\_\_\_

| <b>Subred</b> | <b>#subred</b> | <b>ip red</b> | <b>Ip broadcast</b> | <b>ip host inicial - final</b> |
|---------------|----------------|---------------|---------------------|--------------------------------|
| A             | Tercera subred |               |                     |                                |
| B             | Sexta subred   |               |                     |                                |

|   |                     |  |  |  |
|---|---------------------|--|--|--|
| C | Penúltima<br>subred |  |  |  |
| D | Ultima subred       |  |  |  |

**Tabla 3:** parámetros de subredes a utilizar en procedimiento**Parte 4: Comunicación entre subredes IP**

18. Guarde los cambios en su simulación. Haga una copia de la misma bajo el nombre **Guia4\_Enrutamiento**.
19. En esta nueva simulación, borre el switch central (que conecta solamente al resto de switch)
20. Agregue un router de la serie que usted desee, pero modifíquelo físicamente de tal forma que posea 4 interfaces FastEthernet y 2 interfaces Serials.
21. Conecte el puerto fa0/0 del router a un puerto libre del switch que integra a la Subred A. Ingrese a la configuración de esta interfaz del router y asigne ahí a la 1er ip de host de la subred A, así como su máscara de subred. Active la interface y espere a que el enlace con el switch se active completamente.
22. Desde uno de los host de la Subred A, envíe un ping a la ip asignada a la interface de conexión con el router.  
Si se obtiene eco, significa que alcanza al router; sino es así, no continúe con el procedimiento hasta corregir el problema de comunicación.
23. Repita los 2 pasos anteriores para conectar la 2da interface FastEthernet del router al switch de la subred B y configurarla con la 1er ip para host de la subred B.  
Compruebe la comunicación de un host de esta subred B con la ip asignada a su interface de conexión con el router.
24. De manera similar, integre la subred C al router y haga las pruebas de comunicación.
25. Seleccione un host de la Subred A y otro de la subred B. Haga pruebas de ping entre ambos. ¿Se logra la comunicación entre subredes?
26. Para que la comunicación anterior sea posible, ingrese al host de la Subred A y configure en su IP Gateway a la ip asignada a la interface fa0/0 del router (con el cual accede a la Subred A).
27. Desarrolle el paso anterior en el host de la subred B, pero asignando en su ip de Gateway a la ip de la interface del router que se conecta a la Subred B.

28. De la demostración anterior, se puede deducir el siguiente principio de enrutamiento:  
 “La ip asignada a la interface de un router, se convertirá en la ip Gateway de todos y cada uno de los host de la subred a la cual conecta esa interface”.
29. Aplique el principio anterior, asignando la ip de Gateway apropiada en el protocolo IP de cada host y server de toda la topología, de acuerdo a la subred a la cual se conecte cada terminal.
30. Seleccione un host aleatorio y envíe ping a host del resto de subredes. Cada una de las pruebas debe ser exitosa, de lo contrario, haga el diagnóstico del problema y su solución.
31. Guarde los cambios en su simulación.

#### Parte 5: Subneteo con “Máscara de subred de longitud variable” (VLSM)

32. Prepare una nueva simulación, para implementar una topología lógica de red, que se ajuste a los requerimientos de host indicados en la Tabla 4. Debe utilizar una ip de red base de la clase C.

| # | Red      | Total host requeridos | # | Red        | Total host requeridos |
|---|----------|-----------------------|---|------------|-----------------------|
| 1 | Ventas   | 40                    | 4 | Producción | 16                    |
| 2 | Compras  | 12                    | 5 | Soporte    | 25                    |
| 3 | Gerentes | 18                    | 6 | Servicios  | 8                     |

**Tabla 4:** Topología de red a implementar

33. Aplique el Subneteo VLSM para distribuir apropiadamente el espacio de direccionamiento ip a las redes solicitadas en la topología.
34. Implemente en Packet Tracer a la topología lógica descrita en la Tabla 4.  
 Utilice un router genérico vacío (Router-PT- Empty), para conectar en cada interface a una subred diferente.  
 Y cada subred debe integrarse de 2 host y la de Servicios por 2 servidores.
35. Sobre el área de trabajo de la simulación, comience a documentar con polígonos a los límites de cada subred a implementar, así como por cada red: su *nombre*, la *ip-subred*, *máscara* e ip de *Gateway*.
36. Ingrese a la configuración del router para configurar por cada interface a la ip de Gateway de la subred a la cual conecta y su correspondiente máscara de subred.

37. Seleccione un host aleatorio y desde ahí, realice pruebas de ping hacia un host o server del resto de subredes. Todas las pruebas deben ser exitosas, de lo contrario, revise sus configuraciones hasta corregir el problema.
38. Guarde los cambios en la simulación y cierre el archivo.

## V. DISCUSIÓN DE RESULTADOS

### Parte I

1. Elabore un archivo de hoja de cálculo, que describa el proceso de los cálculos de Subneteo que resuelva el esquema de distribución de direcciones ip listado en la Tabla 5. Debe utilizar una IP Clase B como base para el Subneteo. Recuerde que las redes para *enlaces* entre router solo tienen 2 ip reservadas (no tienen ip gateway)

### Parte II

2. Prepare una simulación en Cisco Packet Tracer.
3. Agregue un router y modifíquelo de tal forma que contenga las interfaces fastethernet necesarias para acceder a las subredes (A hasta Servicios) de la Tabla 5.

**Tabla 5:** esquema de distribución de subredes

4. Configure cada interface de acceso con la ultima ip del rango disponible en la subred correspondiente asignada.
5. Agregue, configure y conecte a 2 host por cada subred configurada en router, excepto a la red de Servicios. A esta última, conecte y configure un Servidor.
6. Realice las pruebas necesarias para demostrar que los equipos de subredes diferentes se comunican correctamente por medio del router.

| Red            | host requeridos |
|----------------|-----------------|
| A              | 40              |
| B              | 8               |
| C              | 80              |
| D              | 30              |
| E              | 65              |
| Servicios      | 12              |
| <i>enlace1</i> |                 |
| <i>enlace2</i> |                 |
| <i>enlace3</i> |                 |

|                                                                                   |                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <b>UNIVERSIDAD AUTONOMA DE CHIHUAHUA<br/>FACULTAD DE INGENIERÍA</b>                                                                                                                                       |
| <b>enero-junio 2023</b>                                                           | <b>GUIA DE LABORATORIO #07</b><br><b>Nombre de la Practica:</b> Enrutamiento estático<br><b>Lugar de Ejecución:</b> Laboratorio de Redes<br><b>Tiempo Estimado:</b> 2h y 30 min.<br><b>MATERIA:</b> Redes |

## I. OBJETIVOS

Que el estudiante:

- Analice los parámetros que conforman a “tabla de enrutamiento ip”
- Comprenda los conceptos de balanceo de carga y distancia administrativa •

Configure rutas de tipo estáticas y rutas por defecto

## II. INTRODUCCION TEORICA

### Capa 3 OSI: Función de Enrutamiento

En términos generales, el enrutamiento es el proceso de reenviar paquetes entre dos redes conectadas.

En cuanto a las redes basadas en TCP/IP, el enrutamiento forma parte del Protocolo Internet (IP) y se utiliza junto con otros servicios de protocolo de red para proporcionar capacidades de reenvío entre hosts que se encuentran en segmentos de red distintos dentro de una red basada en un TCP/IP más grande.

IP es la "oficina de correos" del protocolo TCP/IP, donde se ordenan y entregan los datos IP. Cada paquete entrante o saliente se denomina datagrama IP. Un datagrama IP contiene dos direcciones IP: la dirección de origen del host que realiza el envío y la dirección de destino del host receptor. A diferencia de las direcciones de hardware, las direcciones IP de un datagrama siguen siendo las mismas durante su transmisión a través de una red TCP/IP.

El enrutamiento es la función principal de IP. Los datagramas IP se intercambian y procesan en cada host mediante IP en el nivel de Internet.

**El router** es una computadora diseñada para fines especiales que desempeña una función clave en el funcionamiento de cualquier red de datos.

Los routers son los principales responsables de la interconexión de redes por medio de:

→ La determinación de la mejor ruta para enviar paquetes → El envío de paquetes a su destino.

Los routers envían paquetes al aprender sobre redes remotas y al mantener la información de enrutamiento. El router es la unión o intersección que conecta múltiples redes IP. La principal decisión de envío de los routers se basa en la información de Capa 3, la dirección IP de destino.

La tabla de enrutamiento del router se utiliza para encontrar la mejor coincidencia entre la dirección IP de destino de un paquete y una dirección de red en la tabla de enrutamiento. La tabla de enrutamiento determinará finalmente la interfaz de salida para enviar el paquete y el router lo encapsulará en la trama de enlace de datos apropiada para dicha interfaz de salida.

## Tablas de enrutamiento

Los hosts TCP/IP utilizan una tabla de enrutamiento para mantener información acerca de otras redes IP y hosts IP. Las redes y los hosts se identifican mediante una dirección IP y una máscara de subred. Además, las tablas de enrutamiento son importantes ya que proporcionan la información necesaria a cada host local respecto a cómo comunicarse con redes y hosts remotos.

En cada equipo de una red IP, puede mantener una tabla de enrutamiento con una entrada para cada equipo o red que se comunica con el equipo local. En general, esto no es práctico y se utiliza una puerta de enlace predeterminada (enrutador IP) en su lugar.

## Rutas estáticas

Estas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso del enrutamiento según los parámetros del administrador.

Para conectividad de extremo a extremo, es necesario configurar la ruta en ambas direcciones. Las rutas estáticas permiten la construcción manual de la tabla de enrutamiento. El comando **ip route** configura una ruta estática, los parámetros del comando definen la ruta estática.

### Comandos

Forma 1:

```
Router#configure terminal
Router(config)# ip route "red de destino" "máscara de subred" "siguiente salto"
```

Ejemplo:

```
Router(config)#ip route 192.168.0.0 255.255.255.0 10.0.0.1
```

Forma 2:

```
Router#configure terminal
Router(config)#ip route "red de destino" "máscara de subred" "interfaz de salida"
```

Ejemplo:

```
Router(config)#ip route 172.168.0.0 255.255.255.0 serial 0/0/0
```

## Ruta por Defecto

Las rutas por defecto se utilizan para poder enviar tráfico a destinos que no concuerden con las tablas de enrutamiento de los dispositivos que integran la red.

El caso más común para su implementación sería el de redes con acceso a Internet ya que sería imposible contener en las tablas de enrutamiento de los dispositivos todas las rutas que la componen.

Las rutas por defecto, al igual que las rutas estáticas comunes, se configuran mediante el comando *ip route* en el modo Configuración Global.

**Comandos:**

Forma 1:

```
Router#configure terminal
Router#(config)#ip route 0.0.0.0 0.0.0.0 "siguiente salto"
```

Forma 2:

```
Router#configure terminal
Router#(config)#ip route 0.0.0.0 0.0.0.0 "interfaz de salida"
```

## Distancia administrativa

Es un **número entero entre 0 y 255** que califica la confiabilidad de la información de enrutamiento recibida por un dispositivo de cualquiera de las fuentes de información disponibles.

Tabla de distancias administrativas

La distancia administrativa se utiliza como criterio de selección cuando el dispositivo tiene en su base de información múltiples rutas hacia el mismo destino, obtenidas a través de diferentes fuentes de información.

El algoritmo de selección de la mejor ruta establece que, ante rutas aprendidas de diferentes fuentes, se valorará como mejor ruta aquella que tenga menor distancia administrativa.

| Origen de la ruta      | Distancia Administrativa |
|------------------------|--------------------------|
| Directamente Conectada | 0                        |
| Estática               | 1                        |
| Resumen de ruta EIGRP  | 5                        |
| BGP Externo            | 20                       |
| EIGRP Interno          | 90                       |
| IGRP                   | 100                      |
| OSPF                   | 110                      |
| IS-IS                  | 115                      |
| RIP                    | 120                      |
| EIGRP Externo          | 170                      |
| BGP Interno            | 200                      |

### III. MATERIALES Y EQUIPO

Para la realización de la guía de práctica se requerirá lo siguiente:

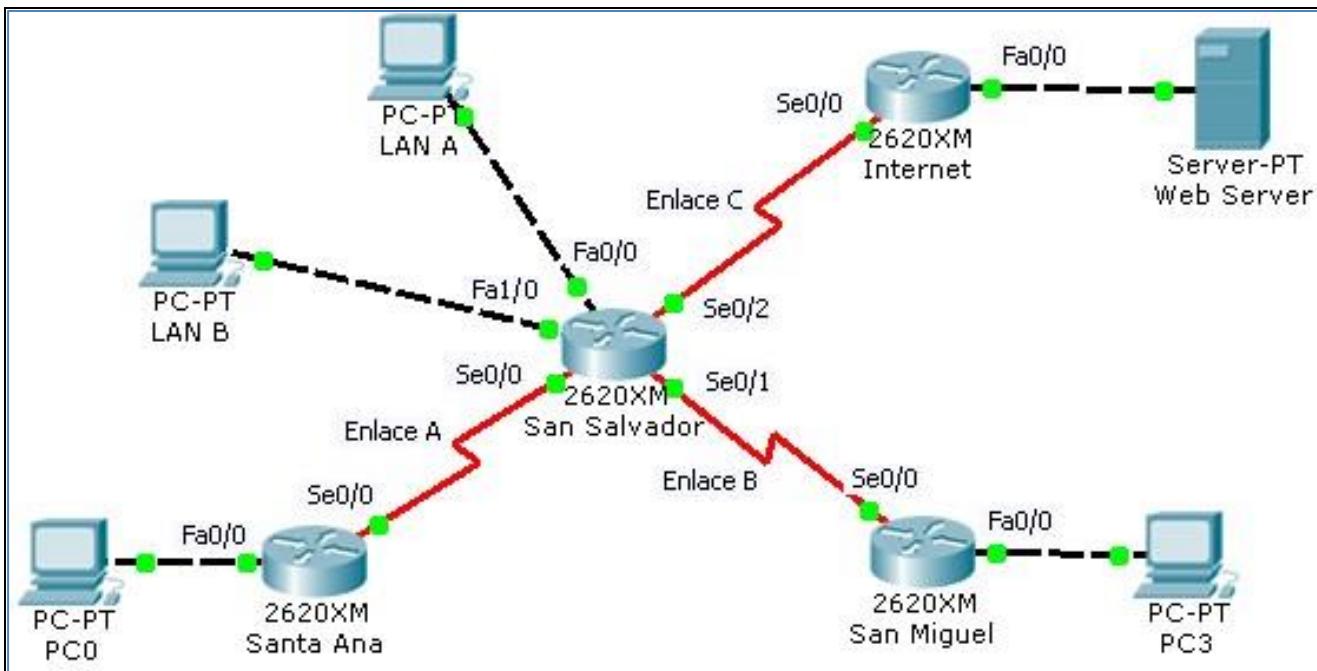
| No. | Requerimientos                                              | Cantidad |
|-----|-------------------------------------------------------------|----------|
| 1   | PC con Cisco Packet Tracer instalado                        | 1        |
| 2   | Practica N° 7 de laboratorio                                | 1        |
| 3   | Memoria USB para guardar los ejercicios y Plataforma Moodle | 1        |
|     |                                                             |          |

### IV. PROCEDIMIENTO

#### PARTE 1: Topología a implementar

1. Cargue la aplicación Cisco Packet Tracer y luego coloque la serie de dispositivos de la topología mostrada en la figura 7.1, pero no los conecte aún.

**Figura 7.1: Topología de red inicial a implementar**



2. Modifique a los dispositivos router listados a continuación, agregando los módulos indicados en cada caso:

| Dispositivo Router | Módulos                                |
|--------------------|----------------------------------------|
| Santa Ana          | 2 módulos WIC-1T                       |
| San Miguel         | 2 módulos WIC-1T                       |
| San Salvador       | 2 módulos WIC-2T<br>1 modulo NM-1FE-TX |
| INTERNET           | 1 módulos WIC-1T                       |

3. Realice la conexión de dispositivos, seleccionando las interfaces apropiadas entre parejas de dispositivos indicados en la figura 7.1. *Por cada conexión serial entre router, su extremo DCE debe estar en cada interface serial de SanSalvador.*
4. Configure el direccionamiento IP (ip host, mascara y gateway) de cada host y server de las redes locales de la topología de acuerdo al rango de subredes indicados en la siguiente tabla:

| ID de red local    | IP de RED   | /mk | RANGO     | GATEWAY     |
|--------------------|-------------|-----|-----------|-------------|
| SANTA ANA          | 172.16.50.0 | 24  | .2 - .254 | 172.16.50.1 |
| SAN SALVADOR LAN A | 192.0.5.0   | 26  | .2 – 62   | 192.0.5.1   |

|                    |            |    |            |            |
|--------------------|------------|----|------------|------------|
| SAN SALVADOR LAN B | 192.0.5.96 | 28 | .98 - .110 | 192.0.5.97 |
| SAN MIGUEL         | 196.2.0.0  | 24 | .2 - .254  | 196.2.0.1  |
| LAN WEBSERVER      | 10.2.0.0   | 29 | .2 - .6    | 10.2.0.1   |

5. Proceda a configurar el direccionamiento ip de las interfaces del router *SantaAna* de acuerdo a los parámetros a continuación:

**Router SantaAna**

| Interfaz | clock rate | IP             | Descripción       |
|----------|------------|----------------|-------------------|
| Fa0/0    | -          | 172.16.50.1/24 | Red LAN Santa Ana |
| Se0/0    | -          | 10.10.10.2 /30 | Enlace serial A   |

Para ejecutar esta configuración de interfaces, ingrese a la CLI de SantaAna y ejecute la siguiente secuencia de comandos:

Al inicio, la CLI mostrara el siguiente mensaje:

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Digite **no** y presione tecla *Enter*. Luego continúe con la siguiente configuración:

```
Router>enable
Router#configure terminal
Router(config)#hostname SantaAna
SantaAna(config)#no ip domain-lookup
SantaAna(config)#interface fastEthernet 0/0
SantaAna(config-if)#ip address 172.16.50.1 255.255.255.0
SantaAna(config-if)#description Red LAN Santa Ana
SantaAna(config-if)#no shutdown
SantaAna(config-if)#exit

SantaAna(config)#interface serial 0/0
```

```

SantaAna(config-if)#ip address 10.10.10.2 255.255.255.252
SantaAna(config-if)#description Enlace Serial A
SantaAna(config-if)#no shutdown
SantaAna(config-if)#exit
SantaAna(config)# do copy run start

```

6. En base a la configuración realizada a SantaAna, ingrese a la CLI de cada router restante y configure el direccionamiento ip de las interfaces correspondientes, de acuerdo a los parámetros a continuación:

**Router SanSalvador**

| Interfaz | clock rate | IP             | Descripción           |
|----------|------------|----------------|-----------------------|
| Fa0/0    | -          | 192.0.5.1 /26  | LAN A de San Salvador |
| Fa1/0    | -          | 192.0.5.97 /28 | LAN B de San Salvador |
| Se0/0    | 125000     | 10.10.10.1 /30 | Enlace serial A       |
| Se0/1    | 125000     | 10.10.10.5 /30 | Enlace serial B       |
| Se0/2    | 125000     | 15.0.0.1 /30   | Enlace serial C       |

**Router SanMiguel**

| Interfaz | clock rate | IP             | Descripción        |
|----------|------------|----------------|--------------------|
| Fa0/0    | -          | 196.2.0.1 /24  | Red LAN San Miguel |
| Se0/0    | -          | 10.10.10.6 /30 | Enlace serial B    |

**Router INTERNET**

| Interfaz | clock rate | IP           | Descripción      |
|----------|------------|--------------|------------------|
| Fa0/0    | -          | 10.2.0.1 /29 | Red LAN INTERNET |
| Se0/0    | -          | 15.0.0.2 /30 | Enlace serial C  |

7. Para continuar, desde el Command Prompt de cada host y server, confirme que cada uno alcanza a saludar a su respectiva dirección de Gateway. No continúe con el procedimiento hasta hacer esta prueba de comunicación local por cada red.

**PARTE 2: Configuración de rutas estáticas**

8. Retorne a la CLI de *SantaAna*. Luego, desde el nivel privilegiado, verifique su tabla de enruteamiento, ejecutando al comando *show ip route*. Vera el siguiente resultado:

**Importante:** Observe que solo se listan las redes que están directamente conectadas al router, indicando la interfaz a la que está conectada y marcadas al inicio con la letra **C**

```
SantaAna#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1
- OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 ...
P - periodic downloaded static route
Gateway of last resort is not set

10.0.0.0/30 is subnetted, 1 subnets
C 10.10.10.0 is directly connected, Serial0/0
172.16.0.0/24 is subnetted, 1 subnets
C 172.16.50.0 is directly connected, FastEthernet0/0

SantaAna#
```

9. Ahora, proceda a configurar rutas estáticas en el router *SantaAna*, que permitirán alcanzar las redes locales del resto de router del Sistema Autónomo (SA) interno.

Agregue el siguiente enruteamiento estático al router SantaAna:

```
SantaAna(config)#ip route 192.0.5.0 255.255.255.192 serial 0/0
SantaAna(config)#ip route 192.0.5.96 255.255.255.240 serial 0/0
SantaAna(config)#ip route 196.2.0.0 255.255.255.0 serial 0/0
```

**Importante:** Observe que se ha utilizado rutas estáticas por “**Interfaz de salida**”.

10. Ejecute nuevamente el comando *do show ip route* para ver su tabla de enruteamiento y su configuración de las rutas estáticas.

Note que aparecen 3 nuevas entradas que indican la red de destino, la dirección del siguiente salto y marcadas al inicio con la letra **S**

```
C 10.10.10.0 is directly connected, Serial0/0
172.16.0.0/24 is subnetted, 1 subnets
C 172.16.50.0 is directly connected, FastEthernet0/0
```

```
192.0.5.0/24 is subnetted, 2 subnets
 S 192.0.5.0/26 is directly connect, Serial 0/0
 S 192.0.5.96/28 is directly connect, Serial 0/0
S 196.2.0.0/24 is directly connect, Serial 0/0
```

11. De manera similar, agregue el siguiente enrutamiento estático al router *SanMiguel*:

```
SanMiguel(config)#ip route 192.0.5.0 255.255.255.192 serial 0/0
SanMiguel(config)#ip route 192.0.5.96 255.255.255.240 serial 0/0
SanMiguel(config)#ip route 172.16.50.0 255.255.255.0 serial 0/0
```

12. Genere la tabla de enrutamiento actual de *SanSalvador* y luego, determine

¿Cuáles son las redes de destino de la topología que este router no alcanza a “ver”?

13. Tome de modelo a los 2 ejemplos previos de enrutamiento estático y configure las rutas estáticas por ip del próximo salto que le faltan a *San Salvador* para alcanzar al resto de redes locales, pero ignore a la red local conectada al router *Internet*.

14. Una vez configuradas las rutas en el router *San Salvador*, realice pruebas de conectividad entre las diferentes parejas de PC's

Cada prueba deberá ser exitosa. De lo contrario, no continúe con este procedimiento hasta detectar y corregir el enrutamiento completo de la topología.

### **PARTE 3: Rutas por defecto**

Hasta el momento hemos configurado los router para permitir la comunicación entre las redes locales del SA (Santa Ana, San Miguel y San Salvador), pero en un ambiente de producción es indispensable la comunicación hacia Internet.

En la vida real resulta imposible conocer todas las redes e ips de siguiente salto que están en Internet. Es por eso que no se pueden utilizar rutas estáticas para este fin.

La solución a este problema es utilizar **rutas por defecto**.

15. Ingrese al router *SanSalvador* y configure la siguiente *ruta por defecto*, para brindar conexión hacia Internet (representado en este ejemplo por el Web Server que está conectado al router INTERNET).

Configuración de ruta por defecto en router **San Salvador**:

```
SanSalvador(config)# ip route 0.0.0.0 0.0.0.0 se0/2
```

16. De manera similar, configure una ruta por defecto en el router Santa Ana y luego en el router San Miguel.

#### PARTE 4: Rutas estáticas summarizadas

17. Ingrese a la CLI del router INTERNET y cree las siguientes rutas estaticas:

```
INTERNET(config)# ip route 172.16.50.0 255.255.255.0 se0/0
INTERNET(config)# ip route 196.2.0.0 255.255.255.0 se0/0
INTERNET(config)# ip route 192.0.5.0 255.255.255.0 se0/0
```

Esta configuración permite al router INTERNET alcanzar a las redes locales del resto de redes locales de la topología. *En un entorno real de aplicación, este equipo estaría administrado por el proveedor de servicios (ISP).*

Observe la última ruta (**192.0.5.0 /24**). A esta se le denomina **Ruta summarizada**, porque cubre el rango de direcciones de las redes locales configuradas en router *SanSalvador*.

18. Una vez configuradas a todas las rutas anteriores, desde host de las redes locales de Santa Ana, San Miguel y San Salvador, realice pruebas de conectividad dirigidas hacia el servidor web:

- Para ello, de clic sobre la PC, ingrese a la ficha superior Desktop y seleccione el icono “Web Browser”. Se simula un navegador Web.
- Aquí escriba como *URL* a la ip del WebBrowser.

