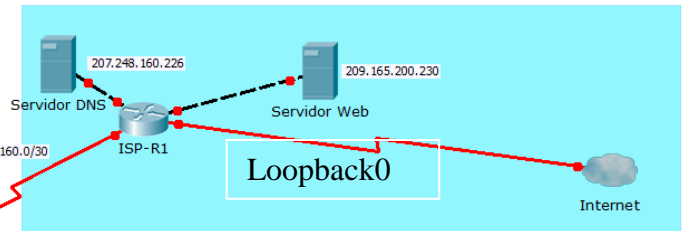
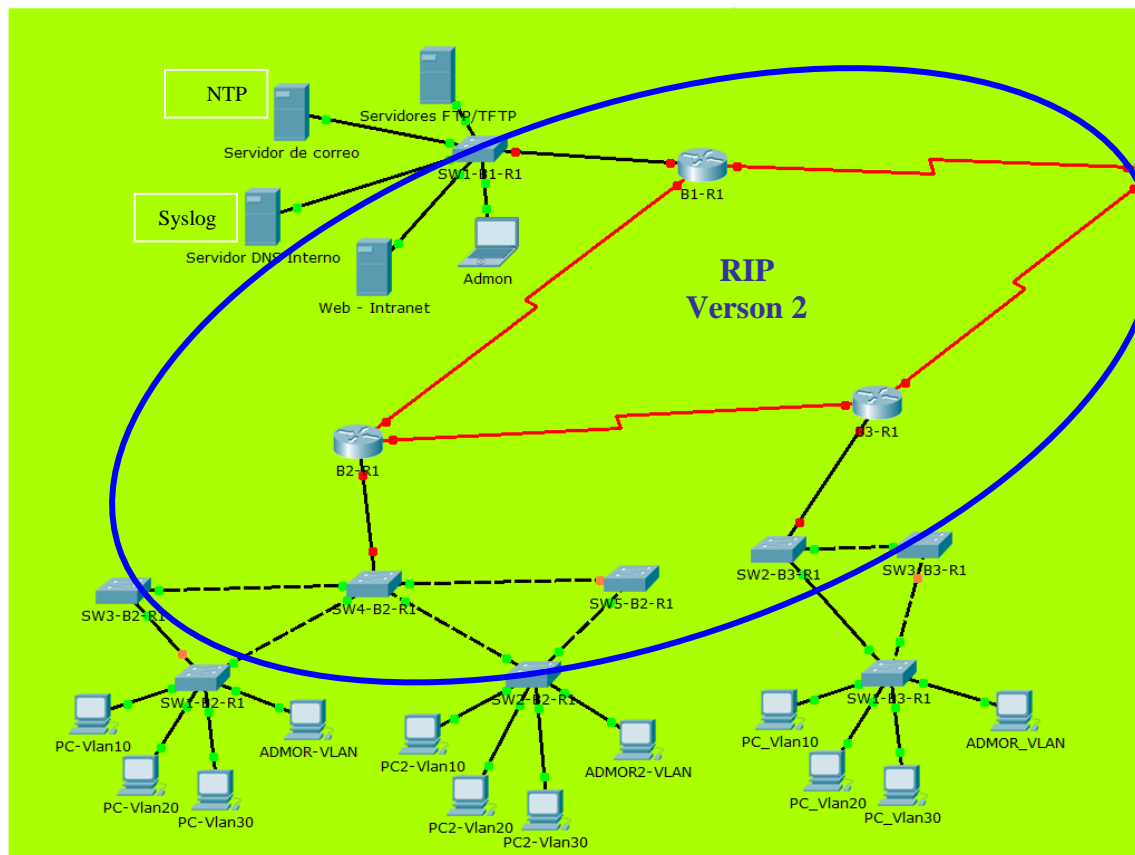