#### PARTE 5: Trazado de rutas seguida por los paquetes (tracert y traceroute)

19. Para determinar los “*saltos/hops entre enrutadores*” que han sido necesarios para que un terminal de origen alcance un terminal de destino, se utilizan los comandos **traceroute** y **tracert**.
20. Ingrese al host de la red local de *SantaAna* y luego, desde su Command Prompt, genere un ping dirigido a la ip del host de LAN A. La prueba será exitosa; pero ¿Cuál fue la ruta seguida por sus paquetes para alcanzar el destino?
21. Del comando ping ejecutado en el paso anterior, reemplácelo por el comando *tracert* y ejecútelo. Obtendrá un resultado similar al siguiente:

```
PC>tracert 192.0.5.2
```

Tracing route to 192.0.5.2 over a maximum of 30 hops:

```
1 0 ms 0 ms 0 ms 172.16.50.1
2 0 ms 16 ms 16 ms 10.10.10.1
3 0 ms 16 ms 32 ms 192.0.5.2
```

Trace complete.

Localice a cada **ip resaltada** de este resultado en los diferentes dispositivos de la topología que las tienen configuradas, para dar seguimiento a cada salto del paquete en todo su recorrido ejecutado.

22. Ingrese a la CLI de *SanMiguel*. Luego, desde el nivel privilegiado, ejecute un ping a la ip del Servidor WebServer.

23. Luego, reemplace el comando *ping* por *traceroute*. El resultado devuelto será similar al siguiente:

```
SanMiguel#traceroute 10.2.0.2
Type escape sequence to abort.
Tracing the route to 10.2.0.2
1 10.10.10.5 16 msec 31 msec 2 msec
2 15.0.0.2 62 msec 46 msec 31 msec 3 10.2.0.2 33 msec 16 msec 47 msec
SanMiguel#
```

De igual forma, haga un seguimiento de cada ip obtenida en el resultado anterior, para analizar la ruta (saltos) seguida por los paquetes para alcanzar al servidor web.

24. Ingrese al host de la red local conectado a SanMiguel, para ejecutar un tracert hacia la ip del WebServer.

Compare este resultado con el del paso anterior. ¿Se obtuvo igual resultado en ambas pruebas?

¿Si o No? Justifique su respuesta.

## PARTE 6: Balanceo de Carga

25. Para continuar, agregue un enlace serial entre el router Santa Ana como extremo DCE en la interfaz se0/1 (con la IP 10.10.10.9/30) y a la interface Se 0/1 de San Miguel como DTE (con la IP 10.10.10.10/30).

Configure las ip indicadas en cada interface de los router indicados.

26. En router Santa Ana cree una ruta estática hacia la red local de San Miguel (referenciando a este nuevo enlace físico).

```
SantaAna(config)#ip route 196.2.0.0 255.255.255.0 serial 0/1
```

Luego ejecute el comando **do show ip route**, para confirmar la nueva ruta en este router:

```
SantaAna(config)#do show ip route
```

...

```
S 196.2.0.0/24 is directly connect, Serial 0/0 is directly
connect, Serial 0/1
S* 0.0.0.0/0 is directly connected, Serial0/0
```

```
SantaAna(config)#

```

Observe que se crean 2 rutas diferentes para alcanzar a la red 196.2.0.0 /24

27. Redacte un traceroute dirigido al host de la red local de SanMiguel. Observe un ejemplo de resultado:

```
SantaAna#traceroute 196.2.0.2 Type
escape sequence to abort.
Tracing the route to 196.2.0.2
```

```
1 10.10.10.10 2 msec 2 msec 2 msec
2 10.10.10.6 4 msec 16 msec 31 msec
```

Esta vez se obtienen 2 saltos finales para alcanzar la ip de destino. Localice cuales router tienen asignados estas **ip de próximo salto** resaltadas y luego analice.

- ¿Qué enrutadores generaron este resultado?
- ¿Cómo se llama a este tipo de enrutamiento ejecutado?

28. El enrutamiento con “balanceo de carga”, permite que el router *SantaAna* utilice ambos saltos de manera alternativa, enviando la mitad de paquetes por una ruta y el resto por la 2da ruta.

29. De manera similar al ejemplo anterior, en *SanMiguel*, ejecute los comandos necesarios para que genere enrutamiento con balanceo de carga cuando se le pida alcanzar a las redes LAN A y LAN B.
30. Compruebe si *SanMiguel* realmente ejecuta balanceo de carga de los paquetes de prueba dirigidos al host de LAN A y LAN B.

#### **PARTE 7: Rutas flotantes (Respaldo)**

Al agregar el nuevo enlace, se ha creado una ruta más corta entre las redes locales de San Miguel y SantaAna.

Además, ha optimizado la transferencia de paquetes de SanMiguel a la red de SantaAna, aplicando balanceo de carga.

31. Ingrese a la CLI de *SantaAna* y elimine la ruta original que permite alcanzar la red local de *SanMiguel*, ejecutando este comando:

```
SantaAna(config)#no ip route 196.2.0.0 255.255.255.0 serial 0/0
```

32. Genere la tabla de enrutamiento de *SantaAna*. Observe que el balanceo de carga desapareció, porque solo queda una ruta para alcanzar a red local de *SanMiguel* (a través del nuevo enlace).
33. Desde el host local de *SantaAna*, envíe un ping hacia el host de la red local de *SanMiguel*. Confirme si la comunicación entre ambas redes aún se mantiene.
34. Cree nuevamente la ruta previamente eliminada, pero modificando el parámetro distancia administrativa (**AD**) a 20, así:

```
SantaAna(config)#ip route 196.2.0.0 255.255.255.0 serial 0/0 20
```

35. Genere la tabla de enrutamiento y localice las rutas que permiten alcanzar a la red local de *San Miguel*. Solo se muestra una ruta, directa, por el nuevo enlace con *SanMiguel*.
36. Ingrese al modo de configuración de la interface serial de *SantaAna* que lo conecta directamente a *SanMiguel* y desactívela, ejecutando al comando shutdown.
37. Genere la tabla de enrutamiento de *SantaAna* y ubique si existe rutas hacia la red local de *SanMiguel*. Muestra la ruta original que se dirige a *SanSalvador*.

Se ha creado una ruta flotante hacia una red destino, la cual tendrá una AD mayor que la ruta principal al mismo destino.

El router utilizará solamente a la ruta principal, pero si falla esta ruta, se utilizará la ruta flotante registrada en la tabla de rutas (que tenga una AD mayor a la de la principal).

38. Para visualizar las rutas estáticas, solo visualice el contenido del archivo de ejecución (running-config), con el comando:

```
do show running-config
```

Presione *Enter* continuamente hasta localizar las rutas estáticas registradas.

39. Guarde las configuraciones de cada router y del switch. Cierre la simulación.

## V. ANALISIS DE RESULTADOS.

Cree una carpeta principal denominada **RECguia7\_CARNETrepresentante**, en el cual se almacenaran los siguientes archivos:

**NOTA: Todas las rutas estáticas deberá trabajarlas utilizando el “siguiente salto”, y por “la interfaz de salida”. (ver introducción teórica, e investigar por su cuenta.)**

### Parte A:

Archivo formal en formato PDF llamado **analisisguia7.pdf**

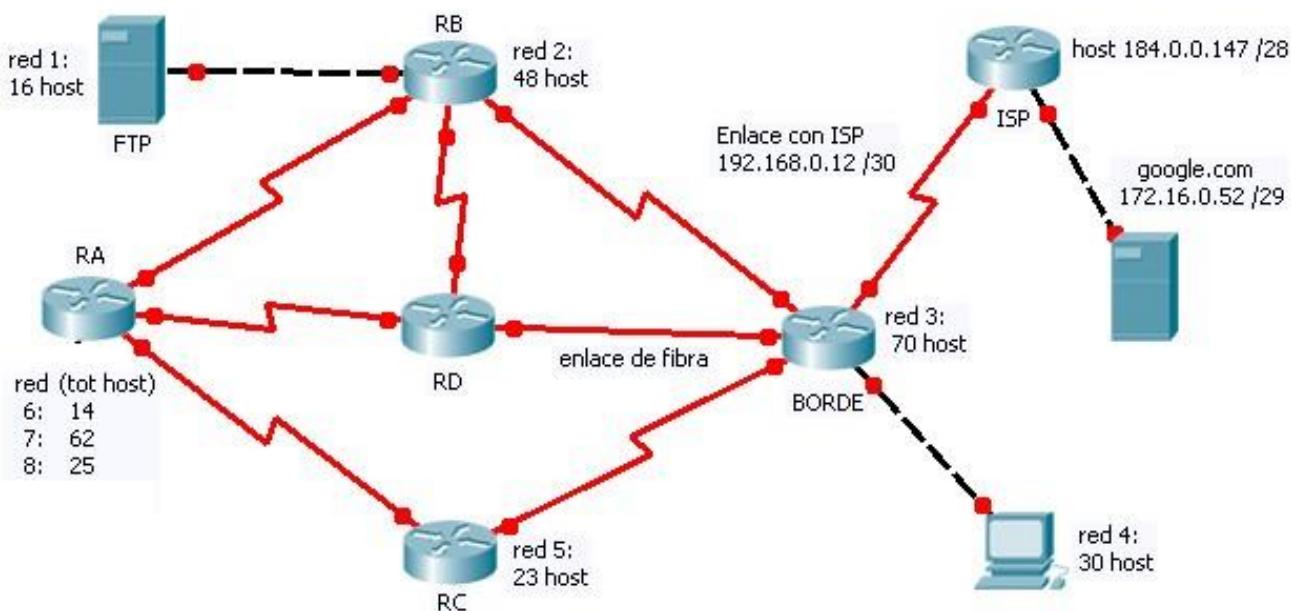
Este documento contendrá las respuestas a estas preguntas:

- ¿Que es una interface de loopback?
- ¿Cuáles son los usos que se da a las interfaces de loopback?
- ¿Cómo se configura una interface de loopback y como se identifica al visualizar la tabla de enrutamiento?

### Parte B:

Archivo de simulación en Cisco Packet Tracer, llamado **REC\_analisis7** con la solución a la topología de red mostrada en la figura 7.2.

**Figura 7.2:** Topología a implementar con enrutamiento estático



Desarrolle el subneteo necesario para implementar el esquema de direccionamiento ip requerido en la topología de red, utilizando la ip de red inicial **190.0.64.0 Mk 255.255.240.0** para el subneteo.

Este proceso incluye las redes finales y de enlaces entre router internos del sistema autónomo (SA). Luego, digite la tabla de direccionamiento de subredes finales en el doc. PDF solicitado en la Parte A de este análisis.

Implemente con interfaces loopback a las redes que no muestran un host físico en el diagrama de la red.

Documente cada ip subred sobre el segmento de red al cual se aplica.

### Parte C: políticas de enrutamiento estático

Configure el siguiente enrutamiento estático entre los siguientes router específicos de la topología anterior:

1. Todas las rutas estáticas a crear deben ser solamente por "ip del próximo salto".

2. Todos los router (excepto BORDE) del sistema autonomo:

Deben alcanzar a cada una de las redes finales restantes a través de 2 rutas diferentes, pero para cada destino, solo una sera utilizada, la otra deberá ser de respaldo.

3. Router BORDE:

Las políticas de enrutamiento serán las mismas que las implementadas en el resto de router, excepto para alcanzar a las 3 redes finales de RA, que lo hará aplicando "balanceo de carga" entre 2 rutas para cada una.

4. Cada router alcanzara al ISP con una ruta principal "del último recurso" y otra ruta alterna como respaldo.

5. Router ISP:

Debe configurar solamente a una ruta estática, que permita acceder al sistema autónomo por medio de BORDE. Esta ruta debe ser una “**ruta summarizada**”, que cubra a todas las redes obtenidas del subneteo inicial.

|                                                                                   |                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <b>UNIVERSIDAD AUTONOMA DE CHIHUAHUA</b><br><b>FACULTAD DE INGENIERÍA</b>                                                                                                                     |
| <b>enero-junio 2023</b>                                                           | <b>GUIA DE LABORATORIO #08</b><br><b>Nombre de la Practica:</b> RIP y OSPF<br><b>Lugar de Ejecución:</b> Laboratorio de Redes<br><b>Tiempo Estimado:</b> 2h y 30 min<br><b>MATERIA:</b> Redes |

## I. OBJETIVOS

- Configurar el protocolo de enrutamiento RIPv1 y RIPv2.
- Identificar redes conocidas por los routers a partir de la tabla de enrutamiento.  Configuración mediante rutas dinámicas.

## II. INTRODUCCIÓN

### Introducción al enrutamiento dinámico con el protocolo RIP

**RIP (Routing Information Protocol)** es un protocolo de enrutamiento de puerta de enlace interna (IGP - Internal Gateway Protocol) basado en un protocolo original de Xerox, el GWINFO.

RIP cuenta con una distancia administrativa de 120 y utiliza un algoritmo de vector distancia utilizando como métrica el número de saltos.

|           | Protocolos de gateway interiores                   |       |                                                | Protocolos de Gateway Externos |                |
|-----------|----------------------------------------------------|-------|------------------------------------------------|--------------------------------|----------------|
|           | Protocolos de enrutamiento por vector de distancia |       | Protocolos de enrutamiento de estado de enlace | Vector de ruta                 |                |
|           | Con clase                                          | RIP   | IGRP                                           |                                | EGP            |
| Sin clase |                                                    | RIPv2 | EIGRP                                          | OSPFv2                         | IS-IS          |
| IPv6      |                                                    | RIPng | EIGRP for IPv6                                 | OSPFv3                         | IS-IS for IPv6 |
|           |                                                    |       |                                                |                                | BGPv4          |
|           |                                                    |       |                                                |                                | BGPv4 for IPv6 |

Al carecer de otro mecanismo para evitar loops posee una métrica de 15 saltos, tomando al salto 16 como infinito y marcándolo como inalcanzable en la tabla de enrutamiento.

Hoy en día hay 3 versiones: **RIP**, **RIPv2** y **RIPng**,

En el procedimiento restante se configurara a RIP y RIPv2.

La versión RIPng es para implementaciones de direccionamiento con IPv6 y se verá en una práctica posterior.

## Configuración de RIP

RIP actualiza cada 30 segundos utilizando el protocolo UDP y el puerto 520, enviando la tabla de enrutamiento completa a sus vecinos.

La versión original del protocolo de enrutamiento RIP es “con clase”, es decir que no soporta subredes, VLSM ni CIDR, no posee mecanismos de autenticación y no realiza actualizaciones desencadenadas por eventos. Todas estas limitaciones hicieron que con el paso del tiempo y las nuevas necesidades cayera en desuso.

Comprender el RIP es importante para sus estudios de networking debido a 2 motivos. Primero, RIP aún está en uso. Puede enfrentarse a la implementación de una red lo suficientemente amplia para necesitar un protocolo de enrutamiento y aun lo suficientemente simple para utilizar el RIP en forma efectiva. Además, la familiaridad con muchos de los conceptos fundamentales de RIP facilitara la comprensión de otros protocolos de enrutamiento.

## Configuración desde la línea de comandosRIPV1

Las siguientes analogías pueden ayudar a aclarar el concepto de rutas conectadas, estáticas y dinámicas:

- ✓ **Rutas conectadas directamente:** para visitar a un vecino, lo único que tiene que hacer es caminar por la calle donde vive. Esta ruta es similar a una ruta conectada directamente porque el "destino" está disponible directamente a través de su "interfaz conectada", la calle.
- ✓ **Rutas estáticas:** un tren siempre usa las mismas vías en una ruta específica. Esta ruta es similar a una estática porque la ruta hacia el destino es siempre la misma.
- ✓ **Rutas dinámicas:** al conducir un automóvil, usted puede elegir "dinámicamente" una ruta diferente según el tráfico, el clima y otras condiciones. Esta ruta es similar a una ruta dinámica porque puede elegir una nueva ruta en muchos puntos diferentes en su trayecto hacia el destino.

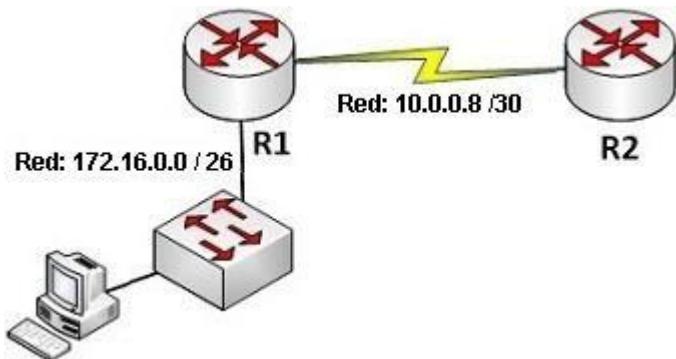
Suponga que tenemos la red de la figura.

El procedimiento para configurar RIP es sencillo.

Lo único que se hace es publicar las redes que tiene directamente conectadas cada Router por sus interfaces.

Previamente debes haber configurado los puertos y direcciones IP.

El enruteamiento se activa con comando **router rip** y luego, desde el modo de configuración, publicas las redes utilizando comandos **network** y la ip de cada red que deseamos publicar.



Observa el siguiente ejemplo:

```
Router1>enable
Router1#config terminal
Router1(config)#router rip (Aquí se inicia la configuración del protocolo RIP)
Router1(config-router)#network 10.0.0.0 (publicamos la red directamente conectada) Router1(config-router)#network 172.16.0.0 (publicamos la red directamente conectada)
```

En donde:

- ✓ **router rip.** Comando para acceder al modo de configuración de router asignando el protocolo de enruteamiento RIP.
- ✓ **network.** Comando que se utiliza para que el router publica las redes en sus paquetes de actualización RIP.
- ✓ **10.0.0.0** Red que será publicada por el router.

Los comandos que se puede utilizar bajo la configuración de RIP son:

| Comando             | Description                                            |
|---------------------|--------------------------------------------------------|
| auto-summary        | Enter Address Family command mode                      |
| default-information | Control distribution of default information            |
| distance            | Define an administrative distance                      |
| exit                | Exit from routing protocol configuration mode          |
| network             | Enable routing on an IP network                        |
| no                  | Negate a command or set its defaults                   |
| passive-interface   | Suppress routing updates on an interface               |
| redistribute        | Redistribute information from another routing protocol |
| timers              | Adjust routing timers                                  |
| versión             | Set routing protocol version                           |

## Configuración de RIPv2

**Routing Information Protocol v2**, es la evolución de RIP v1 hacia un protocolo de enrutamiento “sin clase”, es decir, además de CIDR, éste soporta VLSM (Máscara de subred de longitud variable), resumen de rutas. También realiza actualizaciones desencadenadas por eventos y posee mecanismos de autenticación mediante texto plano o codificación MD5.

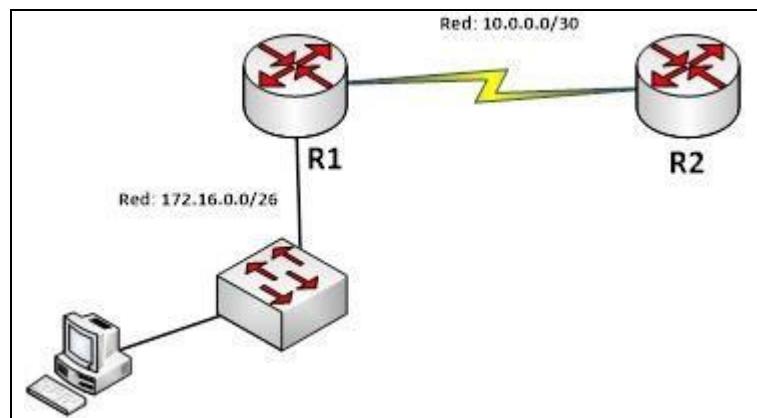
Las rutas tienen un TTL (tiempo de vida) de 180 segundos, es decir que si en 6 intercambios la ruta no aparece activa, esta es borrada de la tabla de enrutamiento

Su configuración no varía mucho al RIP original, sólo que debemos agregar el comando "version 2" al entrar al modo de configuración de RIP en el router.

Observa la red de la figura, con ip de redes con VLSM y la configuración de RIPv2 en el router R1:

### Secuencia de configuración de Rip V2:

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0
R1(config-router)#network 172.16.0.0
```



En donde:

- ✓ **router rip**.- Comando para acceder al modo de configuración de router asignando el protocolo de enrutamiento RIP.
- ✓ **version 2**.- Comando que indica que se usará la versión del protocolo RIP
- ✓ **network**.- Comando que se utiliza para que el router publique las redes en sus paquetes de actualización RIP
- ✓ **10.0.0.0** - Red que será publicada por el router.

El comando versión 2, puede ejecutarse tanto al inicio como se puede apreciar en el ejemplo o al final, inmediatamente después de haber publicado la última red conectada al router.

## OSPF (Open Shortest Path First)

OSPF es un protocolo de enrutamiento “sin clase” y de tipo de “Estado de enlace”.

El desarrollo inicial de OSPF comenzó en 1987 por parte del grupo de trabajo de OSPF, el Grupo de trabajo de ingeniería de Internet (IETF). En aquel momento, Internet constituía fundamentalmente una red académica y de investigación financiada por el gobierno de los EE. UU.

## **Establecimiento de vecinos**

Antes de que un router OSPF pueda saturar a otros routers con sus estados de enlace, primero debe determinar si existe algún otro vecino OSPF en alguno de sus enlaces. Para lograrlo, los routers OSPF envían paquetes de saludo a todas las interfaces habilitadas con OSPF para determinar si hay vecinos en dichos enlaces.

La información en el saludo de OSPF incluye la ID del router OSPF del router que envía el paquete de saludo. La recepción de un paquete de saludo OSPF en una interfaz confirma a un router la presencia de otro router OSPF en dicho enlace. OSPF luego establece la adyacencia con el vecino.

## **Intervalos muerto y de saludo de OSPF**

Antes de que dos routers puedan formar una adyacencia de vecinos OSPF, éstos deben estar de acuerdo con respecto a tres valores: Intervalo de saludo, intervalo muerto y tipo de red. El intervalo de saludo de OSPF indica la frecuencia con que un router OSPF transmite sus paquetes de saludo. De manera predeterminada, los paquetes de saludo OSPF se envían cada 10 segundos en segmentos multiacceso y punto a punto, y cada 30 segundos en segmentos multiacceso sin broadcast (NBMA) (Frame Relay, X.25, ATM).

En la mayoría de los casos, los paquetes de saludo OSPF se envían como multicast a una dirección reservada para ALL SPF Routers en 224.0.0.5. La utilización de una dirección multicast permite a un dispositivo ignorar el paquete si la interfaz no está habilitada para aceptar paquetes OSPF. Esto ahorra tiempo de procesamiento de CPU en los dispositivos que no son OSPF.

El intervalo muerto es el período, expresado en segundos, que el router esperará para recibir un paquete de saludo antes de declarar al vecino "desactivado". Cisco utiliza en forma predeterminada cuatro veces el intervalo de Hello. En el caso de los segmentos multiacceso y punto a punto, dicho período es de 40 segundos. En el caso de las redes NBMA, el intervalo muerto es de 120 segundos. Si el intervalo muerto expira antes de que los routers reciban un paquete de saludo, OSPF retirará a dicho vecino de su base de datos de estado de enlace. Luego, el router satura con la información de estado de enlace acerca del vecino "desactivado" desde todas las interfaces habilitadas con OSPF.

## **Velocidad (ancho de banda) de un enlace y el comando bandwidth**

Para determinar el ancho de banda (Band Width: BW) estándar de algún enlace WAN o de conexión a Internet (ISP), se utiliza el comando show interfaces.

El siguiente ejemplo, muestra el resultado de ejecutar show interfaces para localizar y determinar el ancho de banda disponible para un enlace FastEthernet con cable UTP:

```

Router#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up (connected)
 Hardware is Lance, address is 00e0.f71c.2a01 (bia 00e0.f71c.2a01)
 Internet address is 172.16.48.1/22
 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
 reliability 255/255, txload 1/255, rxload 1/255

```

El ancho de banda se mide siempre en Kilobits por segundo (Kbit).

## Uso de comando bandwidth

El comando bandwidth permite indicar la velocidad de la interfaz a los protocolos de nivel superior (protocolos de enrutamiento) que utilizan el ancho de banda como parte de la métrica para elegir la mejor ruta hacia una red de destino. Este parámetro lo toman de los valores configurados por el comando bandwidth en cada interfaz.

Por ejemplo, EIGRP y OSPF utilizan la información de bandwidth para determinar parte de su métrica de enrutamiento.

## Alterando el ancho de banda de una interfaz

El bandwidth debe configurarse en el modo de configuración de la interfaz correspondiente.

Algunos ejemplos sobre como alterar el ancho de banda que usaran los protocolos de enrutamiento como elemento de la métrica de sus algoritmos de enrutamiento se muestran a continuación:

|                                                                                                                                                                                                                                       |                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Ejemplo 1:<br>Se asigna un ancho de banda de 128 Kbits a un enlace T1 (enlace serial):                                                                                                                                                | Router(config)#interface serial 0/0<br>Router(config-if)#bandwidth 128        |
| Ejemplo 2:<br>Se requiere asignar un ancho de banda de 4 Mbits a un enlace Fastethernet 1/0.<br>En este caso, se debe convertir el ancho de banda dado en Mbits a Kbits, dando un valor de 4096 Kbits y configurarlo en la interface: | Router(config)#interface FastEthernet 0/0<br>Router(config-if)#bandwidth 4096 |

Cada tipo de interfaz tiene asignado un valor de ancho de banda por defecto, lo que significa que aun cuando no se configure ningún bandwidth, siempre hay un valor de BW para realizar los cálculos necesarios.

En el caso de las interfaces seriales, el valor predeterminado de su ancho de banda será de 1544 Kbits

Es de aclarar que el uso de comando bandwidth no altera la velocidad real de la interface sobre la cual se aplica.

Por ejemplo:

Si se ha contratado un enlace E1 (cuyo ancho de enlace estándar es de 2048 Kbits) y sobre la interfaz conectada a ese enlace se configura al comando bandwidth 4096.

El ancho de banda real de este enlace seguirá siendo de 2048 Kbps, es decir, que no afecta el ancho de banda real del enlace.

El valor asignado de ancho de banda (4096) con el comando bandwidth le servirá únicamente a los protocolos de enrutamiento para generar la métrica a utilizar en sus rutas a publicar que se generen sobre este enlace.

En conclusión, la configuración del valor de bandwidth correcto en cada interfaz es de suma importancia cuando se trabaja con protocolos de enrutamiento que utilizan el ancho de banda en sus métricas.

Sin embargo, no importa el valor de bandwidth que configure en una interfaz, esto no modificará en nada el ancho de banda real del enlace conectado a esa interfaz.

## Velocidad (ancho de banda) de un enlace

Para determinar el ancho de banda (Band Width: BW) estándar de algún enlace WAN o de conexión a Internet (ISP), se utiliza el comando show interfaces.

El siguiente ejemplo, muestra el resultado de ejecutar show interfaces para localizar y determinar el ancho de banda disponible para un enlace FastEthernet con cable UTP:

```
Router#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up (connected)
 Hardware is Lance, address is 00e0.f71c.2a01 (bia 00e0.f71c.2a01)
 Internet address is 172.16.48.1/22
 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, reliability 255/255,
 txload 1/255, rxload 1/255
```

El ancho de banda se mide siempre en Kilobits por segundo (Kbit).

## Uso de comando bandwidth

El comando bandwidth permite indicar la velocidad de la interfaz a los protocolos de nivel superior (protocolos de enrutamiento) que utilizan el ancho de banda como parte de la métrica para elegir la mejor ruta hacia una red de destino. Este parámetro lo toman de los valores configurados por el comando bandwidth en cada interfaz.

Por ejemplo, EIGRP y OSPF utilizan la información de bandwidth para determinar parte de su métrica de enrutamiento.

## Alterando el ancho de banda de una interfaz

El bandwidth debe configurarse en el modo de configuración de la interfaz correspondiente.

Algunos ejemplos sobre como alterar el ancho de banda que usaran los protocolos de enrutamiento como elemento de la métrica de sus algoritmos de enrutamiento se muestran a continuación:

|                                                                                                                                                                                                                                       |                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Ejemplo 1:<br>Se asigna un ancho de banda de 128 Kbits a un enlace T1 (enlace serial):                                                                                                                                                | Router(config)#interface serial 0/0<br>Router(config-if)#bandwidth 128        |
| Ejemplo 2:<br>Se requiere asignar un ancho de banda de 4 Mbits a un enlace Fastethernet 1/0.<br>En este caso, se debe convertir el ancho de banda dado en Mbits a Kbits, dando un valor de 4096 Kbits y configurarlo en la interface: | Router(config)#interface FastEthernet 0/0<br>Router(config-if)#bandwidth 4096 |

Cada tipo de interfaz tiene asignado un valor de ancho de banda por defecto, lo que significa que aun cuando no se configure ningún bandwidth, siempre hay un valor de BW para realizar los cálculos necesarios.

En el caso de las interfaces seriales, el valor predeterminado de su ancho de banda será de 1544 Kbits

Es de aclarar que el uso de comando bandwidth no altera la velocidad real de la interface sobre la cual se aplica.

Por ejemplo:

Si se ha contratado un enlace E1 (cuyo ancho de enlace estándar es de 2048 Kbits) y sobre la interfaz conectada a ese enlace se configura al comando bandwidth 4096.

El ancho de banda real de este enlace seguirá siendo de 2048 Kbps, es decir, que no afecta el ancho de banda real del enlace.

El valor asignado de ancho de banda (4096) con el comando bandwidth le servirá únicamente a los protocolos de enrutamiento para generar la métrica a utilizar en sus rutas a publicar que se generen sobre este enlace.

En conclusión, la configuración del valor de bandwidth correcto en cada interfaz es de suma importancia cuando se trabaja con protocolos de enrutamiento que utilizan el ancho de banda en sus métricas.

Sin embargo, no importa el valor de bandwidth que configure en una interfaz, esto no modificará en nada el ancho de banda real del enlace conectado a esa interfaz.

## III. MATERIALES Y EQUIPO

| Nº | REQUERIMIENTO | CANTIDAD |
|----|---------------|----------|
|----|---------------|----------|

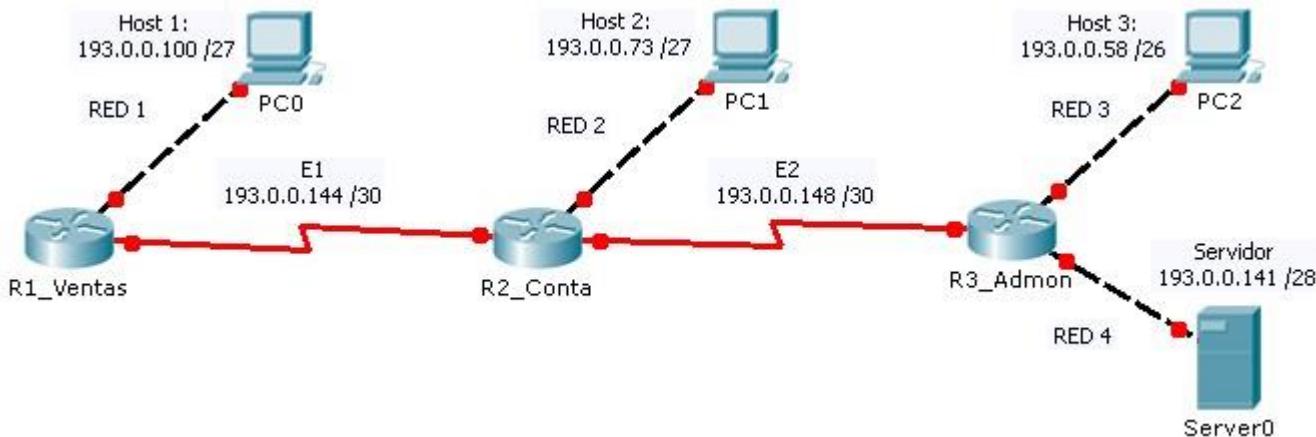
|   |                                                                          |   |
|---|--------------------------------------------------------------------------|---|
| 1 | Practica Nº 8                                                            | 1 |
| 2 | Estación de trabajo de PC con Simulador de Packet Tracer 6.01 o superior | 1 |
| 3 | Memoria USB para guardar los ejercicios y Plataforma Moodle              | 1 |

#### IV. PROCEDIMIENTO

##### **PARTE 1: Configuración del enrutamiento dinámico utilizando RIPv2.**

1. Prepare una nueva simulación de Cisco Packet Tracer bajo el nombre **Ejemplo1\_RIP** y agregar el siguiente equipo:  
3 router de la serie 2621, 3 host y en Server-PT
2. Modifique los módulos de interfaces de los router para desarrollar la topología lógica de red descrita en la figura 8.1. Asegúrese que los router tengan 4 puertos seriales.
3. A cada host y al server, configurarle el direccionamiento (ip host y mascara de subred) específico indicado en la figura 8.1
4. Determine la ip-red a la cual pertenece cada uno de los host, para elaborar el esquema de direccionamiento ip de cada subred.
5. Del rango de direcciones ip de cada subred (RED 1, RED 2 y RED 3), seleccione la 1er dirección de host para ser utilizada como ip de Gateway. Luego, en cada host, configure la ip-gateway apropiada.

**Figura 8.1:** Topología de red a implementar



6. Ingrese a la CLI del router **R1\_Ventas**.

Configure su nombre de host y luego defina el direccionamiento ip de cada interfaz conectada.

De la ip de subred E1, seleccione la ip de host (193.0.0.145) y configúrela en la interface serial de conexión. Levante administrativamente cada interface (no shutdown).

7. Confirme que puede alcanzar al Host1, ejecutando al comando: do ping 193.0.0.100 La prueba deberá ser exitosa. De lo contrario, revise las configuraciones de las interfaces, así como la ip de Gateway en el Host1.
8. Guarde los datos de configuración de este router en su archivo de configuración de inicio (**startup-config**), para que no se pierda al apagarlo y/o reiniciarlo.
9. Proceda a configurar el protocolo de enrutamiento dinámico RIPv2, ejecutando la secuencia de comandos a continuación (\*):

```
R1_Ventas>
R1_Ventas>enable
R1_Ventas#configure terminal
R1_Ventas(config)#router rip
R1_Ventas(config-router)#version 2
R1_Ventas(config-router)#network 192.168.1.0
R1_Ventas(config-router)#network 172.25.3.0
```

(\*) **Muy importante:**

Debe reemplazar ambas **ip de redes resaltadas** por la ip de subred que ha determinado para la red RED1 y la ip de red del enlace E1, respectivamente.

10. Ingrese a la CLI del router **R2\_Conta**, para luego ejecutar una configuración similar a la aplicada en R1\_Ventas.

Asigne las ip apropiadas en cada interface y activelas.

Haga una prueba de ping dirigida a la ip 193.0.0.145 (que fue configurada en el router R1\_Ventas, bajo la red E1 que comparten en común) y luego, envíe un ping hacia el Host 2. Ambas pruebas deben ser exitosas.

11. Ingrese al modo de configuración de RIP. Indique que usara la versión 2 del protocolo y publique las 3 ip de subred que este router tiene configuradas directamente por sus interfaces.

12. Retorne a la CLI de R1\_Ventas y ejecute al comando **show ip route**, para ver su tabla de enrutamiento. Identifique cuales son las redes directamente conectadas (marcadas con C) y las rutas de redes aprendidas dinámicamente bajo el protocolo RIP (marcadas con R).

13. De manera similar, visualice las rutas de R2\_Conta. Anota en la tabla a continuación a las redes (con ip red y mascara) que cada dispositivo tiene registradas.

| Equipo    | Redes Conectadas (C) | Redes Aprendidas con RIP (R) |
|-----------|----------------------|------------------------------|
| R1_Ventas | -<br>-<br>-          | -<br>-<br>-                  |
| R2_Conta  | -<br>-<br>-          | -<br>-<br>-                  |

14. Realice el envío de ping entre ambos host (Host 1 y Host 2). La prueba debe ser exitosa!!

15. Guarde la configuración de ambos router configurados hasta ahora.

16. Proceda a configurar el router R3\_Admon, tanto en sus interfaces como al protocolo RIPv2.

17. Cuando finalice la configuración, genere su tabla de enrutamiento y confirme que puede ver las redes locales del resto de router, gracias a RIPv2. Haga pruebas de ping dirigidos a las Host 1 y Host 2. Ambas pruebas serán exitosas. 18. Guarde la simulación general hasta ahora.

## PARTE 2: Creando enlaces redundantes

19. Guarde una copia de la simulación actual con el nombre **Ejemplo2\_RIP**,

20. Haga una conexión serial entre router R1\_Ventas y R3\_Admon.

21. Determine la siguiente ip de subred a la asignada a E2, para definir la red E3, que será configurada en esta nueva conexión.
22. Configure en ambos routers al nuevo enlace de conexión, utilizando el direccionamiento de la red E3.
23. Desde R1\_Ventas, haga pruebas de ping a la ip asignada al otro extremo (de R3\_Admon) del nuevo enlace. La prueba deberá ser exitosa.  
Luego, genere su tabla de enrutamiento. Observe la topología actual y las rutas de la tabla, para determinar  
¿Cuáles son las redes que requieren “balanceo de carga” para ser alcanzadas?, justifique técnicamente su respuesta
24. Guarde las configuraciones de cada router en su correspondiente archivo de inicio (startupconfig)
25. Al concluir con el ejercicio llame a su instructor para que evalúe el funcionamiento.

### PARTE 3: Publicando rutas estáticas por defecto en RIP

26. Agregar a su simulación el siguiente equipo, para efectuar los cambios ahí indicados:

#### + Router 2811

Este router ISP representa el equipo usado por el proveedor de servicio de conexión a Internet.

Cambiar su nombre a **ISP** y agregar un módulo de conexión (WIC-2T).

Ingresar a su CLI y configurar su nombre de host. Levantar su interfaz serial 0/1/0 como DCE y configurarle la ip 10.0.0.65 /29.

Activar su interfaz fastethernet fa0/0 con la ip 150.0.0.110 /16.

Agregar la siguiente ruta estática al ISP: **ip route 193.0.0.0 255.255.255.0 10.0.0.67**

#### + ServerPT

Cambiar su nombre a **ServerFacebook**, conectarlo a la interfaz fa0/0 de router ISP, configurar su NIC con una ip host perteneciente a la red de la fa0/0 del router ISP.

Configurar su ip Gateway apropiadamente. Comprobar que este equipo alcanza a su conexión con ISP enviando ping a su ip Gateway.

27. Conecte la interfaz serial s0/1/0 del ISP (extremo DCE con clock-rate 9600) hacia una interface serial libre del router **R3\_admon**.

28. Su proveedor de internet le ha brindado a usted la ip **10.0.0.67 /29** para que la configure en la interfaz de su router R3\_admon conectada a ISP y así acceda a sus servicios de conexión externos (representados por el acceso a red externa del ServerFacebook).

Haga esta configuración ip en el serial de R3\_Admon y compruebe que alcanza a ver al router ISP de su proveedor, enviando ping a la ip 10.0.0.65.

29. Agregue la siguiente ruta por defecto en router R3\_admon y confirme en su tabla de enrutamiento que esta ruta estática ha sido registrada:

**ip route 0.0.0.0 0.0.0.0 serial 0/1**

30. Desde el host de red de Ventas, envíe un ping hacia la ip del ServerFacebook. Obtendrá mensaje del router R1\_Ventas, indicando una red inalcanzable. Confirme esta respuesta, visualizando los cambios en la tabla de enrutamiento de router R1\_Ventas.

Este último router aun no sabe de esta ruta por defecto configurada a router R3\_admon.

31. Retorne a la CLI de R3\_admon e ingrese a la configuración del protocolo RIP. Ahí digite el comando **default-information originate**.

32. Genere nuevamente la tabla de enrutamiento de router R1\_Ventas y determine si este tiene o no una ruta por defecto.

Luego repita la prueba de envío de ping de host de red ventas hacia el server. La prueba debe ser exitosa, de lo contrario, revise las últimas configuraciones efectuadas.

33. Observar que con este ultimo comando de rip, el router R3\_admon publica su ruta por defecto hacia el resto de router, para que estos también la agreguen a sus tablas de enrutamiento.

#### **PARTE 4: Bloqueando las publicaciones de enrutamiento RIP**

34. Desde la CLI de R1\_Ventas, ejecute el comando **show ip protocols**

Observe el resultado a continuación, en el cual se han resaltado algunos parámetros:

```

R1_Ventas#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 16 seconds
...
...
Interface Send Recv Triggered RIP Key-chain
FastEthernet0/0 2 2
Serial0/0 2 2
Serial0/1 2 2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks: 193.0.0.0
Passive Interface(s):
Routing Information Sources:
Gateway Distance Last Update
193.0.0.154 120 00:00:27
193.0.0.146 120 00:00:26
Distance: (default is 120)
R1_Ventas#

```

Este resultado indica que se están enviando y recibiendo actualizaciones RIP desde las 3 interfaces conectadas.

También, se han recibido actualizaciones desde sus router vecinos.

35. Las actualizaciones de enrutamiento generados por RIP enviada por la Fa 0/0 generarán saturación innecesaria a los clientes de esa red local, por lo que hay que indicarle a RIP que no envie sus actualizaciones por esa interface.

36. Ingrese al modo de configuración de RIP de R1\_Ventas y ejecute el comando:

```
R1_Ventas(config-router)#passive-interface fastEthernet 0/0
```

37. Ejecute de nuevo al comando: **do show ip protocols**

```

R1_Ventas(config-router)#do show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 11 seconds
...
...
Interface Send Recv Triggered RIP Key-chain
Serial0/0 2 2
Serial0/1 2 2
Automatic network summarization is in effect

```

```

Maximum path: 4
Routing for Networks:
193.0.0.0
Passive Interface(s):
FastEthernet0/0
Routing Information Sources:
Gateway Distance Last Update
193.0.0.154 120 00:00:17
193.0.0.146 120 00:00:13
Distance: (default is 120) R1_Ventas(config-router)#

```

38. Gracias a la configuración de la Fa0/0 como interface pasiva, RIP publicara su red local al resto de la topología, pero no enviara publicaciones RIP por esta interface.
39. Para finalizar, en el protocolo RIP de R2\_CConta y R3\_admon, configure las interfaces pasivas apropiadas.
40. Guarde los cambios en la configuración de cada router y guarde el archivo de simulación general.

## PARTE 5: Configurando al protocolo OSPF

41. Haga una copia del archivo actual de simulación, haciendo clic en opción del menú Archivo -> Salvar como... Guarde la copia con el nombre: **Ejemplo1 OSPF**
42. Para continuar, eliminara la configuración de RIP en los router R1\_Ventas, R2\_CConta y R3\_Admon.  
Ingresel modo de configuración global de estos 3 router y ejecute ahí al comando **no router rip**. Esto borra el proceso RIP.
43. Genere la tabla de enrutamiento de R1\_Ventas y confirme que nuevamente muestra solamente a las rutas de las redes directamente configuradas en sus interfaces.
44. Configure el protocolo de enrutamiento dinámico OSPF en R1\_Ventas, ejecutando la secuencia de comandos siguientes desde su modo global:

| Comando a ejecutar    | Descripción                    |
|-----------------------|--------------------------------|
| <b>router ospf 10</b> | Activa el proceso 10 bajo OSPF |

|                                           |                                                                                                                                   |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>network 193.0.0.96 0.0.0.31 area 0</b> | Publicara en OSPF a la red local R1.<br>Cada id de red usa la máscara de wildcard (*) y se publican bajo el área administrativa 0 |
| <b>network 193.0.0.144 0.0.0.3 area 0</b> | Publica las id de red de sus enlaces a sus 2 router                                                                               |
| <b>Comando a ejecutar</b>                 | <b>Descripción</b>                                                                                                                |
| <b>network 193.0.0.152 0.0.0.3 area 0</b> | vecinos                                                                                                                           |
| <b>passive-interface fa0/0</b>            | Evita envío de paquetes de enrutamiento ospf por la interface a la cual se conecta la Red1.                                       |

**(\*) Importante:**

Recuerde que una máscara de wildcard se obtiene calculando el complemento binario A1 a la máscara de la subred a publicar en OSPF.

Por ej.: la máscara de la Red1 es /27 o 255.255.255.224, su complemento binario A1 es 0.0.0.31

45. Guarde los cambios en R1\_Ventas, para luego, cambiarse al modo global de R2\_Conta.

Tome de modelo la configuración anterior, para activar a OSPF bajo el proceso #20 en R2\_Conta y publicar sus redes directamente conectadas. Cuida que cada red se publique bajo la misma área 0 en comun.

Y define la interface pasiva correspondiente

46. Cuando ambos router detecten paquetes de saludo OSPF enviados por el enlace entre ambos, se generara un intercambio de paquetes y finalmente mostrara el siguiente mensaje, confirmando una “adyacencia” OSPF generada entre los router R1\_Ventas y R2\_Conta:

```
R2_Conta(config-router)#
01:35:07: %OSPF-5-ADJCHG: Process 1, Nbr 193.0.0.153 on Serial0/0 from LOADING to
FULL, Loading Done
```

47. Guarde los cambios en R2\_Conta e ingrese en R3\_Admon. Configure OSPF con el proceso #30, pero asegúrese de no publicar la red de enlace con la que alcanza al ISP.

Y configure también a sus 2 interfaces pasivas.

48. Para que R3\_Admon distribuya su ruta estática por defecto hacia el resto de router del Sistema Autónomo, ejecuta el comando: **default-information originate**

49. Compruebe que los diferentes host del SA se pueden ver entre sí y que cada una saluda al equipo externo (internet), gracias al equipo ISP.

50. Guarda los cambios en la configuración de cada router y guarda la simulación general.

## V. ANALISIS DE RESULTADOS

### Ejercicio 1: configuración de RIPv2

Desarrolle la simulación mostrada en la figura 8.2.

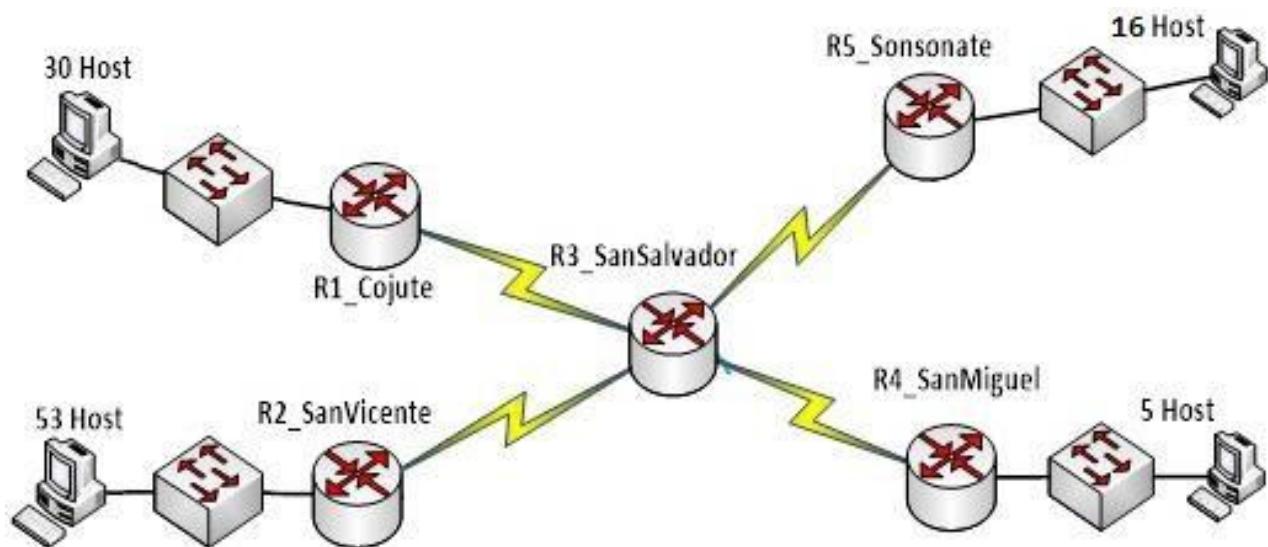
Diseñe un esquema de subneteo que se ajuste a los requerimientos de las redes de la topología.

Utilice como dirección base del subneteo a una dirección ip clase C.

Proceda a configurar el direccionamiento IP de los diferentes host y de las interfaces de los router.

Finalmente, para el enrutamiento dinamico, configure el protocolo RIPv2

**Figura 8.2:** topología de red a configurar con RIPv2



### Ejercicio 2: configuración de OSPF

Desarrolle el subneteo para la topología mostrada en la figura 8.3, iniciando con la ip base 10.0.5.0 /24.

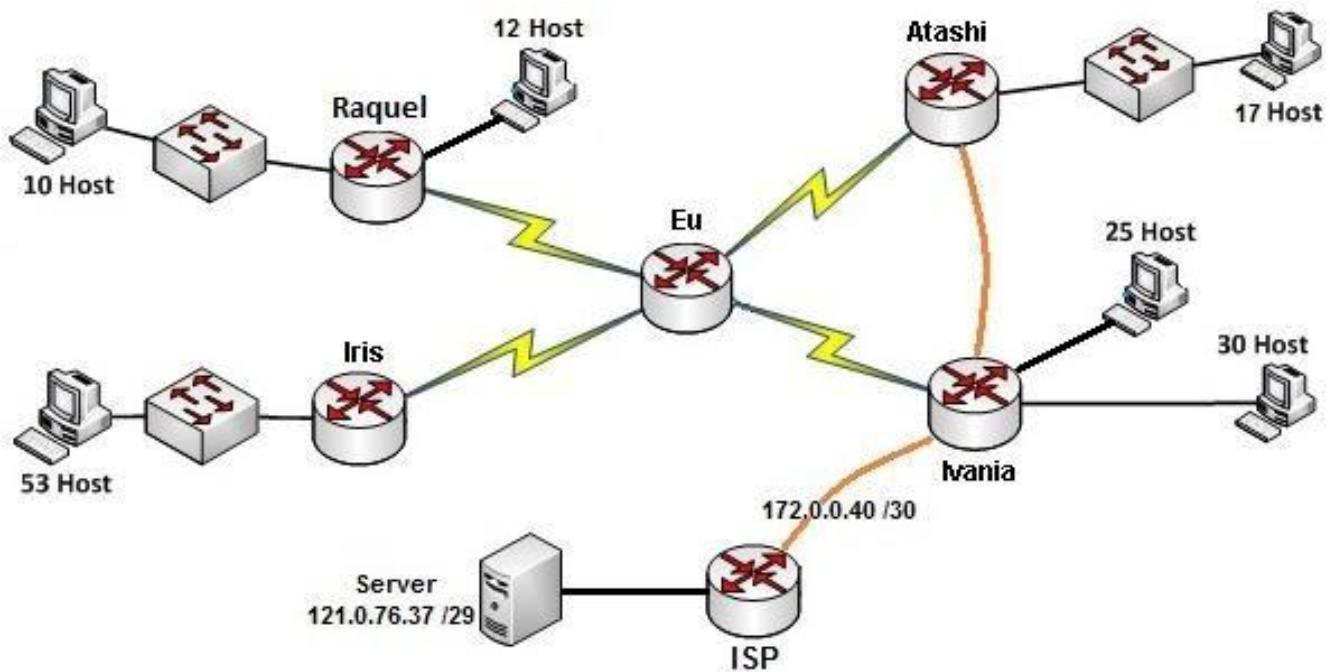
Luego implemente la respectiva simulación en Cisco Packet Tracer.

Recuerde implementar los siguientes aspectos:

- Los enlaces Ivania-Atashi e Ivania-ISP son de fibra óptica.
- El enrutamiento de los router (excepto el ISP) se hará con el protocolo OSPF.
- Deshabilitar envío de paquetes OSPF por las interfaces de conexión hacia redes de usuarios.
- Router Ivania es el router de borde del SA, por lo que este no debe publicar la red privada de enlace con el ISP hacia el dominio de enrutamiento OSPF.
- Así que, debe configurar una ruta por defecto que envíe todo tráfico desconocido al ISP.

- Al router ISP no se le configura ningún protocolo de enrutamiento dinámico. Solamente se le configura una ruta estática sumarizada que resume a todas las redes obtenidas del subneteo y permite enviar así al tráfico hacia cualquiera de las redes internas del SA.

**Figura 8.3:** Topología de red con enrutamiento bajo OSPF



|                                                                                   |                                                                                                                |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
|  |                                                                                                                |
| enero-<br>junio<br>2023                                                           | <p style="text-align: center;"><b>UNIVERSIDAD AUTONOMA DE CHIHUAHUA</b><br/> <b>FACULTAD DE INGENIERÍA</b></p> |

**GUIA DE LABORATORIO #9**

**Nombre de la Practica:** NAT y PAT  
**Lugar de Ejecución:** Laboratorio de Redes  
**Tiempo Estimado:** 2h y 30 min  
**MATERIA:** Redes

## I. OBJETIVOS

- Controlar el acceso a redes privadas desde internet
- Hacer uso de un proveedor de acceso a internet (ISP) para que los equipos de una red privada accedan a la “Nube” (Internet).
- Configurar en el router de Borde de un Sistema Autónomo al proceso NAT estático, NAT dinámico y NAT dinámico con sobrecarga (PAT).

## II. MATERIALES Y EQUIPO

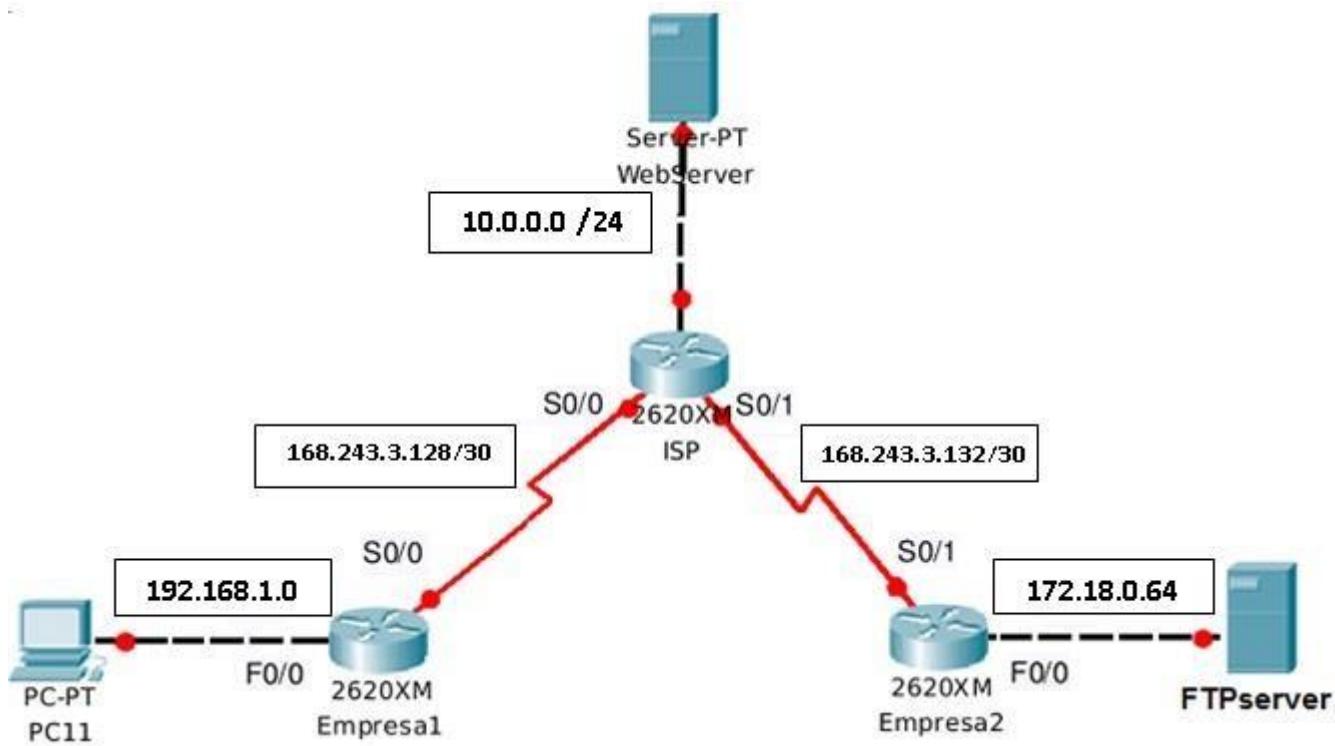
Para la realización de la guía de práctica se requerirá lo siguiente:

| No. | Requerimientos                                              | Cantidad |
|-----|-------------------------------------------------------------|----------|
| 1   | PC con Cisco Packet Tracer instalado                        | 1        |
| 2   | Practica N° 9 de laboratorio                                | 1        |
| 3   | Memoria USB para guardar los ejercicios y Plataforma Moodle | 1        |
|     |                                                             |          |

## III. PROCEDIMIENTO

### Parte 1: Preparación de la topología base

1. Preparar una simulación en Cisco Packet Tracer y llamarla **RAAproc12**. Implementar ahí la topología mostrada en la imagen 9.1 a continuación:



**NOTA:** En esta configuración ambas interfaces del router ISP usarán cables DCE

**Imagen 9.1:** topología inicial a implementar

2. Proceda a realizar la configuración de cada router indicada a continuación.

a. Configuración para Empresa1:

```

Router# configure terminal
Router(config)# hostname Empresa1
Empresa1(config)# interface f0/0
Empresa1(config-if)# ip address 192.168.1.1 255.255.255.0
Empresa1(config-if)# no shutdown
Empresa1(config-if)# exit
Empresa1(config)# interface s0/0
Empresa1(config-if)# ip address 168.243.3.130 255.255.255.252
Empresa1(config-if)# no shutdown
Empresa1(config-if)# exit

```

**b.** Configuración para Empresa2:

```
Router# configure terminal
Router(config)# hostname Empresa2
Empresa2(config)# interface f0/0
Empresa2(config-if)# ip address 172.18.0.65 255.255.255.192
Empresa2(config-if)# no shutdown
Empresa2(config-if)# exit
Empresa2(config)# interface s0/0
Empresa2(config-if)# ip address 168.243.3.134 255.255.255.252
Empresa2(config-if)# no shutdown
Empresa2(config-if)# exit
Empresa2# copy running-config startup-config
```

**c.** Configuración para ISP:

```
Router# configure terminal
Router(config)# hostname ISP
ISP(config)# interface f0/0
ISP(config-if)# ip address 10.0.0.1 255.255.255.0
ISP(config-if)# no shutdown
ISP(config-if)# exit
ISP(config)# interface s0/0
ISP(config-if)# ip address 168.243.3.129 255.255.255.252
ISP(config-if)# clockrate 9600
ISP(config-if)# no shutdown
ISP(config-if)# exit
ISP(config)# interface s0/1
ISP(config-if)# ip address 168.243.3.133 255.255.255.252
ISP(config-if)# clockrate 9600
ISP(config-if)# no shutdown
ISP(config-if)# exit
ISP# copy running-config startup-config
```

3. Configure las estaciones de trabajo y los servidores con el siguiente direccionamiento IP:

a) PC11: Dirección IP: 192.168.1.2, máscara de subred: 255.255.255.0, gateway: 192.168.1.1

b) FTPserver: Dirección IP: 172.18.0.66, máscara de subred: 255.255.255.192, gateway: 172.18.0.65

c) WebServer: Dirección IP: 10.0.0.2, máscara de subred: 255.255.255.0, gateway: 10.0.0.1 4.

Comprobación de direccionamiento IP

a. Visualice la tabla de enrutamiento de los enrutadores Empresa1 y Empresa2, ejecutando al comando show ip route

b. Verificar la tabla de enrutamiento del enrutador ISP.

Observe que debido al carácter de redes privadas que tienen las redes de sus 2 clientes (Empresa1 y Empresa2), la red 192.168.1.0/24 y el conjunto de redes 172.18.0.0 /20 no deben aparecer en la tabla de ISP.

5. Realizar las siguientes pruebas con la herramienta PING desde las estaciones de trabajo y el web server (se anotan a continuación de cada prueba el resultado que debería obtenerse, compárelo con sus propios resultados:

- Ping desde: PC11; hacia: 192.168.1.1; resultado: prueba exitosa
- Ping desde: FTPserver; hacia: 172.18.0.65; resultado: prueba exitosa
- Ping desde: PC11; hacia: 10.0.0.2; resultado: host de destino inaccesible
- Ping desde: FTPserver; hacia: 10.0.0.2; resultado: host de destino inaccesible
- Ping desde: WebServer; hacia: 10.0.0.1; resultado: host de destino inaccesible
- Ping desde: WebServer; hacia: 168.243.3.129; resultado: prueba exitosa
- Ping desde: WebServer; hacia: 168.243.3.133; resultado: prueba exitosa
- Ping desde: WebServer; hacia: 192.168.1.2; resultado: host de destino inaccesible
- Ping desde: WebServer; hacia: 192.168.2.2; resultado: host de destino inaccesible

Nuevamente se hace la aclaración. Los fallos al realizar las pruebas Ping entre las estaciones de trabajo y el servidor, y viceversa, son un comportamiento normal, ya que el enrutador ISP desconoce la existencia de las redes locales privadas de Empresa1 y Empresa2. La comunicación entre estas redes se logrará usando NAT o PAT.

## Parte 2: Configuración de NAT estático en enrutador Empresa1

6. Asignación de una red IP pública para realizar el proceso de traducción.

Las direcciones de carácter público (Globales) para su cliente 1 que configurara el proveedor en su equipo ISP serán las ip host contenidas en la red:

199.6.13.8 / 29

Estas ip globales serán configuradas en el procedimiento restante.

7. Proceda a crear en ISP a la siguiente ruta estática, dirigida al rango de ip público asignado para Empresa1 (ver paso anterior) y referenciando a la ip del próximo paso (La ip 168.243.3.130, configurada en la interfaz de conexión con su cliente Empresa1). ip route 199.6.13.8 255.255.255.248 168.243.3.130

8. Configure una ruta estática por defecto en el enrutador **Empresa1**: ip route 0.0.0.0 0.0.0.0 serial 0/0

9. Ejecute el siguiente código para configurar NAT estático en Empresa1, que permitirá que la dirección privada de PC11 se traduzca a la 1er ip global (**199.6.13.9**) del rango asignado por ISP para este Cliente 1.

Además, se definen aquí a las interfaces de entrada y de salida para el proceso de traducción NAT:

```
Empresa1# configure terminal
Empresa1(config)# ip nat inside source static 192.168.1.2 199.6.13.9
Empresa1(config)# interface f0/0
Empresa1(config-if)# ip nat inside
Empresa1(config-if)# exit
Empresa1(config)# interface s0/0
Empresa1(config-if)# ip nat outside
Empresa1(config-if)# exit
Empresa1(config)# do write
```

Con los comandos anteriores se logra que cada vez que un paquete de la ip local de host PC1 llegue a la interface f0/0 de Empresa1, y este necesite ser enviado a redes externas (por medio de la s0/0), se traducirá su dirección privada a la ip pública **199.6.13.9**

#### 10. Pruebas de conectividad.

Realizar las siguientes pruebas y evaluar sus resultados.

- Ping desde: PC11; hacia dirección del WebServer (10.0.0.2); resultado: prueba exitosa
- Ping desde: WebServer; hacia ip privada de PC1 (192.168.1.2); resultado: host de destino inaccesible
- Ping desde: WebServer; hacia ip publica asignada a PC1 (199.6.13.9); resultado: prueba exitosa

Tal como se ve en las pruebas anteriores, con el uso de NAT ya no es posible hacer *ping* directamente a direcciones locales (este es uno de los objetivos de la práctica), por lo que, si desea acceder a la PC11 desde Internet, deberá hacer referencia a su dirección pública asignada con NAT.

11. Finalmente, desde el enrutador Empresa1, revise el estado de la traducción de direcciones ip's privadas-publicas, ejecutando al comando: show ip nat translation

### Parte 3: Configuración de traducciones dinámicas en enrutador Empresa1

12. Desconecte a PC11 de Empresa1. En su lugar, agregue un Hub a la red local del Cliente1 y conecte uno de sus puertos a la Fa0/0 de Empresa 1. Conecte a PC11 a uno de los puertos libres del Hub.

Agregue una nueva PC (llamada **PC12**) a la red del Cliente 1 y configure la siguiente dirección IP: **192.168.1.3/24**. Luego conectarlo al HUB, para expandir así a la red local de Empresa1.

13. Desde el nuevo host, repita las pruebas de conectividad del último paso de la parte anterior de este procedimiento.

Notará que aun es imposible acceder a redes externas desde otra dirección local que no sea la ip 192.168.1.2.

14. Si se mantiene este esquema de traducción estática de direcciones, se haría necesario crear una traducción para cada dirección privada de manera manual e individual.

Para solventar esta situación, activaremos una traducción basada en un grupo de direcciones públicas, que serán asignadas dinámicamente por orden de llegada con respecto a las direcciones privadas.

15. Elimine las traducciones desarrolladas por NAT y luego vuelva a ver los procesos de traducción de ip's:

```
Empresa1# clear ip nat translation *
```

```
Empresa1#show ip nat translations
```

| Pro | Inside global | Inside local | Outside local | Outside global | --- | 199.6.13.9 | 192.168.1.2 | --- |
|-----|---------------|--------------|---------------|----------------|-----|------------|-------------|-----|
| --- |               |              |               |                |     |            |             |     |

```
Empresa1#
```

El comando ***clear ip nat translation \**** elimina el contenido actual de la tabla de traducción NAT.

Al ejecutar el comando show de la última línea podrá verificar que la traducción anterior aun existe, porque esta traducción ha sido definida de manera estática.

16. Cree el siguiente pool (**grupo1**), que reservara las proximas 2 de las direcciones públicas disponibles para usarlas en un futuro proceso NAT dinámico:

```
Empresa1# configure terminal
```

```
Empresa1(config)# ip nat pool grupo1 199.6.13.10 199.6.13.11 netmask 255.255.255.248
```

```
Empresa1(config)# do write
```

17. Crear la lista de acceso estándar 1 a continuación, que permite comparar las direcciones de origen (privadas), para decidir si luego estas serán traducidas a direcciones públicas (globales).

En esta demostración, incluiremos en el derecho a ser traducidas a toda la red 192.168.1.0 / 24.

```
Empresa1# configure terminal
```

```
Empresa1(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

```
Empresa1(config)# CTRL+Z
```

18. La lista de acceso anterior NO SE DEBE APLICAR a ninguna interface del router.

Recuerde que esta ACL 1 se usa solo para efectos de comparar el origen de los paquetes y tomar la decisión sobre la traducción. No se usa la lista de acceso para afectar al tráfico entrante o saliente en las interfaces involucradas en la traducción.

19. Ahora se configurará la traducción dinámica con base en el pool y la lista de acceso creada previamente.

**EMPRESA1(config)# ip nat inside source list 1 pool grupo1**

No es necesario volver a definir el sentido de la traducción (inside / outside), ya que si recuerda eso ya se ha configurado en la traducción estática y no debe cambiarse (f0/0 inside; s0/0 outside).

20. Haga una prueba Ping desde PC12 hacia la ip 10.0.0.2. En este caso la traducción se llevará a cabo correctamente y se obtendrá una respuesta exitosa. Revise de nuevo el estado de las traducciones usando el comando: **show ip nat translation**

21. Veamos que sucede cuando las traducciones requeridas exceden el número de direcciones públicas que comprenden el pool. Hacer los siguientes cambios en la red local de Empresa1:

- Expanda la red, agregando 3 PC mas, para conectarlas al Hub. Asignarles las ip **192.168.1.4**, **192.168.1.5** y **192.168.1.6**, respectivamente.
- Desde host 192.168.1.4, haga ping a la ip 10.0.0.2
- Desde host 192.168.1.5, haga ping a la ip 10.0.0.2
- Revise las traducciones nat en Empresa1. Notará que por cada ip privada de los host anteriores, se crea una nueva traducción para acceder a redes externas.
- Desde el host con ip 192.168.1.6; haga ping a: 10.0.0.2.

En este último caso podrá notar que la prueba Ping no tiene éxito. Esto se debe a que el pool de direcciones públicas (de 199.6.13.10 hasta 199.6.13.11) se ha agotado.

- Espere unos 10 segundos, para intentar nuevamente la comunicación desde el host 192.168.1.6 hacia la ip 10.0.0.2. La prueba deberá ser exitosa, debido a que el router Empresa1 retiro la asignación de la ip publica a uno de los primeros host que accedieron a internet y que ya no la volvieron a utilizar.

22. Limpie las traducciones nat en Empresa1 con el comando siguiente:

**EMPRESA1# clear ip nat translation \***

23. Ejecute nuevamente la prueba ping desde la PC que dio resultado no exitoso en el paso anterior. Ahora si se tendrá éxito.

Revise el estado de las traducciones, para confirmar que las anteriores fueron eliminadas y ahora solo queda la ip publica que se utilizó para el host de esta prueba.

24. Guarde los últimos cambios de configuración en Empresa1 y reinicie su IOS, con el comando **reload**.

#### **Parte 4: Configuración de NAT Sobrecargado en enrutador EMPRESA2**

25. Modificar router Empresa2 con las siguientes características y configuraciones:

- Conectar una nueva interface fastethernet, configurarle la dirección **172.18.0.129 /27** y levantarla. Conectar a esta interface un nuevo host, asignándole la ip **172.18.0.130 /27** y su respectiva ip de gateway.
- Crear una red de manera virtualizada con la **Loopback 3**, asignándole la dirección **172.18.0.161 /28**. - Desde FTPserver, comprobar con **ping** que saluda exitosamente al nuevo host y también a la ip de Lo3.

26. Ahora analice el siguiente escenario que describirá la topología de red privada del Cliente 2 a implementar en los pasos restantes.

- Este Cliente 2, tendrá un router de borde denominado **Empresa2** y usara el mismo ISP.
- Se expandirá su red interna mostrada en la Figura 12.1 (al inicio de este proc.) a un total de 3 redes diferentes:
  - Red 1:** 172.18.0.64 /26 (de FTPserver, ya configurada)
  - Red 2:** 172.18.0.128 /27
  - Red 3:** 172.18.0.160 /28
- El server FTPserver debe ser alcanzado desde el exterior (internet).
- El host de la red 3, implementado en la Lo 3, virtualizara a un Server, el cual deberá ser visto desde internet.
- Solamente la mitad superior del rango de ip de los host de la red 2 tendrán acceso a internet. Al resto de host se les permitirá solamente comunicación interna con el resto de redes privadas del mismo cliente.
- Este cliente ha comprado de su ISP solamente 3 direcciones públicas (**100.0.0.33/28**, **100.0.0.34/28** y **100.0.0.35/28**).

27. Según el escenario anterior, las condiciones se vuelven muy críticas, ya que las direcciones públicas adquiridas, deben ser distribuidas entre los 2 servidores y las estaciones de trabajo de la LAN que deberán acceder a internet por medio de router EMPRESA2.

28. Para iniciar la solución, a continuación se describe la configuración de NAT estático en Empresa2, que asigna la 1er ip publica (**100.0.0.33 /28**) al FTPserver, para que este pueda tener acceso hacia/desde internet.

Y de igual manera, se asigna la 2da ip publica (**100.0.0.34 /28**) al server virtualizado con la Lo3. Y se definen las interfaces de entrada (direcciones privadas) de NAT y la interface de salida (direcciones públicas).

```
Empresa2(config)#ip nat inside source static 172.18.0.66 100.0.0.33
Empresa2(config)#ip nat inside source static 172.18.0.161 100.0.0.34
Empresa2(config)#interface fastEthernet 0 / 0
Empresa2(config-if)#ip nat inside
Empresa2(config-if)#exit
Empresa2(config)#interface fastEthernet 1 / 0
Empresa2(config-if)#ip nat inside
```

```

Empresa2(config-if)#exit
Empresa2(config)#interface Lo 3
Empresa2(config-if)#ip nat inside
Empresa2(config-if)#exit
Empresa2(config)#inter serial 0/1
Empresa2(config-if)#ip nat outside
Empresa2(config-if)#do write
Empresa2(config-if)#exit

```

- Observe como la Lo 3 se convierte en una interface de entrada de NAT.

29. Configure una ruta por defecto en Empresa2, que utilice la interface de salida **Serial 0/1** con la que se conecta al ISP.

30. En ISP, configure la manera de cómo este dispositivo deberá alcanzar la red privada de su cliente 2, referenciando con rutas estáticas a solamente las 3 ip publicas que este proveedor le vendió.

```

ISP(config)# ip route 100.0.0.32 255.255.255.252 168.243.3.134 ISP(config)#
ip route 100.0.0.35 255.255.255.255 168.243.3.134

```

31. Haga pruebas de ping desde WebServer dirigidos a la ip pública (**100.0.0.33**) asignada al FTPserver. La prueba debe ser exitosa.

De igual forma, desde host PC11, ejecute ping dirigido a la ip pública (**100.0.0.34**) asignada para la Lo3. La prueba también debe ser satisfactoria.

32. Hasta este momento, ya solo queda disponible una ip publica (**100.0.0.35**) adquirida al proveedor ISP, y con ella debe darse acceso a internet a solamente a la mitad superior de ip's de la Red2 (172.18.0.128 /27).

Este rango de ip que tendrán internet incluye desde la ip 172.18.0.144 hasta la 172.18.0.158. Veamos cómo es posible solventar este problema usando PAT.

33. Ejecute la siguiente configuración de PAT (NAT Overloaded) en Empresa2. Analice los comentarios previos en cada bloque.

|                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------|
| Configura una pila, formada por una “única dirección” 100.0.0.35 como inicio y final del rango de ip publicas aun disponibles para NAT. |
|-----------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                            |
|--------------------------------------------------------------------------------------------|
| <b>Empresa2(config)#ip nat pool cliente2 100.0.0.35 100.0.0.35 netmask 255.255.255.240</b> |
|--------------------------------------------------------------------------------------------|

|                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Crea la ACL 2 para determinar las redes que tendrán acceso al proceso NAT y alcanzar así internet.<br>En este caso, solo se aceptaran ip de la mitad superior del rango de ip's de la Red 2. |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------|
| <b>Empresa2(config)#access-list 2 permit 172.18.0.144 0.0.0.15</b> Empresa2(config)# <b>access-list 2 deny any</b> |
|--------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------|
| Crea a NAT de manera sobrecargada ( <i>overload</i> ), utilizando la pila de direcciones públicas cliente2 y como filtro a la ACL 2. |
|--------------------------------------------------------------------------------------------------------------------------------------|

```
Empresa2(config)#ip nat inside source list 2 pool cliente2 overload
```

34. Desde la PC de la Red 2 ejecute un ping hacia la ip 10.0.0.2; resultado: falla, porque su ip actual (**172.18.0.130 /27**) no tiene acceso a internet.

Cambiar su ip asignada a **172.18.0.153 /27** y repetir la prueba de comunicación. Esta vez si se le permitirá acceder a Internet.

35. Notara que al usar la sobrecarga en la traducción de direcciones de forma dinámica, ya no hay mayores problemas si nuestro pool de direcciones públicas es más pequeño que el número real de direcciones privadas a traducir.

#### Parte 5: Expandiendo la red del proveedor ISP

36. Guardar las configuraciones actuales de cada router y la simulación en general. Luego, hacer una copia de la simulación actual bajo el nombre **RAAproc12extra**.

37. Agregue un router y cambiarle de nombre a **Borde3**.

Este enrutador hará las funciones del router de borde de un tercer cliente (Cliente 3) del mismo proveedor propietario del router ISP inicial.

Modificar los módulos de interfaces de Borde3 para permitir un enlace de fibra óptica y los módulos

FastEthernet y/o Ethernet que considere necesarios **Tabla 1:** Redes a implementar en Borde3 para implementar las redes indicadas en la Tabla 1.

| #     | Ip Red          |
|-------|-----------------|
| Red 1 | 180.0.0.0/29    |
| Red 2 | 180.0.0.16 /28  |
| Red 3 | 180.0.0.32 /28  |
| Red 4 | 180.0.0.64 /27  |
| Red 5 | 180.0.0.128 /25 |

38. Proceda a configurar en Borde3 a c/u de las interfaces agregas en la subred que le corresponda. Conecte una nueva PC por cada interface configurada y modifique su ip para integrarla a la subred correspondiente.

Luego genere la tabla de enrutamiento de Borde3 y confirme la lista de redes solicitadas en la Tabla 1.

39. Agregar un nuevo router y configurarlo con el hostname como **ISP2**. Este equipo es de la misma empresa proveedora de internet del router ISP.

Ahora desarrolle las siguientes tareas sobre este ISP2:

+ Agregue un modulo de interface para conexión de fibra óptica.

+ Implemente un enlace T1 entre ambos router (ISP e ISP2) del proveedor y configurar los extremos de este enlace bajo la red 168.244.0.0 /30.

+ Para que ambos router intercambien a las redes públicas de sus diferentes clientes, levante en ambos al protocolo EIGRP bajo el SA 500.

A continuación se muestra la configuración que deberá ejecutar en cada router del proveedor de internet:

|                                                                                                                                                                                                                                               |                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <pre> ISP(config)#router eigrp 500 ISP(config-router)#network 168.244.0.0 ISP(config-router)#network 10.0.0.0 ISP(config-router)#passive-interface fastEthernet 0/0 ISP(config-router)#redistribute static ISP(config-router)#do write </pre> | <pre> ISP2(config)#router eigrp 500 ISP2(config-router)#network 168.244.0.0 ISP2(config-router)#do write </pre> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|

Observe que ISP no publica a ISP2 la red privada de su Cliente 1 ni la ip-red física compartida con el router de borde Empresa1.

Solamente redistribuye las rutas estáticas con el rango de ip públicas que le asigno a su cliente para que sus usuarios accedan a internet.

40. Genere la tabla de enrutamiento de ISP2, para identificar cuáles son las redes que este conoce para alcanzar la red privada de Empresa1

De igual forma, determine si este alcanzaría a ver a las redes del otro cliente (Empresa2). Guardar las configuraciones de cada router modificado.

10. Llame a su instructor para demostrarle el resultado de cada una de las siguientes pruebas de comunicación:

- a) Desde ISP2, enviar ping hacia la ip pública asignada a PC11 (el cliente publicado desde Empresa1).
- b) Desde WebServer, ping hacia la ip pública asignada a la Lo3 de Empresa2
- c) Desde PC11, ping hacia la ip de la interface de conexión serial de ISP2.

41. Tome de ejemplo la configuración ejecutada entre router (ISP y Empresa2), para luego hacer las configuraciones indicadas a continuación que permitan conectar al Cliente 3 (cuyo router de borde es **Borde3**) al ISP2, para acceder a la red pública (internet) administrada por este proveedor de internet:

a) Hacer la conexión entre ISP2 y Borde3 con fibra óptica, configurando la ip 168.243.3.137 /30 en el extremo de ISP2 y la otra ip en el puerto de conexión de Borde3.

b) **El proveedor ha vendido un total de 4 ip's públicas a su cliente 3, iniciando en la 102.0.0.97/28 hasta 102.0.0.100/28.**

c) Cliente 3 usara la 1er ip asignada por el proveedor de internet para publicar el host conectado a su Red 5.

Configurar NAT dinámico sobrecargado con las siguientes 2 direcciones públicas disponibles para que los usuarios de las redes restantes, excepto la Red 2, puedan acceder a internet.

d) Hacer los cambios necesarios en ISP2, para que redistribuya a ISP las ip públicas de su cliente 3.

42. Llamar a su instructor, para que este ejecute las pruebas necesarias que demuestren que cada uno de los 3 clientes del proveedor de internet se comunican haciendo uso de NAT.

## Parte 6: Traducción estática de Puertos (PAT), ejemplo 2

43. Reemplazar al host conectado a la Red 2 por un Server. Configurar a este Server con la misma ip que tenía el host que sustituyo, y cambiar su nombre a **ServerHTTP**.

44. Ingresar a ficha Config del nuevo Server y confirmar que tiene activados todos los servicios.

45. Ahora, se publicara a Internet este Server utilizando la última ip pública disponible. Pero se restringirá su acceso desde internet para acceder solamente a su servicio de páginas web (protocolo http, puerto 80).

Ingresar al modo global de Borde3 y ejecutar el siguiente comando:

```
ip nat inside source static tcp 180.0.0.18 80 102.0.0.100 80
```

46. Luego, observe las traducciones de nat registradas en Borde3. Vera que existen solamente las 2 traducciones estáticas ya configuradas.

47. Desde un host de Empresa1 que tenga acceso a internet, envíe un ping dirigido a la ip publica asignada a ServerHTTP. Vera que no se obtiene respuesta alguna.

Ver las estadísticas de NAT en Borde3 y confirme que no hay traducciones NAT ejecutadas

48. Desde el host seleccionado en el paso anterior, ingresar a ficha Desktop y seleccionar WebBrowser. Escribir ahí a la ip publica de ServerHTTP. Se cargara la pág. Web predeterminada.

Ver nuevamente las estadísticas de NAT en Borde3 y confirme que esta vez, se tradujo la ip publica de ServerHTTP a su ip privada.

49. Expanda la red 2, agregando un Hub y otro Server.

Cambiar nombre de este nuevo Server a **ServerFTP** y asignarle la ultima ip disponible de la Red 2 y su respectivo Gateway.

Conectar ambos servidores al Hub y este ultimo al puerto de la Red en Borde3.

50. Ingresar al modo global de Borde3 y ejecutar el siguiente comando:

```
ip nat inside source static tcp 180.0.0.30 21 102.0.0.100 21
```

Observe que se utiliza la misma ip global asignada al ServerHTTP, pero la ip local es la del ServerFTP y tambien, ambos puertos son del servicio FTP (puerto 21) bajo el protocolo TCP.

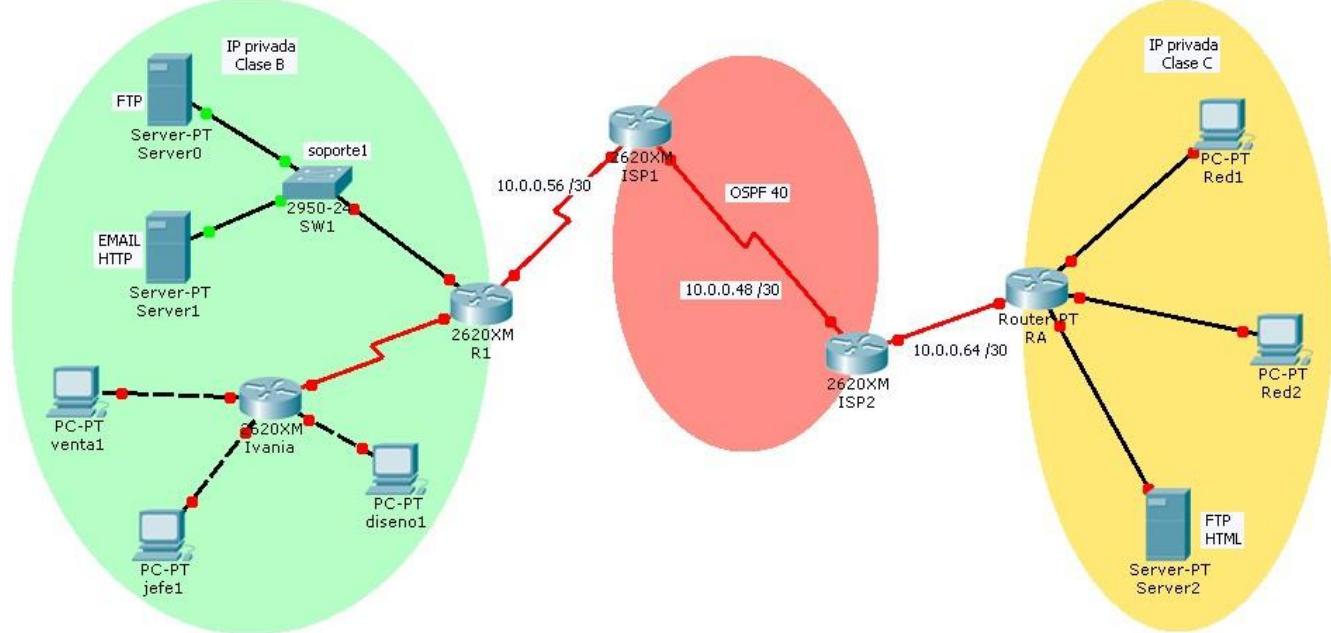
51. Ingresar a ficha Config de ServerFTP y ver la cuenta de usuario predeterminada el servicio FTP. Ir a la red de la Empresa2 y seleccionar un host que tenga derecho a acceder a Internet, ingresar a su Command Prompt y digitar comando: ftp 102.0.0.100

Observe que se intenta acceder al ServerFTP, pero usando la misma ip publica asignada al ServerHTTP. La clave de funcionamiento radica en la sobrecarga de puertos (PAT).

Se usa la misma ip global en ambas traducciones estáticas, pero referenciando a una ip interna diferente y usando un puerto público específico en cada traducción.

## IV. ANALISIS DE RESULTADOS.

En una nueva simulación de Cisco Packet Tracer, desarrolle la siguiente topología de red:



Por cada dominio de red privado, seleccione una ip privada del tipo indicado en cada área, para luego realizar el subneteo correspondiente.

Los requerimientos de red para el dominio privado conectado por ISP1, es el siguiente:

| Red    | Host | Red              | Host |
|--------|------|------------------|------|
| Ventas | 200  | Servicios        | 16   |
| Jefes  | 100  | Enlace Ivania-R1 | 2    |
| Diseño | 25   |                  |      |

ISP1 ha vendido 2 direcciones públicas (196.0.0.14/29 y 196.0.0.15/29) a su cliente.

Diseñe un plan de direccionamiento con NAT/PAT que permita que los diferentes servicios internos (FTP y HTTP) puedan ser vistos desde internet, así como también, permita acceso a internet al resto de clientes de toda la topología internet

Con respecto al cliente conectado al ISP2. Los requerimientos de host de cada una de las redes internas del dominio conectado por ISP2 son:

Red 1 (30 host)

Red 2 (40 host)

Servicios (12 host).

El proveedor ISP2 ha vendido las direcciones ip 198.0.0.67/29, 198.0.0.68/29 y 198.0.0.69/29, para que su cliente pueda acceder y publicar recursos hacia internet.

Cada servicio de red indicado en el diagrama podrá ser alcanzado desde internet, pero usando una ip pública diferente. El resto de servicios no deben ser publicados.

Solamente los clientes de la Red 2 podrán acceder a internet.

Hacer las configuraciones entre ambos router del ISP para que se logre la comunicación entre ambos clientes.

Cada router (ISP1 e ISP2) del proveedor de internet debe bloquear (denegar) los paquetes que sean enviados por su respectivo cliente, que vayan con una ip origen que no sean las ip públicas vendidas al mismo.

Para cumplir este objetivo, investigue a detalle el concepto de ACL (Access Control List).



**UNIVERSIDAD AUTONOMA DE  
CHIHUAHUA  
FACULTAD DE INGENIERÍA**

Enero junio  
2023

**GUIA DE LABORATORIO #10**  
**Nombre de la Practica:** Simulador GNS3  
**Lugar de Ejecución:** Laboratorio de Redes  
**Tiempo Estimado:** 2 horas y 30 minutos  
**MATERIA:** Redes

## **I. OBJETIVOS**

Al finalizar esta práctica, el estudiante podrá:

- Reconocer el entorno de trabajo para diseño y pruebas de topologías de red implementadas con la aplicación GNS3.
- Diseñar topologías de redes locales bajo GNS3.
- Levantar imágenes binarias de IOS de dispositivos switches.

## **II. INTRODUCCION TEORICA**

### **1. Simulador de Redes GNS3**

GNS3 es un simulador de red muy potente que permite mediante un entorno gráfico dibujar y configurar topologías de red complejas, para posteriormente simular su comportamiento.

Este software soporta configuración y emulación de dispositivos de interconexión, routers, con sistemas operativos IOS CISCO; permite incorporar hosts (maquinas Linux, MAC OS, Windows).

Además, simula niveles de enlace diversos como Ethernet, Frame Relay, ATM, etc., así como dispositivos de interconexión del nivel de enlace como SWITCH.

GNS3 puede extender el diseño de la topología virtual de la red, para incluir conexiones a equipos de red y redes completas externas.

1 / 10

Para realizar esta magia, GNS3 se fundamenta, depende en las siguientes aplicaciones complementarias:

- **Dynamips:** Es un emulador de routers Cisco escrito por Christopher Fillot. Emula al software real de las plataformas 1700, 2600, 3600, 3700 y 7200, y ejecuta imágenes de IOS estándar de switches. De esta forma, prueba y experimenta las funciones del Cisco IOS.
- **Dynagen:** es una interface front end basado en texto para Dynamips escrito por Greg Anuzelli, utilizada por GNS3 para interactuar con Dynamips. GNS3 utiliza la consola de administración de Dynagen para que los usuarios listen los dispositivos, suspender y recargar instancias, determinar y administrar los valores de idle-pc, realizar capturas, y mucho más.

## Instalando GNS3

GNS3 se puede ejecutar en Windows, Linux y sobre Mac OS X. GNS3 requiere que se cumplan las siguientes dependencias (versiones) de los componentes:

|           |               |             |                                         |
|-----------|---------------|-------------|-----------------------------------------|
| Qt >= 4.3 | Python >= 2.4 | PyQt >= 4.1 | Sip >= 4.5 si requiere compilar<br>PyQt |
|-----------|---------------|-------------|-----------------------------------------|

Bajo Windows, debe instalar el paquete Windows all-in-one, que provee lo necesario para que GNS3 se ejecute en máquinas locales o remotas, excepto las imágenes de IOS.

Los usuarios Linux deben descargar Dynamips y extraerlo en alguna ubicación. Luego instalar las dependencias de GNS3 y finalmente ejecutar GNS3.

## Imágenes IOS

Gracias a Dynamips, GNS3 puede ejecutar imágenes de Cisco IOS reales.

En Windows, los archivos de imágenes IOS de Cisco se ubican por defecto bajo la carpeta:

**C:\Program Files\Dynamic\images**

En sistemas Linux/Unix, la ubicación sugerida es **/opt/images**

Las imágenes del Cisco IOS se ofrecen comprimidas. Estas imágenes comprimidas funcionan bien con Dynamips, aunque el proceso de arranque es significativamente más lento debido a la descompresión (igual que en los routers reales). Es recomendable que previamente descomprima las mismas.

### **Utilización de Recursos requeridos por Dinamics**

Dynamips hace uso intensivo de memoria RAM y del CPU para generar la magia de la emulación.

Por ej. Si bajo una simulación GNS3 se pretende ejecutar una imagen de IOS que requiere 256 MB de RAM (en un router 7200 real), consumirá 256 MB de RAM de la maquina real para levantar la instancia virtual del router.

También utiliza (por defecto) 64 MB de RAM por cada instancia en un sistema Unix (16 MB en Windows).

Y hace uso intensivo de CPU, porque está emulando la CPU de un router instrucción-por-instrucción. En principio no tiene manera de saber cuándo el router virtual está en estado ocioso (idle), por esa razón ejecuta cuidadosamente todas las instrucciones que constituyen las rutinas de idle del IOS, al igual que las instrucciones que conforman el “real” funcionamiento.

Pero una vez que haya ejecutado el proceso de “Idle-PC” para una determinada imagen de IOS, la utilización de CPU decrecerá en forma drástica.

### III. MATERIALES Y EQUIPO

Para la realización de la guía de práctica se requerirá lo siguiente:

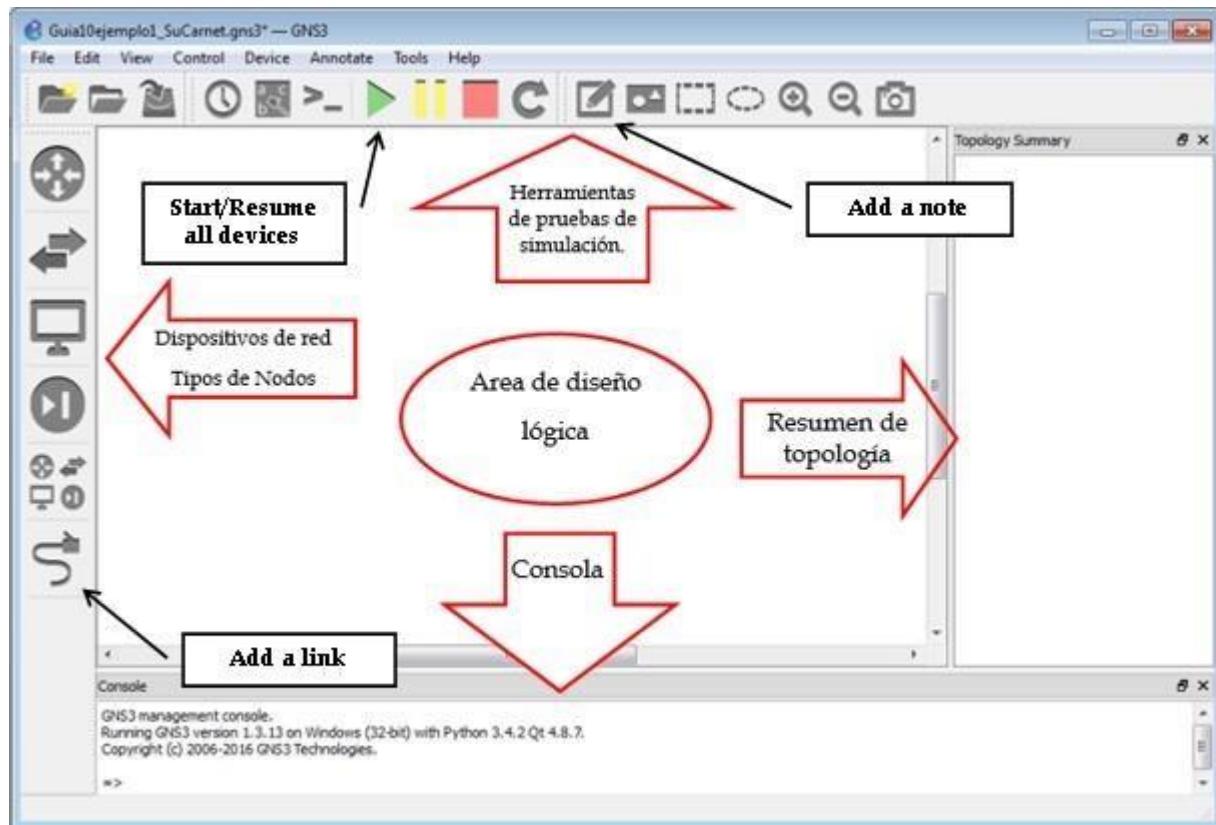
| No. | Requerimiento                                           | Cantidad |
|-----|---------------------------------------------------------|----------|
| 1   | Guía # 10 de Redes                                      | 1        |
| 2   | PC con el software de simulación “GNS3”                 | 1        |
| 3   | Archivo de imagen .bin o .zip de IOS de un router Cisco | 1        |
|     |                                                         |          |

### IV. PROCEDIMIENTO

#### Parte 1: Diseñando una simulación de red con GNS3

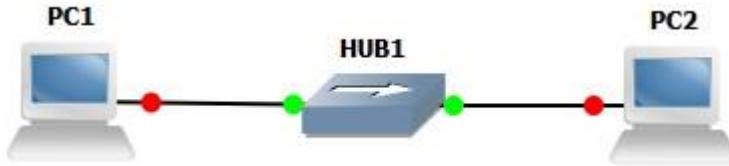
1. Active su PC y acceda a la aplicación *GNS3* instalada ahí
2. Se solicita el nombre del proyecto bajo el cual se guardara la topología de red.

**Imagen 10.1:** Entorno de trabajo de GNS3



3. De clic en botón Buscar (Browse) y ubique la carpeta del Escritorio. Como nombre asigne **Guia10ejemplo1\_SuCarnet**. Reemplace (**Sucarnet**) por su carnet correspondiente.
4. Como se muestra en la imagen 10.1, el área para diseño de la simulación se divide en barras de herramientas.
5. A continuación, diseñara una topología en estrella, que incluya 2 host conectados a un Hub Ethernet (ver imagen 10.2).

**Imagen 10.2:** Topología en estrella a implementar



6. De la barra de “tipos de nodos” (ver imagen 10.1) ubique y de clic en el ícono de “Browse End Device”. La barra se expande para mostrar los dispositivos disponibles. Seleccione al dispositivo VPCS y arrástrelo al área de trabajo.

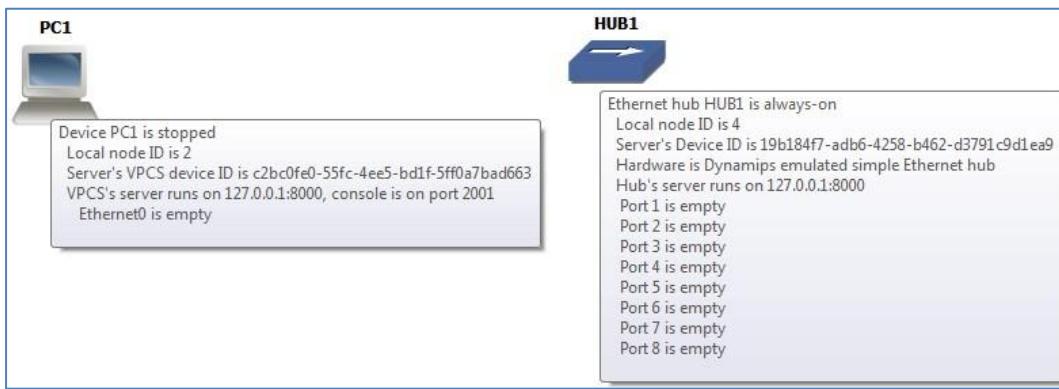
Se mostrara un dispositivo de host final virtualizado, asignándole un nombre de PC1.

7. Repita el paso anterior para agregar a otro VPC.
8. Busque la categoría de “Browse Switches” y de los nodos, ubique y arrastre a un dispositivo “Ethernet Hub” al área de trabajo.
9. Guarde los cambios de su proyecto, ubicando del menú principal a opción “File” y en “Save project” (o las teclas Ctrl + S).
10. Observe la barra “Resumen de topología”. Le indica los nombres de los dispositivos agregados y su estado de funcionamiento.
11. Ubique el cursor del ratón sobre PC1 y confirme (como muestra la Imagen 10.3) que esta desactivada, cuenta con solamente un puerto Ethernet y este esta desconectado (empty).

Repita la acción sobre Hub1 y determine el estado y su lista de puertos (y estado de conexión) disponibles.

12. Ahora, para conectar a los dispositivos. De los “tipos de nodos”, seleccione el botón “Add a link”. Desplace el ratón sobre el área de trabajo y vera que cambio de forma.
13. De clic sobre PC1 y seleccione su único puerto disponible (Ethernet 0). Luego de clic sobre Hub1 y seleccione el puerto Ethernet1. Ambos dispositivos se conectarán entre sí. Coloque nuevamente el ratón sobre PC1 y Hub1, para analizar el estado de conexión de sus puertos.

**Imagen 10.3:** descripción del estado de funcionamiento y puertos de cada dispositivo de la topología



14. Finalmente, conecte a PC2 con el puerto 5 de Hub1.

Presione tecla Esc para desactivar el modo de conexión con el ratón.

15. Guarde los cambios de su proyecto actual.

#### Parte 2: Ejecución de la simulación y configuración ip de los host

16. De la barra superior, ubique el botón “Start/Resume on devices”, para iniciar la ejecución de la topología actual.

17. Ahora, debe configurar el protocolo IP de ambos host para que puedan comunicarse por medio del hub.

18. Inicie la configuración de PC1. De doble sobre la misma, para generar una ventana de consola, desde la cual podrá ejecutar comandos de verificación y configuración.

19. En el cursor escriba al símbolo ? y presione Enter. Se mostrara una descripción general de los diferentes comandos disponibles y sus argumentos.

20. Ejecute el comando **show ip all**, para ver el direccionamiento IP asignado a PC1.

21. Ejecute el siguiente comando, el cual asignara la ip: 192.168.0.3 /24 al host PC1:

**ip 192.168.0.3/24**

Ejecute el comando show del paso anterior y confirmar el cambio.

22. Guarde la configuración de PC1, ejecutando al comando **save**.

23. Ingrese a la consola de PC2, para asignarle la dirección ip 192.168.0.7 /24, confirme el cambio de dirección y guarde sus cambios.

24. Desde la consola de PC2, verifique que se realiza la comunicación con PC1, ejecutando el comando ping dirigido a la de PC1.

25. Cierre las ventanas de consola y luego, suspenda la ejecución de la simulación, dando clic sobre el botón “Stop all devices” en la barra superior de la ventana.

**Parte 3: Montando la imagen .bin del IOS de un Router.**

26. Revise las series de router ya montados en GNS3, haciendo clic en el icono “Browse Routers”.

27. Solicite a su instructor la imagen del IOS del router que montara en GNS3 y cópiela en el Escritorio.

28. Haga clic en la opción de menú: Edit -> Preferences.

29. En la nueva ventana, seleccione la opción Dynamips -> IOS routers.

Confirme la lista de imágenes de los IOS ya configuradas en GNS.

30. De clic en el botón New. Se inicia un asistente de instalación.

De clic en botón Browse y seleccione la imagen .bin previamente ubicada en su Escritorio.

GNS3 le preguntara si desea descomprimir la imagen del IOS seleccionado. Responda que sí.

31. Si la descompresión es correcta, retornara a la ventana del asistente. Observe la URL en donde se descomprimirá la imagen .bin del IOS elegido.

32. De clic en botón Next. Se muestran el nombre, la plataforma (serie) y el tipo de dispositivo para el cual va orientada la IOS seleccionada. De clic en Next.

Se sugiere la memoria RAM mínima que requiere el dispositivo para que su IOS funcione. De clic en Next.

33. Ahora, debe seleccionar los puertos Fastethernet con los cuales contara el router cuando sea utilizado en las simulaciones. Solicite a su instructor cual será la elección de puertos a configurar.

34. De clic en Next. Se solicita los módulos de puertos seriales (T1) que tendrá el dispositivo. Seleccione 2 módulos WIC-2T. De esta forma, constara de 4 puertos seriales.

35. En el siguiente paso del asistente, se solicita el identificador idle-PC. De clic en botón “idle-PC finder” para que GNS3 le genere el valor correspondiente.

Espere hasta que se genere el **idle-PC** y luego de clic en Finalizar.

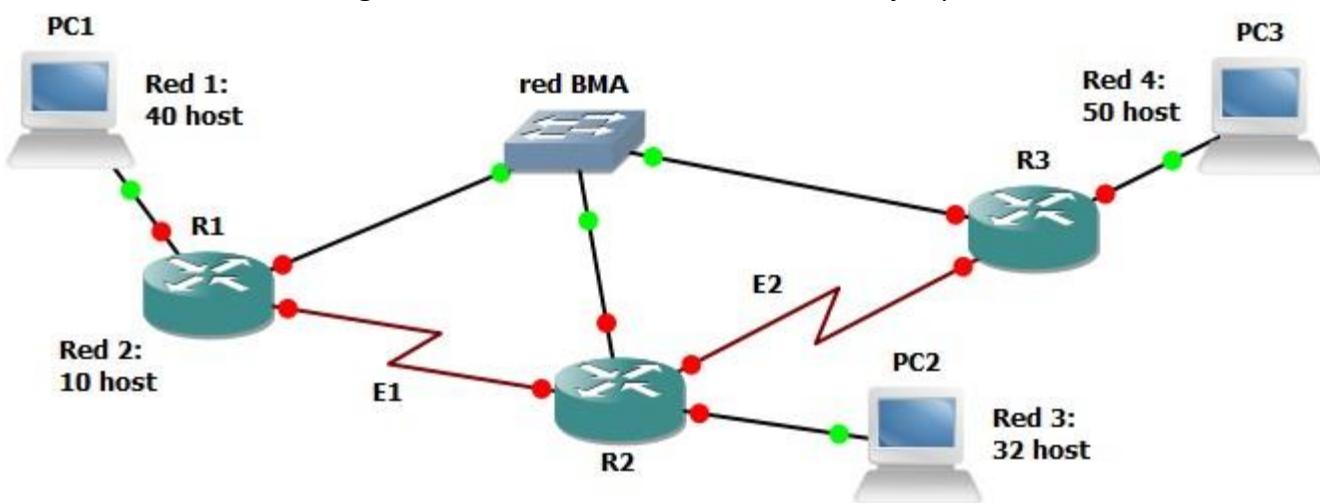
36. Retornara a la lista de IOS disponibles. Confirme que la imagen elegida ya se agregó al listado. Revise la memoria RAM y los tipos de puertos elegidos.

Si todo es correcto, de clic en el botón inferior “Apply” y cierre la ventana de configuración.

37. Guarde su proyecto actual y de clic en opción de menú File -> New black Project

Asigne el nombre **Guia10ejemplo2\_SuCarnet**

38. En esta nueva simulación, proceda a levantar la simulación mostrada en la imagen 10.4.

**Imagen 10.4:** Simulación a desarrollar en el Ejemplo 2.**Importante:**

- Para visualizar los nombres de las interfaces que se conectan, puede hacer clic en botón *Show/Hide interfaces labels*.
- En las conexiones entre pares de router-host y de router-Switch, se usaran interfaces Ethernet o FastEthernet.
- En los enlaces R1-R2 y R2-R3 se usaran enlaces seriales (T1).

39. Solicite a su instructor la dirección ip de red que utilizará para realizar el subneteo requerido para la topología a implementar y anótela aquí: \_\_\_\_\_ / \_\_\_\_\_

40. Desarrolle el cálculo del Subneteo correspondiente. Para el mismo, tome en cuenta las siguientes aclaraciones:

- La red 2 se implementará de forma virtual con la interface Loopback 2.
- La red BMA (Broadcast Multiple Access) será una red compartida entre todos los router, por lo que la subred asignada requerirá 3 direcciones ip's.
- En todas las redes finales, configure la primer ip como Gateway y la siguiente para el host correspondiente.

41. Configure las direcciones ip de cada uno de los host, tomando en cuenta que deberá asignarles además a una ip de Gateway. Por ej.: si a una PC debe asignarle direccionamiento de la subred 10.0.0.64 /27, su ip host podría ser la 10.0.0.69 y su gateway 10.0.0.65; el comando a ejecutar en su consola seria:

**ip 10.0.0.69/27 10.0.0.65**

Y no olvide guardar los cambios de configuración del host con el comando **save**.

42. Para ingresar a la CLI de router R1, siga estos pasos:

- a) De clic secundario sobre R1 e inicie su ejecución (opción Start).
- b) De nuevamente clic secundario y elija opción Console. Observe la secuencia real de inicio del IOS.
- c) Finalmente, se mostrara el cursor del modo privilegiado.
- d) Proceda configurar el nombre (hostname), banner de acceso y el direccionamiento ip de las diferentes interfaces.

43. Repita los últimos 2 anteriores para cada router y host restante de la topología, con las direcciones ip obtenidas del Subneteo realizado. secuencia del paso anterior para cada router restante de la topología.

44. Confirme con ping que existe comunicación entre pares de dispositivos bajo la misma subred.

45. Para alcanzar el estado de convergencia de la red, proceda a configurar el protocolo OSPF en los diferentes router de la topología.

No olvide configurar las interfaces pasivas.

46. Genere la tabla de enrutamiento de R3 y confirme que este alcanza a ver el resto de subredes no conectadas directamente en sus interfaces.

47. Realice pruebas de ping entre host y confirme la comunicación exitosa.

48. Guarde las configuraciones actuales de cada router hacia su archivo de configuración de inicio (startup-config), ejecutando al comando **copy running-config startup-config**.

49. Pare la ejecución de la simulación y guarde los cambios de su proyecto.

50. Guarde su proyecto actual y llame a su instructor, para evaluar la configuración realizada y el funcionamiento esperado de la simulación.

51. Suspenda la ejecución de su simulación y cierre el simulador.

## V. BIBLIOGRAFIA

- Documentation: The official GNS3 Documentation, (2023). [Getting Started with GNS3 | GNS3 Documentation](#)

|                                                                                   |                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p style="text-align: center;"><b>UNIVERSIDAD AUTONOMA DE<br/>CHIHUAHUA<br/>FACULTAD DE INGENIERÍA</b></p>                                                                                                                          |
| Enero junio 2023                                                                  | <p><b>GUIA DE LABORATORIO #11</b></p> <p><b>Nombre de la Practica:</b> Implementación de IPv6<br/> <b>Lugar de Ejecución:</b> Laboratorio de Redes<br/> <b>Tiempo Estimado:</b> 2 horas y 30 minutos<br/> <b>MATERIA:</b> Redes</p> |

## I. OBJETIVOS

Que el estudiante:

- Conozca y aplique los conceptos básicos de IPv6
- Implemente en los host a la configuración stateless y la configuración stateful
- Implemente el protocolo de enrutamiento RIPng.

## II. INTRODUCCION

Es importante tener en cuenta algunos conceptos importantes básicos de IPv6 antes de iniciar con la configuración de las simulaciones, cabe destacar alguno de ellos:

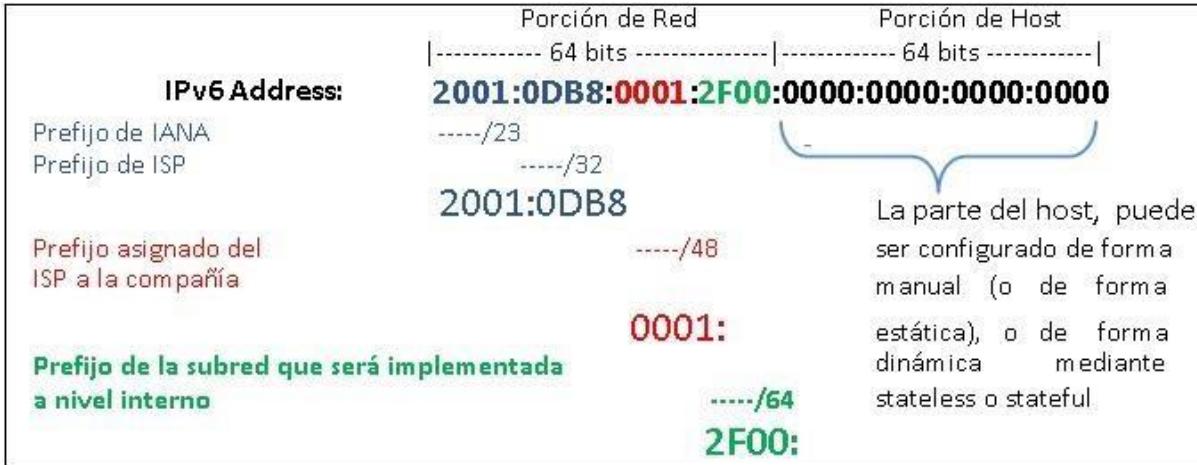
- Las direcciones IPv6 cuentan ahora con 128 bits para formar las direcciones.
- No existen máscaras de subred en las direcciones IPV6, la parte de la subred o porción de subred será básicamente un prefijo en la dirección IP del ordenador.
- No hay necesidad de reservar direcciones de red, ni broadcast como se hacía anteriormente en IPV4.
- No necesariamente se debe de disponer de un servidor DHCP para la obtención de parámetros de red.

En IPv6 los ordenadores pueden auto configurarse mediante stateless formando su propia IP con la porción de red del router y la dirección MAC de cada ordenador.



Ahora bien, se tienen que explicar algunos aspectos de la formulación de direcciones IPV6.

Para ello, a continuación se presenta un ejemplo:



Por lo que la porción que identifica la red sería abreviada de la siguiente forma: **2001:DB8:1:2F00/64**.

### Configuración stateless

Es un mecanismo de autoconfiguración que permite que direcciones unicast sean asignadas a los nodos sin necesidad de configuraciones manuales, sin servidores adicionales como el DHCP. Se requieren solo configuraciones mínimas en los router's.

### Configuración stateful

Es una técnica alternativa a stateless, donde es necesaria la utilización de servidores que informen a los hosts, los nodos a ser utilizados en la obtención de direcciones, además de otras configuraciones de red.

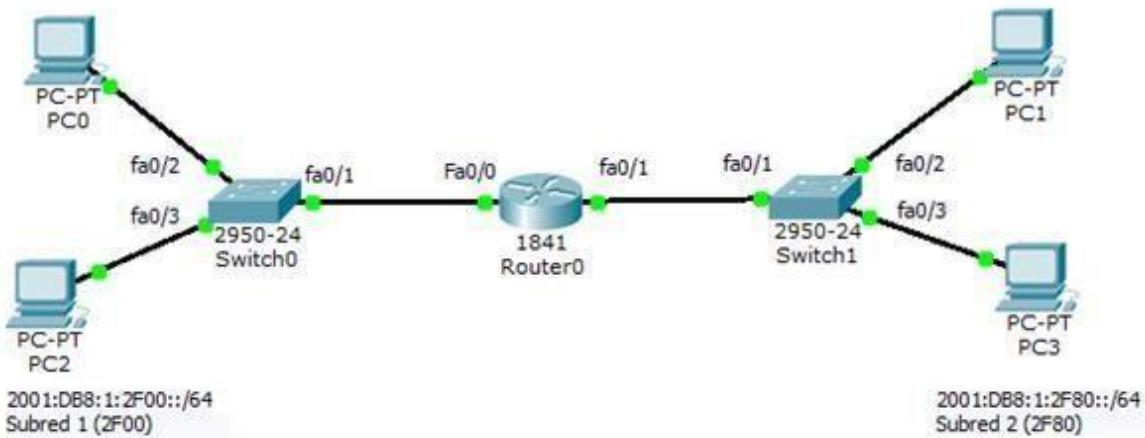
## III. MATERIALES Y EQUIPO

| Nº | REQUERIMIENTO                                                            | CANTIDAD |
|----|--------------------------------------------------------------------------|----------|
| 1  | Practica de laboratorio Nº 11 de REC404                                  | 1        |
| 2  | Estación de trabajo de PC con sistema operativo Linux Centos y Windows 7 | 1        |
| 3  | Simulador Packet Tracer instalado                                        | 1        |
|    |                                                                          |          |

## IV. PROCEDIMIENTO

### PARTE I – CONFIGURACIÓN STATELESS

1. Prepare una simulación en Cisco Packet Tracer. Luego arme la siguiente topología. Cuide de conectar las interfaces indicadas ahí.



- Proceda a configurar el router para la comunicación entre la Subred1 y la Subred2.

| Comandos de IOS                                                                                                                                                                   | Descripción                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>Router&gt;enable Router#configure terminal Router(config)#ipv6 unicast-routing</pre>                                                                                         | Con “ipv6 unicast-routing” se habilita el enruteamiento con ipv6 en el router                                                                  |
| <pre>Router(config)#int fa0/0 router(config-if)#ipv6 enable Router(config-if)#ipv6 address 2001:DB8:1:2F00::/64 eui-64 Router(config-if)#no shutdown Router(config-if)#exit</pre> | Configurar la int fa0/0 de tal forma que sólo se le dé el prefijo de red y automáticamente obtenga la dirección MAC de la interfaz respectiva. |
| <pre>Router(config)#int fa0/1 Router(config-if)#ipv6 enable Router(config-if)#ipv6 address 2001:DB8:1:2F80::/64 eui-64 Router(config-if)#no shutdown Router(config-if)#end</pre>  | Configurar la int fa0/1 de tal forma que sólo se le dé el prefijo de red y automáticamente obtenga la dirección MAC de la interfaz respectiva  |
| <pre>Router#copy run startup-config Router#reload</pre>                                                                                                                           | Guarda cambios en la configuración de inicio del router.<br>Reinicia el SO del Router.                                                         |

- Para verificar la auto-configuración puede auxiliarse del comando “show ipv6 interface brief” en modo privilegiado.

```

Router#show ipv6 interface brief
FastEthernet0/0 [up/up]
 FE80::2D0:FFFF:FE0E:6401
 2001:DB8:1:2F00:2D0:FFFF:FE0E:6401
FastEthernet0/1 [up/up]
 FE80::2D0:FFFF:FE0E:6402
 2001:DB8:1:2F80:2D0:FFFF:FE0E:6402
Vlan1 [administratively down/down]
Router#

```

4. En cada una de las PC's se deberá de activar el soporte para configuración stateless de la siguiente forma:

Dar clic sobre la pc -> Dirigirse a la pestaña Desktop  
 Elegir la opción command prompt    Digitar los comandos:

- ipv6config autoconfig (para activar la autoconfiguración)
- Ipv6config (para visualizar los parámetros de red obtenidos)

5. Con cada computadora que configure, asegúrese que tenga IPv6 de Gateway, pues de no ser así, no habrá conexión entre las computadoras de las diferentes LAN.

Si esto sucede deberá apagar administrativamente (**shutdown**) a la interfaz fastEternet del router por la cual recibe/envía paquetes a la computadora que no tiene Gateway. Luego active nuevamente esta interface.

6. Una vez realizados los pasos anteriores la conectividad a través de toda la red deberá de ser exitosa.

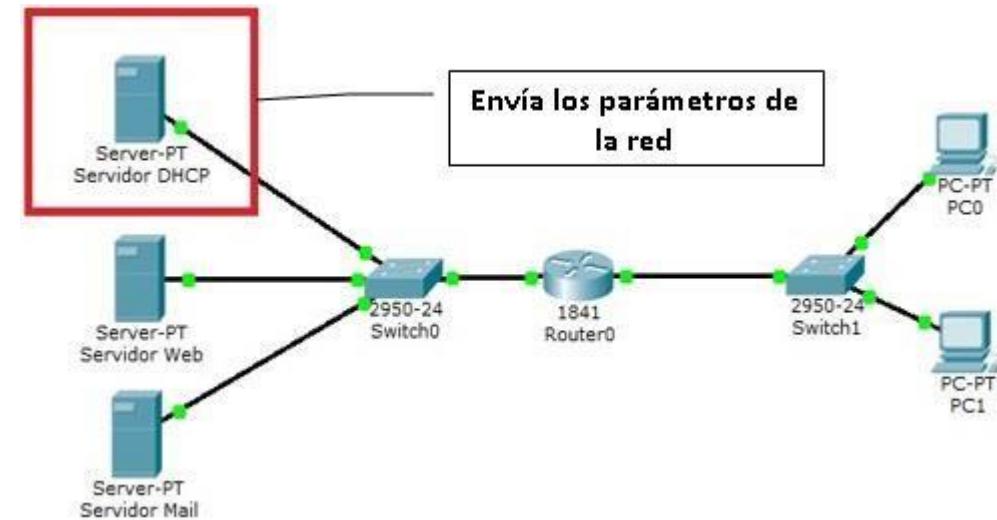
Proceda a enviar paquetes de tipo ICMPv6 en el modo de simulación para verificar que todo funcione de forma adecuada.

## PARTE II – CONFIGURACIÓN STATEFUL

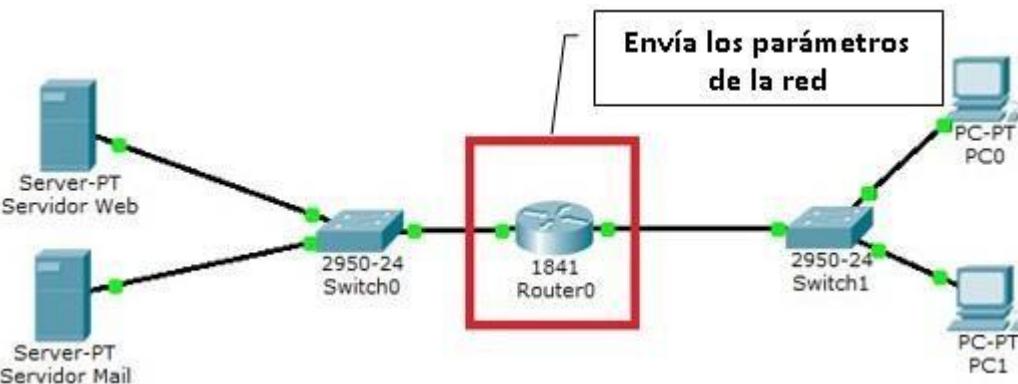
Se ha mencionado anteriormente que con este tipo de configuración los parámetros de red son obtenidos desde un servidor DHCP

En IPv6, este proceso se puede administrar incluso desde el mismo router, sin necesidad de invertir en una máquina extra que realice dichas funciones.

## IPv4

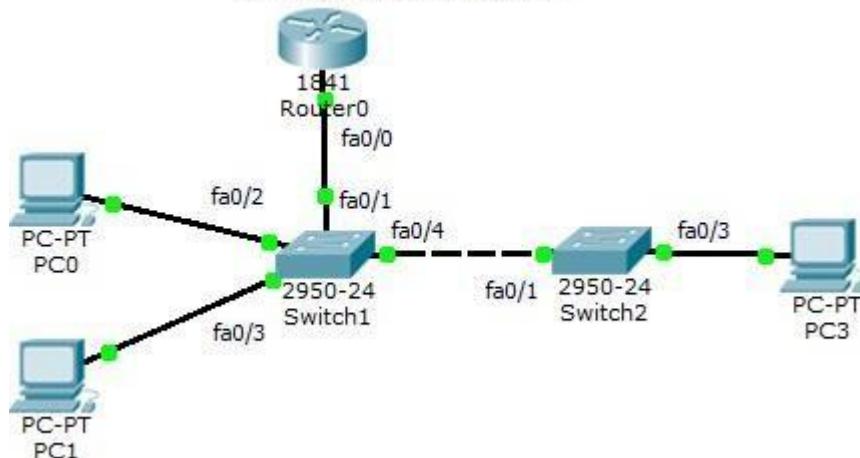


## IPv6



1. Prepare una nueva simulación, para luego, elaborar la siguiente topología de red

Subred1 2001:DB8:1:2:2f00::/64

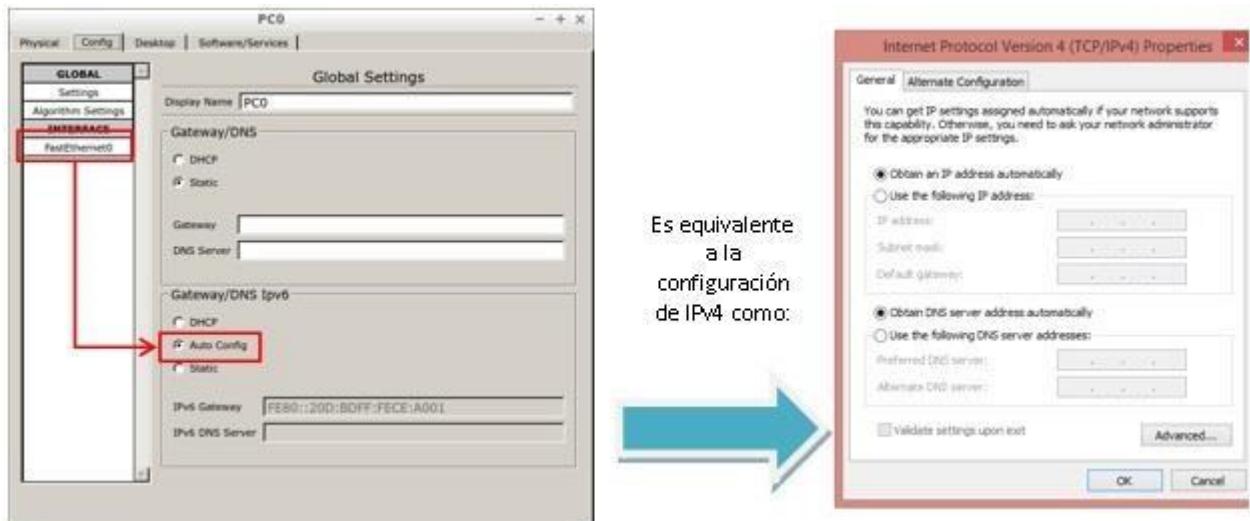


2. Proceda a configurar el Router como servidor DHCP para la red 2001:DB8:1:2:2F00::/64.

|                                                                                                                                                                                                                                                                               |                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router>enable Router#configure terminal<br>Router(config)#ipv6 dhcp pool PRUEBA<br>Router(config-dhcp)#prefix-delegation pool PRUEBA-prefijo Router(config-dhcp)#exit                                                                                                         | Crea el pool de direcciones llamado PRUEBA y se agrega un parámetro de prefijo para el servidor que se configurará a continuación.                                           |
| Router(config)#ipv6 unicast-routing<br><br>Router(config)#int fa0/0<br>Router(config-if)#ipv6 enable<br>Router(config-if)#ipv6 address 2001:DB8:1:2F00:201:97FF:FE28:c529/64<br>Router(config-if)#ipv6 dhcp server PRUEBA<br>Router(config-if)#no shut Router(config-if)#exit | Habilita el enrutamiento con ipv6 en el router<br><br>Configura la int fa0/0 con una ip de tipo estática y además se asigna un nombre al servidor DHCP, en este caso PRUEBA. |
| Router(config)#ipv6 local pool PRUEBA-prefijo 2001:DB8:1:2F00::/64 64<br>Router(config)#end                                                                                                                                                                                   | Establece que las direcciones a repartir vía DHCP serán de la red: 2001:DB8:1:2F00::/64 Y estarán en el rango 00-64.                                                         |

3. Proceda a dar clic en cualquier PC (este paso se repetirá para todas en la red), luego de clic en la pestaña Config.

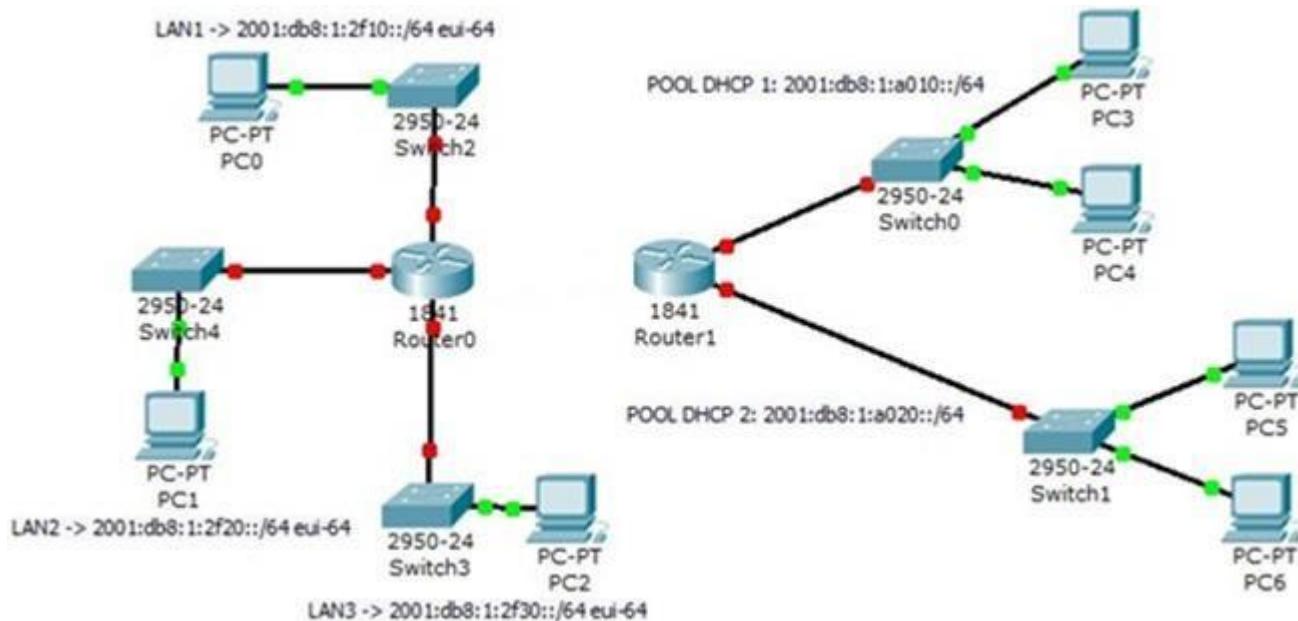
En el panel izquierdo localice la opción FastEthernet0/0 dando clic en ella, luego seleccione el parámetro DHCP tal como se muestra en la siguiente figura.



4. Cuando todos los indicadores se encuentren en color verde, proceda a hacer pruebas de conectividad entre las diferentes PC's.

## VI. INVESTIGACION COMPLEMENTARIA

Arme la siguiente topología, bajo direccionamiento IPv6.



Del lado izquierdo configure redes auto configurables y del lado derecho DHCP's.

|                                                                                                                                                                                                                                                                  |                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
|                                                                                                                                                                                 | <b>UNIVERSIDAD AUTONOMA DE<br/>CHIHUAHUA<br/>FACULTAD DE INGENIERÍA</b> |
| <p>Enero junio 2023</p> <p><b>GUIA DE LABORATORIO #12</b></p> <p><b>Nombre de la Practica:</b> Enrutamiento con IPv6</p> <p><b>Lugar de Ejecución:</b> Laboratorio de Redes</p> <p><b>Tiempo Estimado:</b> 2 horas y 30 minutos</p> <p><b>MATERIA:</b> Redes</p> |                                                                         |

## I. OBJETIVOS

Que el estudiante:

- Implemente simulaciones de topologías de red con el software de simulación GNS3.
- Configure rutas estáticas y rutas por defecto con direccionamiento ipv6.
- Identifique las similitudes y diferencias entre el protocolo de enrutamiento RIPng para IPv6 con el RIP original.
- Configure el protocolo RIPng en una topología de red.
- Identifique las similitudes y diferencias entre el protocolo de enrutamiento OSPFv3 para IPv6 y el OSPF.
- Configure el enrutamiento de una topología de red con OSPFv3.

## II. INTRODUCCION

### El enrutamiento bajo IPv6

Los protocolos de enrutamiento se han adaptado al esquema de direccionamiento de IPv6.

El concepto y funcionamiento básico de estos protocolos es el mismo que el de sus predecesores en IPv4, pero con algunas características que lo diferencian.



En esta guía se verá la configuración del enrutamiento estático (manual) y del enrutamiento dinámico generados por los protocolos RIPng y OSPFv3.

## Enrutamiento estático

Al igual como se desarrolla el enrutamiento bajo IPv4, la información de enrutamiento a utilizar en IPv6 puede ser ingresada de manera estático (manualmente) o en modo dinámico (utilizando un protocolo de enrutamiento).

### Configuración del enrutamiento estático

El procedimiento para crear una ruta estática en IPv6 utilizando Cisco IOS es el siguiente:

#### 1. Habilitar el enrutamiento IPv6.

Ya que el enrutamiento IPv6 no se encuentra habilitado por defecto en el IOS, es necesario habilitarlo explícitamente de la siguiente forma

```
Router#configure terminal
Router(config)#ipv6 unicast-routing
```

#### 2. Definir a cada una de las rutas estáticas.

La sintaxis del comando que crea rutas IPv6 es semejante a la que utiliza bajo redes con direccionamiento IPv4.

```
ipv6 route [prefijo] [próximo salto] [distancia administrativa] [ip próximo salto]
```

Bajo IPv6 no se indica una máscara de subred, sino la longitud del prefijo.

Observe un ejemplo:

```
ipv6 route 2001:db8:acad:2::/64 2001:db8:acad:4::2 s0/0/0 52
```

En donde:

- Dirección de red de destino: 2001:db8:acad:2::
- Longitud de prefijo: /64
- IP del siguiente salto: 2001:db8:acad:4::2
- Interfaz de salida: s0/0/0
- Distancia Administrativa: 1 (implícitamente) o mayor para crear una ruta de backup o flotante como en este ejemplo: 52 **Importante:**

Si se especifica una dirección link-local como IP del siguiente salto, el router solicitará que defina una interfaz de salida, ya que estas direcciones pueden ser la misma en diferentes interfaces al mismo tiempo. Por ejemplo:

```

R1(config)# ipv6 route 2001:db8:acad:2::/64 fe80::2
% Interface has to be specified for a link-local nexthop
R1(config)# ipv6 route 2001:db8:acad:2::/64 s0/0/0 fe80::2

```

## Ruta por defecto

Bajo IPv6, una ruta por defecto o del último recurso se hace bajo la misma lógica de su equivalente de IPv4.

```
ipv6 route ::/0 [próximo salto]
```

Observe un ejemplo:

```
ipv6 route ::/0 2001:db8:acad:4::2 s0/0/0 95
```

## Enrutamiento dinámico: RIPng (RIP next Generation)

Es el sucesor de RIPv2, es la versión más reciente del protocolo y está diseñado para el uso en redes IPv6.

El funcionamiento de RIPng es muy similar al de RIP para IPv4, por ejemplo:

Ambos envían periódicamente actualizaciones completas de rutas; ambos usan la regla de horizonte dividido, etc. La comparativa de RIPng y RIPv2 es la siguiente:

| Característica                             | RIPv2     | RIPng     |
|--------------------------------------------|-----------|-----------|
| Tipo de redes en las que publica rutas     | IPv4      | IPv6      |
| Protocolos de transporte para mensajes RIP | IPv4, UDP | IPv6, UDP |
| Puerto UDP                                 | 520       | 521       |
| Usa vector distancia                       | Si        | Si        |
| Distancia administrativa por defecto       | 120       | 120       |
| Soporta VLSM                               | Si        | Si        |
| Sumarización automática                    | Si        | N/A       |
| Usa Horizonte dividido                     | Si        | Si        |
| Usa envenenamiento de ruta                 | Si        | Si        |
| Actualizaciones cada 30segundos            | Si        | Si        |

| Usa triggered updates           | Si            | Si                                   |
|---------------------------------|---------------|--------------------------------------|
| Usa métrica de conteo de saltos | Si            | Si                                   |
| Característica                  | RIPv2         | RIPng                                |
| Métrica usada como infinita     | 16            | 16                                   |
| Soporta etiquetado de rutas     | Si            | Si                                   |
| Dirección Multicast             | 224.0.0.9     | FF02::9                              |
| Autenticación                   | Propia de RIP | Usa la propia de IPv6, que es AH/ESP |

Como se observa, hay pocos cambios con respecto de una versión a otra. La mayor diferencia se establece a la hora de configurarlo.

Los comandos básicos requeridos para configurar RIPng son los siguientes:

| Comando de RIPng                         | Función                                                                                                                                                                                                                                                 |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6 router rip [nombre de la instancia] | En modo global, activa el protocolo RIPng<br>La instancia es un identificador para el protocolo.<br>Permite implementar redistribución de la ruta por defecto y de rutas con otros protocolos de routing.                                               |
| ipv6 rip [nombre de la instancia] enable | Dentro de una interface específica:<br>Publica las redes y activa el envío de paquetes del protocolo por esta interfaz.<br>El nombre de la instancia sólo tiene importancia local.<br>Debe usar la misma instancia para publicar las redes en el router |

- En RIPng ya no es necesario el comando network para publicar las redes.

### Enrutamiento dinámico: OSPFv3

Al igual que los protocolos vistos hasta ahora (RIP y EIGRP), OSPFv3 es la última versión disponible de OSPF y diseñada para su uso en redes IPv6.

La comparación (similitudes y diferencias) de OSPFv3 y su predecesor se resumen a continuación:

| Característica | OSPFv2 | OSPFv3 |
|----------------|--------|--------|
|----------------|--------|--------|

| Tipo de redes en las que publica rutas                | IPv4           | IPv6                                 |
|-------------------------------------------------------|----------------|--------------------------------------|
| Protocolo de capa 3 para mensajes OSPF                | IPv4           | IPv6                                 |
| Protocolo de capa 3 para tipo de cabecera             | 89             | 89                                   |
| Usa Link State                                        | Si             | Si                                   |
| Característica                                        | OSPFv2         | OSPFv3                               |
| Soporta VLSM                                          | Si             | Si                                   |
| Proceso para selección de RID comparado con OSPFv2    | Igual          | Igual                                |
| Inundación de LSAs comparado con OSPFv2               | Igual          | Igual                                |
| Estructura de áreas comparado con OSPFv2              | Igual          | Igual                                |
| LSID de 32 bits                                       | Si             | Si                                   |
| Métrica obtenida del ancho de banda de la interfaz    | Si             | Si                                   |
| Métrica usada como infinita                           | $2^{16}-1$     | $2^{16}-1$                           |
| Soporta etiquetado de rutas                           | Si             | Si                                   |
| Elección de DR basada en mayor prioridad              | Si             | Si                                   |
| Publicación periódica cada                            | 30min          | 30min                                |
| Dirección multicast para todos los routers OSPF       | 224.0.0.5      | FF02::5                              |
| Dirección multicast para todos los routers designados | 224.0.0.6      | FF02::6                              |
| Autenticación                                         | Propia de OSPF | Usa la propia de IPv6, que es AH/ESP |
| Múltiples instancias por interface                    | No             | Si                                   |

**Pasos para la configuración básica de OSPFv3** Desde

el modo de configuración global:

1.- Habilitar el router para tráfico IPv6 con el comando `ipv6 unicast-routing`.

2.- Habilitar el proceso OSPFv3 usando el comando:

```
 ipv6 router ospf [id de proceso]
```

3.- Luego, dentro del modo de configuración de EIGRP, configurar el router-ID con el cual OSPFv3 se identificara ante el resto de vecinos del SA.

El comando a utilizar es:

```
 router id [RID]
```

Donde RID hace referencia a una IP en formato IPv4. Si no configura este comando, el router tomará como router id la IPv4 más alta configurada en cualquier interfaz.

Si no tiene una IPv4 configurada en alguna interfaz, deberá configurar este comando.

Luego, desde el modo de configuración de una interface:

4.- Habilitar las interfaces con IPv6 con el comando:

```
 ipv6 address [opciones]
```

Entre las diferentes opciones, la más utilizada es:`ipv6 address [prefijo / longitud] eui64`.

5.- Habilitar OSPF en las interfaces donde queramos publicar rutas con el comando:

```
 ipv6 ospf [id de proceso] area [núm. de área]
```

### **Visualización de la tabla de enrutamiento**

Las rutas bajo IPv6 se almacenan en una tabla separada de las rutas bajo IPv4.

El contenido de esta tabla de rutas IPv6 se visualiza con el comando:

```
 show ipv6 route
```

### **III. MATERIALES Y EQUIPO**

| Nº | REQUERIMIENTO                                                             | CANTIDAD |
|----|---------------------------------------------------------------------------|----------|
| 1  | Guía de Práctica #12 de REC404                                            | 1        |
| 2  | Estación de trabajo de PC con sistema operativo Linux Centos y Windows 7. | 1        |
| 3  | Software de Simulación de redes Packet Tracert                            | 1        |

#### IV. PROCEDIMIENTO

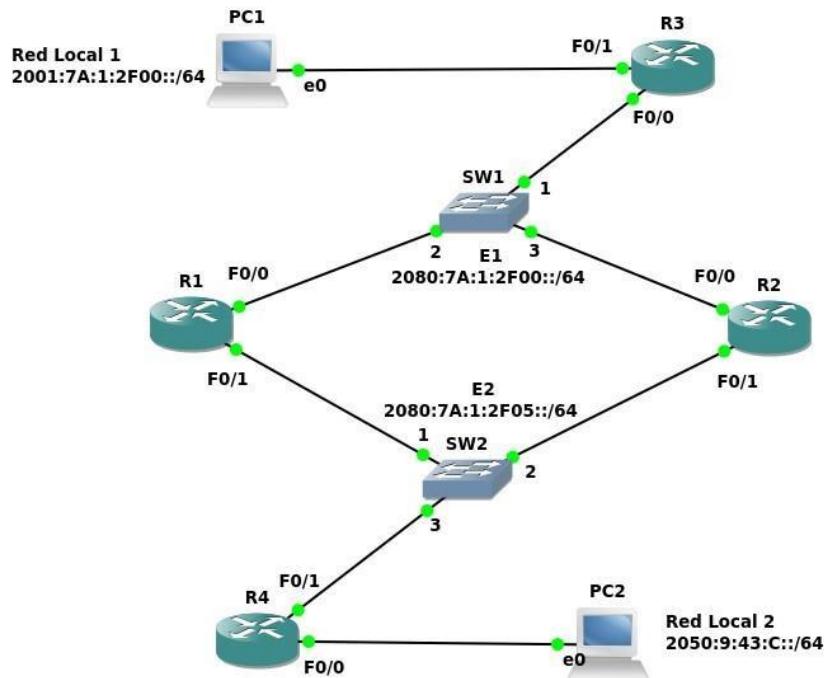
##### Parte 1: Configuración de enrutamiento estáticas

1. Inicie el software de simulación GNS3.

En la ventana inicial (*Nuevo proyecto...*), presione el botón **Browse**, y luego diríjase hasta la carpeta *Escritorio. Una vez ahí, en el recuadro **nombre***, definirá el nombre de su carpeta en la que se guardará su proyecto. Asigne el nombre **Practica12\_SuCarnet** y luego clic en botón **OK**.

Después, al retornar a la ventana anterior, asigne el nombre **Practica12\_parte1** - en le recuadro **name** - a su primer proyecto y de clic en botón **Ok**.

**Imagen 12.1:** Topología de red a implementar y configurada bajo IPv6



2. A continuación, elaboraremos la simulación mostrada en la imagen 12.1. Tome en cuenta los siguientes aspectos al implementar esta topología:
  - Se proporcionan los ID redes
  - La red E1 permite conectar a los router R1, R2 y R3 en una red en comun. • Igual sucede con la red E2, que enlaza a R1, R2 y R4

3. Para iniciar su diseño, cada router será de la serie c3725. Ubique en la barra de herramientas izquierda al botón “**Browse Routers**”, seleccione el modelo c3725 y arrástrelo al área de trabajo. Repita esta acción hasta colocar los dispositivos requeridos
4. De la barra de herramientas, de clic en el botón “**Browse Switches**” y arrastre los modelos “Ethernet switch” requeridos en la topología. De igual forma, agregue a las PC, de clic en el botón “**Browse End Devices**” y arrastre 2 modelos “VPCS”.
5. Haga las conexiones/enlaces entre los dispositivos descritas en la topología.
6. Utilice el botón “**Add a note**” para realizar la documentación interna de la topología.
7. Haga clic secundario sobre R1 y seleccione la opción **Start**, para que inicie el IOS de este router.
8. Nuevamente de clic secundario sobre R1 y elija opción Console, para ingresar a la CLI. Espere un poco hasta que se muestre el cursor del modo privilegiado (si después de un minuto no se muestra el **prompt** presione **enter**).
9. Proceda a ejecutar las configuraciones para **R1** indicadas en la imagen 12.2.

Con el resultado del último comando, confirme el ingreso correcto de la ipv6 en cada interfaz del R1.

10. Una vez terminada la configuración del router R1, continúe con la configuración los router's **R2**, **R3** y **R4**, tomando en cuenta a las configuraciones de **R3** y **R4** descritas en la imagen 12.3.
11. Retorne la CLI de **R2**, y compruebe que hay comunicación de **R2** hacia **R1**, **R3** y **R4**, por las redes E1 y E2, ejecutando los comandos **ping - desde R2** - dirigido a la ip de la **F0/0 y F0/1 de R1; F0/0 de R3 y F0/1 de R4**, así: **ping 2080:7A:1:2F00::1 → de R2 a la F0/0 de R1 ping 2080:7A:1:2F05::1 → de R2 a la F0/1 de R1 ping 2080:7A:1:2F00::3 → de R2 a la F0/0 de R3 ping 2080:7A:1:2F05::3 → de R2 a la F0/1 de R4**
12. Abra la CLI de **R1**, y compruebe que hay comunicación de **R1** hacia **R3 y R4**, por las redes E1 y E2 respectivamente, ejecutando los comandos **ping - desde R1** - dirigido a la ip de la **F0/0 de R3 y F0/1 de R4**: **ping 2080:7A:1:2F00::3 → de R2 a la F0/0 de R3 ping 2080:7A:1:2F05::3 → de R2 a la F0/1 de R4**

**Imagen 12.2: Configuración de direccionamiento IPv6 en router R1 y R2**

|           |           |
|-----------|-----------|
| <b>R1</b> | <b>R2</b> |
|-----------|-----------|

| R1#conf t<br>R1(config)#ipv6 unicast-routing<br>R1(config)#inter f0/0<br>R1(config-if)#ipv6 enable<br>R1(config-if)#ipv6 address 2080:7A:1:2F00::1/64<br>R1(config-if)#no shutdown<br>R1(config-if)#exit<br>R1(config)#inter f0/1 | R2#conf t<br>R2(config)#ipv6 unicast-routing<br>R2(config)#interface fa 0/0<br>R2(config-if)#ipv6 enable<br>R2(config-if)#ipv6 address 2080:7A:1:2F00::2/64<br>R2(config-if)#no shutdown<br>R2(config-if)#exit<br>R2(config)#interface fa 0/1 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R1                                                                                                                                                                                                                                | R2                                                                                                                                                                                                                                            |
| R1(config-if)#ipv6 enable<br>R1(config-if)#ipv6 address 2080:7A:1:2F05::1/64<br>R1(config-if)#no shutdown<br>R1(config-if)#end<br>R1#do copy run start<br>R1#show ipv6 interface brief                                            | R2(config-if)#ipv6 enable<br>R2(config-if)#ipv6 address 2080:7A:1:2F05::2/64<br>R2(config-if)#no shutdown<br>R2(config-if)#end<br>R2#do copy run start<br>R2#show ipv6 interface brief                                                        |

**Imagen 12.3: Configuración de direccionamiento IPv6 de router R3 y R4**

| R3 | R4 |
|----|----|
|    |    |

|                                                          |                                                    |
|----------------------------------------------------------|----------------------------------------------------|
| R3#conf t                                                | R4#conf t                                          |
| R3(config)#ipv6 unicast-routing                          | R4(config)#ipv6 unicast-routing                    |
| R3(config)#interface f0/0                                | R4(config)#interface f0/0                          |
| R3(config-if)#ipv6 enable                                | R4(config-if)#ipv6 enable                          |
| R3(config-if)#ipv6 address 2080:7A:1:2F00::3/64          | R4(config-if)#ipv6 address 2050:9:43:C::/64 eui-64 |
| R3(config-if)#no shutdown                                | R4(config-if)#no shutdown                          |
| R3(config-if)#exit                                       | R4(config-if)#exit                                 |
| R3(config)#interface f0/1                                | R4(config)#interface f0/1 R4(config-if)#ipv6       |
| R3(config-if)#ipv6 enable                                | enable                                             |
| R3(config-if)#ipv6 address<br>2001:7A:1:2F00::/64 eui-64 | R4(config-if)#ipv6 address 2080:7A:1:2F05::3/64    |
| R3(config-if)#no shutdown                                | R4(config-if)#no shutdown                          |
| R3(config-if)#end                                        | R4(config-if)#end                                  |
| R3#copy run start                                        | R4#copy run start                                  |
| R3#show ipv6 interface brief                             | R4#show ipv6 interface brief                       |

13. Proceda a configurar a PC1. Para ello, de clic secundario sobre ella, seleccione **Start** y espere unos 10 seg.

Luego, nuevamente de clic secundario sobre PC1 y elija opción Console. Presione Enter para acceder al cursor.

14. Ejecute el comando **show ipv6**. Determine si ya genero el direccionamiento IPv6 por medio de direcciones ip stateless. Si aún no la posee, ejecute el comando **ip auto**.

15. Realice ping desde la **PC1 hacia la F0/1 de R3**, mediante el comando **ping**. Recuerde que la IPv6 de esa interfaz se le pedía que la anotara en el paso N° 11 de la presente guía.

16. Realice los pasos **15 y 16** en la **PC2**.

17. Realice ping desde la **PC2 hacia la F0/0 de R4**, mediante el comando **ping**. Recuerde que la IPv6 de esa interfaz se le pedía que la anotara en el paso N° 11 de la presente guía.

18. Procederá a configurar el enrutamiento estático (2 rutas) en R1 para que alcance a las 2 redes locales, utilizando rutas por “ip del próximo salto”

19. Para determinar las ip del próximo salto, identifique las ipv6 que tienen definidas las interfaces de R3 y R4 que alcanzan a R1, ejecutando en cada dispositivo al comando:

### show ipv6 interface brief

20. Compare su resultado con el listado en la tabla de la Imagen 12.4. **Imagen 12.4 Direccionamiento**

#### IPv6 de interfaces de R3 y R4

| R3#show ipv6 interface brief     | R4#show ipv6 interface brief |
|----------------------------------|------------------------------|
| FastEthernet0/0 [up/up]          | FastEthernet0/0 [up/up]      |
| FE80::C803:32FF:FE60:0           | FE80::C804:33FF:FEAC:0       |
| 2080:7A:1:2F00::3                | 2050:9:43:C:C804:33FF:FEAC:0 |
| FastEthernet1/0 [up/up]          | FastEthernet1/0 [up/up]      |
| FE80::C803:32FF:FE60:1C          | FE80::C804:33FF:FEAC:1C      |
| 2001:7A:1:2F00:C803:32FF:FE60:1C | 2080:7A:1:2F05::3            |
| R3#                              | R4#                          |

Cada ipv6 resaltada será la ip del próximo salto en las rutas estáticas que definirá en R1.

21. Ingrese al modo global de **R1** y cree las siguientes rutas estáticas. Observe el uso de las ip resaltadas.

```
R1(config)#ipv6 route 2001:7A:1:2f00::/64 fa0/0 2080:7A:1:2F00::3
R1(config)#ipv6 route 2050:9:43:C::/64 fa0/1 2080:7A:1:2F05::3
```

22. Ingrese al modo global de **R2** y cree las siguientes rutas estáticas. Observe el uso de las ip resaltadas.

```
R2(config)#ipv6 route 2001:7A:1:2f00::/64 fa0/0 2080:7A:1:2F00::3
R2(config)#ipv6 route 2050:9:43:C::/64 fa0/1 2080:7A:1:2F05::3
```

23. Ahora realizaremos la configuración de rutas estáticas en **R3** y **R4** que le permitan alcanzar la Red Local 2, tanto por R1 como por R2.

|                                                                               |                                                                                |
|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| R1#show ipv6 interface brief                                                  | R2#show ipv6 interface brief                                                   |
| FastEthernet0/0 [up/up]<br>FE80::C803:32FF:FE60:0<br><b>2080:7A:1:2F00::1</b> | FastEthernet0/0 [up/up]<br>FE80::C804:33FF:FEAC:0<br><b>2080:7A:1:2F00::2</b>  |
| FastEtherne0/1 [up/up]<br>FE80::C803:32FF:FE60:1C<br><b>2080:7A:1:2F05::1</b> | FastEthernet0/1 [up/up]<br>FE80::C804:33FF:FEAC:1C<br><b>2080:7A:1:2F05::2</b> |
| R1#                                                                           | R2#                                                                            |

24. Ingrese al modo global de **R3** y cree las siguientes rutas estáticas. Observe el uso de las ip resaltadas.

```
R3(config)#ipv6 route 2050:9:43:C::/64 fa0/0 2080:7A:1:2F00::1
```

```
R3(config)#ipv6 route 2050:9:43:C::/64 fa0/0 2080:7A:1:2F00::2
```

25. Ingrese al modo global de **R3** y cree las siguientes rutas estáticas. Observe el uso de las ip resaltadas.

```
R4(config)#ipv6 route 2001:7A:1:2f00::/64 fa0/1 2080:7A:1:2F05::1
```

```
R4(config)#ipv6 route 2001:7A:1:2f00::/64 fa0/1 2080:7A:1:2F05::2
```

26. Finalmente proceda a realizar pruebas de comunicación, ingresando al command prompt de la PC bajo la subred “2001:db8:1:2f00” y hacer ping a la IP de la pc bajo la subred “2001:db8:1:af80” y viceversa.

27. Guarde los cambios realizados en la simulación hasta ahora.

## Parte 2: Configuración de enrutamiento dinámico con RIPng

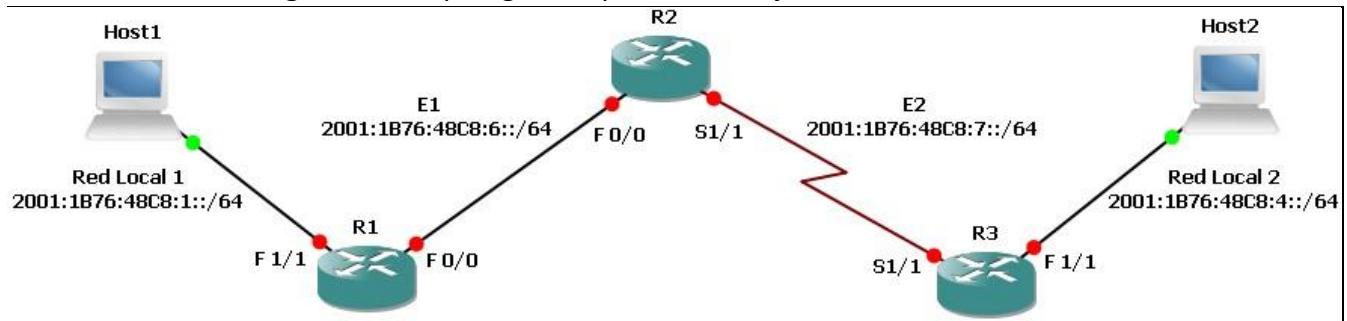
28. Prepare un nuevo proyecto de GNS3 y guarde el archivo con el nombre **Practica12\_parte2**.

29. Elabore la topología base descrita en la Imagen 12.5. Para ello se modificara a R2 y R3, para asignar en su Slot 1 al módulo NM-4T siguiendo los pasos descritos a continuación:

- Clic derecho sobre R2 y elija la opción **configure**
- En la nueva ventana, en el panel izquierdo, elija R2.

- c. En el panel derecho le aparecerán varias opciones de pestañas, de clic en la pestaña **Slot**.
- d. Ahora despliegue la lista de **slot 1**, y elija la interfaz **NM-4T**.
- e. Repita los pasos anteriores, pero sobre **R3**.

**Imagen 12.5:** Topología a implementar bajo enrutamiento dinámico



30. Inicie la simulación, presionando el botón Start/Resume all devices.
31. Espere unos 30 seg. Luego, de clic secundario sobre R1 y seleccione opción Console.
32. Para continuar, proceda con la configuración de R1, ejecutando la siguiente secuencia de comandos:

| Comando a ejecutar                                                                                                                                                                                                                                                                                                                                                                       | Descripción                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| <pre>R1#conf t R1(config)#ipv6 unicast-routing R1(config)#interface f0/1 R1(config-if)#ipv6 enable R1(config-if)#ipv6 address 2001:1B76:48C8:1::/64 eui-64 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#interface f0/0 R1(config-if)#ipv6 enable R1(config-if)#ipv6 address 2001:1B76:48C8:6::1/64 anycast R1(config-if)#no shutdown R1(config-if)#end R1#copy run star</pre> | Se configura la interfaz f 0/1 como en la simulación No.1 para que trabaje con stateless |

33. Ahora desarrolle la siguiente configuración para el Router R2.

| Comando a ejecutar                                                                                                                                                                                                                                                                                                                                                                                                                             | Descripción                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| R2#conf t<br>R2(config)#ipv6 unicast-routing<br>R2(config)#interface fa 0/0<br>R2(config-if)#ipv6 enable<br>R2(config-if)#ipv6 address 2001:1B76:48C8:6::2/64<br>R2(config-if)#no shutdown<br>R2(config-if)#do ping 2001:1B76:48C8:6::1<br>R2(config-if)#exit<br>R2(config)#inter serial 1/1<br>R2(config-if)#ipv6 enable<br>R2(config-if)#ipv6 address 2001:1B76:48C8:7::1/64<br>R2(config-if)#no shutdown<br>R2(config-if)#do copy run start | Se configura la interfaz fa0/0 como stateless<br><br>Se guardan las configuraciones en el router y se reinicia. |

34. Ejecute la configuración de las interfaces de R3 y haga pruebas para confirmar que este router alcanza a ver a R2.

Guarde los cambios en el archivo de configuración de inicio (startup-config) de cada router.

35. Sobre los host PC1 y PC2, ejecute el proceso de autoconfiguración de direcciones IPv6.

36. Guarde los cambios en su proyecto de simulación (clic en botón ‘Save project..’) y presione el botón “Stop all devices”.

37. Del menú principal de GNS3, seleccione la opción File-> Save Project as..

Como ubicación, seleccione su carpeta (**Practica12\_SuCarnet**) y luego, como nombre del proyecto asigne: **Practica12\_parte2\_RIPng**

38. Inicie todos los dispositivos, dando clic en botón ‘Start/Resume all devices’ y espere unos 20 seg.

39. Ingrese a la CLI de R1 y visualice la configuración general, ejecutando al comando **show runningconfig**. Confirme que las interfaces tienen el direccionamiento ipv6 correcto.

40. Luego ejecute la siguiente configuración, para levantar el protocolo RIPng en R1 y publicar sus redes.

41. Ingrese a la CLI de R2, confirme que las interfaces están configuradas correctamente y luego ejecute la configuración, que activara RIPng y compartirá sus rutas con R1.

| Comando a ejecutar                                                                                                                                                                                                          | Descripción                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| R1#conf t<br>R1(config)#interface f0/1<br>R1(config-if)#ipv6 rip UDB enable<br>R1(config-if)#exit<br>R1(config)#interface fa 0/0<br>R1(config-if)#ipv6 rip UDB enable<br>R1(config-if)#exit<br>R1(config)#do copy run start | Ingresa a cada interface (fa1/1 y f0/0), para activar la versión de RIP para IPv6 (RIPng)  |
| R2#conf t<br>R2(config)#interface f 0/0<br>R2(config-if)#ipv6 rip UDB enable<br>R2(config-if)#exit<br>R2(config)#inter s1/1<br>R2(config-if)#ipv6 rip UDB enable<br>R2(config-if)#end<br>R2#copy run startup-config         | Ingresa a cada interface (f 0/0 y s 1/1), para activar la versión de RIP para IPv6 (RIPng) |

42. Ejecute al comando “**show ipv6 routes**”. Confirme que R2 ya puede alcanzar la red local 1, ubicando las rutas con letra (R) recibidas de R1 bajo RIPng.

43. Finalmente, ingrese a la CLI de R3, configure RIPng en sus interface y guarde los cambios en la configuración de inicio.

Confirme que este router ya puede alcanzar el resto de redes. Ingrese a la PC2 y envíe ping a la ipv6 de PC1. La comunicación será exitosa.

44. Guarde los cambios en el proyecto actual.

### Parte 3: Configuración de OSPFv3

45. Cargue nuevamente el archivo de proyecto (**Practica12\_parte2**). Para ello, de clic en opción del menú *File -> Open Project*. Ubique y abra el archivo de este proyecto.
46. Haga una copia de este proyecto bajo el nombre **Practica12\_parte3\_ospfv3**. Luego inicie a todos los dispositivos de la topología.
47. Ingrese a la CLI de R1 y confirme que sus interfaces tienen el direccionamiento ipv6 correcto.
48. Ahora ejecute la siguiente configuración para activar al protocolo OSPFv3.

| Comando a ejecutar                                                                                                                                                                                                                                 | Descripción                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R1#conf t<br>R1(config)#ipv6 router ospf 1<br>R1(config-rtr)#<br><i>*Apr 23 20:42:05.163: %OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id, please configure manually</i><br>R1(config-rtr)#router-id 1.1.1.1<br>R1(config-rtr)#exit | En el modo global del router3, se configura el soporte para IPv6.<br>Se crea el proceso de OSPF con el ID 1.<br>Define el identificador del router 1.1.1.1. |
| R1(config)#interface f1/1<br>R1(config-if)#ipv6 ospf 1 area 0<br>R1(config-if)#exit<br>R1(config)#interface f0/0<br>R1(config-if)#ipv6 ospf 1 area 0<br>R1(config-if)#end<br>R1#copy running-config startup-config                                 | Se configura la interfaz fa0/1 como stateless y se activa OSPFv3                                                                                            |

49. Ingrese a la CLI de R2. Luego, ejecute la siguiente configuración para activar OSPFv3.

| Comando a ejecutar | Descripción |
|--------------------|-------------|
|--------------------|-------------|

|                                                                                                                                                                                                                                                              |                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| R2#conf t<br>R2(config)#ipv6 router ospf 1                                                                                                                                                                                                                   | Se configura en el router a nivel global el soporte para IPv6.                                             |
| R2(config-rtr)#router-id 2.2.2.2<br>R2(config-rtr)#exit<br>R2(config)#inter s 1/1<br>R2(config-if)#ipv6 ospf 1 area 0<br>R2(config-if)#exit<br>R2(config)#inter f 0/0<br>R2(config-if)#ipv6 ospf 1 area 0<br>R2(config-if)#end<br>R2#copy run startup-config | Además se crea el proceso de OSPF con el ID 1.<br>Finalmente se añade el identificador del router 2.2.2.2. |

50. Genere la tabla de enrutamiento de R2 y confirme que alcanza a ver a la red local 1 (marcada con letra O), gracias al enrutamiento OSPFv3 con R1.

51. Ingrese a la CLI de R3 y ejecute la configuración requerida para activar OSPFv3.

Luego, genere su tabla de enrutamiento y confirme que ya se puede ver el resto de redes no conectadas directamente a él.

52. Ingrese al cursor de PC1 y envíe un ping a la ipv6 de PC2. La prueba deberá ser exitosa

53. Guarde la configuración actual de R3 y luego guarde los cambios de la simulación general.

54. Llame a su instructor para demostrar el enrutamiento OSPFv3 de esta última simulación. 55.

Cierre la simulación y cierre a GNS3

## V. ANALISIS DE RESULTADOS

1. **(45%)** En el salón de clases, al finalizar la practica:

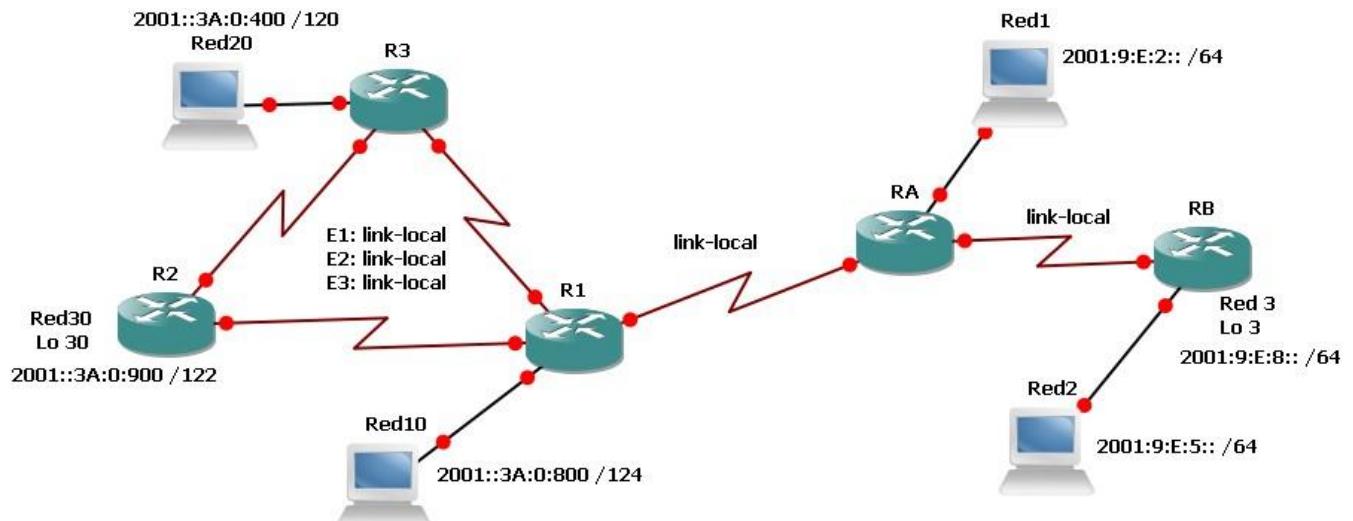
Evaluación del funcionamiento de cada ejemplo desarrollado en el procedimiento.

2. (55%) Implemente la simulación presentada en la figura 4, haciendo uso de los protocolos de enrutamiento bajo IPv6 vistos hasta ahora.

En la solución deben cumplirse los parámetros listados a continuación:

- El direccionamiento de cada red de enlace entre router se hará estáticamente.
- Las redes Red3 y Red10 se implementan con loopback y su direccionamiento ipv6 se hará estáticamente.
- El direccionamiento de las redes Red10 y Red20 se hará con direcciones statefull configurado en sus router de conexión.
- El direccionamiento de host de las redes locales Red1 y Red2, que usaran direcciones Stateless.
- El enrutamiento del Sistema autónomo (R1, R2 y R3) se administra con OSPFv3
- El enrutamiento del Sistema autónomo (RA, RB) se administra bajo RIPng
- Para que el SA bajo RIPng alcance a las redes del otro SA, debe crearse en R1 a una ruta por defecto y ser transferida a R2 y R3.
- El SA bajo OSPFv3 debe alcanzar a las redes del otro SA, creando en RA a solamente una ruta estática de las redes bajo OSPFv3 y luego publicarla al resto de su SA.

**Imagen 12.6:** Topología bajo enrutamiento RIPng y OSPFv3





# UNIVERSIDAD AUTONOMA DE CHIHUAHUA FACULTAD DE INGENIERÍA

Enero junio  
2023

**Guía de Laboratorio #13**  
**Nombre de la Práctica:** Túneles  
**Lugar de Ejecución:** Laboratorio de Redes  
**Tiempo Estimado:** 2 horas y 30 minutos  
**MATERIA:** Redes

## I. OBJETIVOS

Que el estudiante:

- Liste a cada una de las diferentes técnicas de transición de IPv4 a IPv6
- Defina el funcionamiento de la técnica de Túneles para la transición IPv4-IPv6
- Configure un túnel manual, para comunicar islas IPv6 sobre una topología bajo IPv4

## II. INTRODUCCION

### Tunelización IPv6

La segunda técnica de transición (IPv4 a IPv6) más importante es el **tunneling**.

Tunelizar paquetes es un mecanismo por medio del cual un paquete es encapsulado y llevado como carga útil dentro de un paquete IPv6. El paquete resultante es llamado “paquete tunelizado IPv6”.

El camino entre la fuente y el destino del “paquete tunelizado” es llamado “túnel IPv6”. La técnica es llamada **“tunelización IPv6” (IPv6 tunneling)**.

La tunelización IPv6 es una técnica que establece un “enlace virtual” entre dos nodos IPv6 para transmitir paquetes de datos como carga útil de paquetes IPv6. Desde el punto de vista de dos nodos este “enlace virtual” llamado “túnel IPv6”, aparece como un enlace punto a punto sobre el cual IPv6 actúa como un protocolo de capa de enlace.

Los dos nodos IPv6 juegan roles específicos. Un nodo encapsula los paquetes originales recibidos desde otros nodos o desde él mismo y envía los “paquetes tunelizados” resultantes a través del túnel.

El otro nodo desencapsula el “paquete tunelizado” recibido y envía los paquetes originales resultantes hacia su destino, posiblemente a él mismo. El nodo encapsulador es llamado nodo punto de entrada al túnel y es la fuente de los paquetes tunelizados. El nodo desencapsulador es llamado nodo punto de salida al túnel y es el destino de los paquetes tunelizados.

Un túnel IPv6 es un mecanismo unidireccional. El flujo de paquetes de túnel toma lugar en una dirección entre el nodo punto de entrada del túnel y el nodo punto de salida del túnel.

Un túnel bi- direccional se puede obtener fusionando dos mecanismos unidireccionales, es decir, configurando dos túneles, cada uno en dirección opuesta al otro, el nodo punto de entrada de un túnel es el nodo punto de salida del otro túnel.

## **Tipos de tunneling**

Existen varias técnicas de tunneling, entre ellas:

- **Tunneling manual de IPv6 sobre IPv4:** un paquete de IPv6 se encapsula dentro del protocolo IPv4. Este método requiere routers de stack doble.
- **Tunneling dinámico 6to4:** establece automáticamente la conexión de islas de IPv6 a través de la red IPv4, normalmente Internet.

Aplica dinámicamente un prefijo IPv6 válido y único a cada isla de IPv6, lo que posibilita la implementación rápida de IPv6 en una red corporativa sin recuperación de direcciones de los ISP o los registros.

Otras técnicas de tunneling menos utilizadas incluyen:

- **Tunneling del protocolo de direccionamiento automático de túnel dentro de un sitio (ISATAP, Intra-Site Automatic Tunnel Addressing Protocol):**

Mecanismo de tunneling de capa superior automática que utiliza la red IPv4 subyacente como capa de enlace para IPv6.

Los túneles del ISATAP permiten que los hosts de stack doble individuales IPv4 o IPv6 de un sitio se comuniquen con otros hosts similares a través de un enlace virtual y creen así una red IPv6 mediante la infraestructura IPv4.

- **Tunneling Teredo:**

Tecnología de transición a IPv6 que proporciona tunneling automático de host a host en lugar de tunneling de gateway. Este enfoque transmite tráfico IPv6 unicast si hay hosts de stack doble (hosts que ejecutan tanto IPv6 como IPv4) detrás de una o varias NAT IPv4.

El tunneling es una técnica de integración y transición intermedia, y no debe considerarse como una solución definitiva. El objetivo final debe ser una arquitectura IPv6 nativa

### III. MATERIALES Y EQUIPO

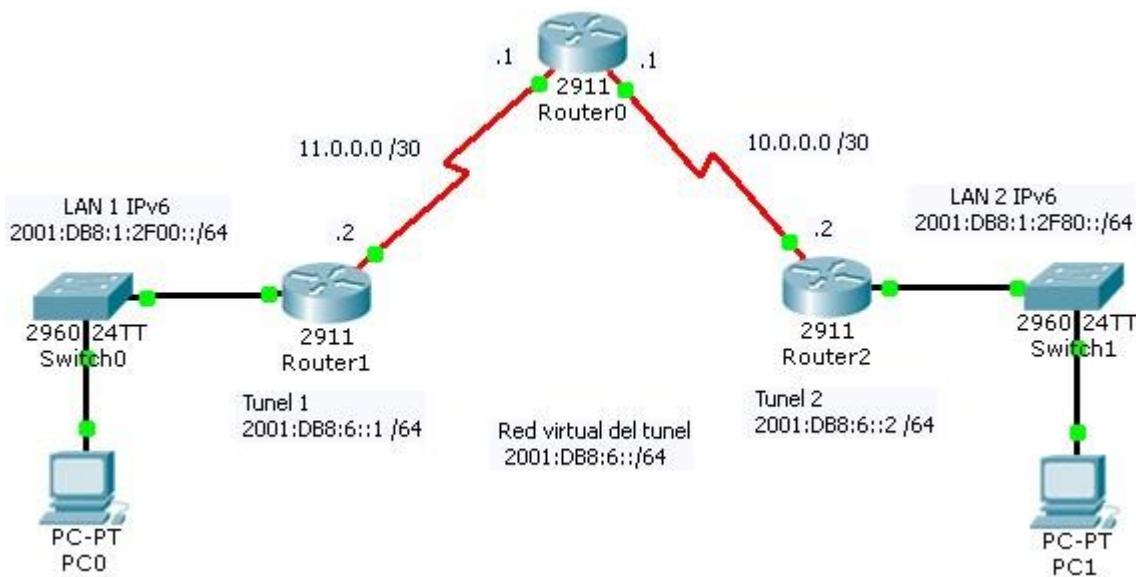
| Nº | REQUERIMIENTO                                                            | CANTIDAD |
|----|--------------------------------------------------------------------------|----------|
| 1  | Guía de Practica #13                                                     | 1        |
| 2  | Estación de trabajo de PC con sistema operativo Linux Centos o Windows 7 | 1        |
| 3  | Simulador Packet Tracer instalado.                                       | 1        |
|    |                                                                          |          |

### IV. PROCEDIMIENTO

#### PARTE I – TÚNEL ESTÁTICO

1. Proceda a armar la siguiente topología en Packet Tracer.

Los enlaces entre router's deberán de ser de tipo Serial (Módulo HWIC-2T) y los enlaces con las redes LAN de tipo GigabitEthernet (no es necesario agregar módulo ya que el router dispone 3 de forma integrada).



**NOTA:** Los diferentes router's deberán de ser modelo 2911 y Switch's 2960

2. Una vez armada la topología proceda a configurar las interfaces de red de cada router.

a. Router0

- S0/0/0: Dirección de interfaz = 11.0.0.1/30
- S0/0/1: Dirección de interfaz = 10.0.0.1/30

b. **Router1**

- Se0/0/0: Dirección de interfaz = 11.0.0.2/30
- Gi0/0: Configuración stateless con el prefijo de red = 2001:DB8:1:2F00::/64
- Definición de la Interfaz de túnel 1:

```
R1#configure terminal
R1(config)#interface tunnel 0
R1(config-if)#ipv6 address 2001:DB8:6::1/64
R1(config-if)#ipv6 enable
R1(config-if)#tunnel source Serial0/0/0
R1(config-if)#tunnel destination 10.0.0.2
R1(config-if)#tunnel mode ipv6ip
R1(config-if)#end
```

c. **Router2**

- Se0/0/1: Dirección de interfaz = 10.0.0.2/30
- Gi0/0: Configuración stateless con el prefijo de red = 2001:DB8:1:2F80::/64.
- Interfaz de la interface del segundo túnel:

```
R2#configure terminal
R2(config)#interface tunnel 0
R2(config-if)#ipv6 address 2001:DB8:6::2/64
R2(config-if)#ipv6 enable
R2(config-if)#tunnel source Serial0/0/1
R2(config-if)#tunnel destination 11.0.0.2
R2(config-if)#tunnel mode ipv6ip R2 (config-if)#end
```

3. Prueba de entrega de parámetros de red a nivel local o LAN.

- a. Configure los clientes de red para adquirir de forma automática los parámetros IPv6 de las respectivas redes LAN.
  - b. Verifique el otorgamiento mediante el comando `ipv6config`.

4. Configuración de rutas estáticas.

a. **Router1**

- Configure una ruta estatica IPv4 dirigida a la red 10.0.0.0/30 y con ip de siguiente salto 11.0.0.1
- Configure una ruta estática dirigida a la red LAN 2 IPv6 y como ip del próximo salto a la ipv6 del Tunel 2, ejecutando el siguiente comando:

**`ipv6 route 2001:DB8:1:2F80::/64 2001:DB8:6::2`**

## b. Router2

- Configure una ruta estatica IPv4 dirigida a la red 11.0.0.0/30 y con ip de siguiente salto 10.0.0.1
  
- Configure una ruta estática dirigida a la red LAN 1 IPv6 y como ip del próximo salto a la ipv6 definida para el Tunel 1, con el siguiente comando:

**ipv6 route 2001:DB8:1:2F00::/64 2001:DB8:6::1**

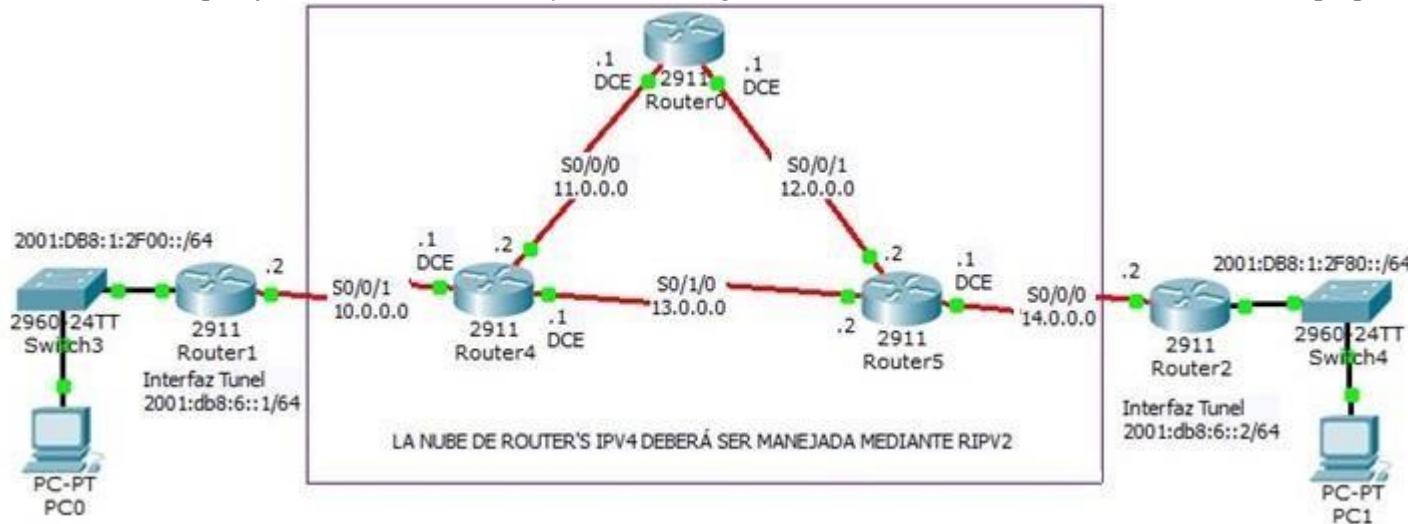
5. Realice pruebas de conectividad entre los host de ambas redes LAN basadas en IPv6.  
Las pruebas deberán ser exitosas.

## INVESTIGACIÓN COMPLEMENTARIA

### Ejercicio 1:

Arme la siguiente topología, en donde la nube de en medio será enrutada bajo el protocolo de configuración RIPv2.

Todos los enlaces seriales tiene un prefijo de máscara de red /30 y deberá configurar en cada router de borde a las rutas estáticas apropiadas



### Ejercicio 2:

Haga una copia de la topología anterior. Agregue un router (Router6) y conéctelo al Router0. La red de enlace entre ambos sera la ip **15.0.0.0 /30**. Router6 conectara a una tercera red LAN IPv6, configurada con Stateless, prefijo **2001:DB8:1:2FA0::/64** y con solamente a un host (agregar a PC2). Finalmente, haga las configuraciones necesarias para que la nueva red local pueda comunicarse con el resto de LAN IPv6 ya existentes.

#### Importante:

Para la configuración de los nuevos tuneles, se hará uso de las redes **2001:DB8:7::/64** y **2001:DB8:8::/64**.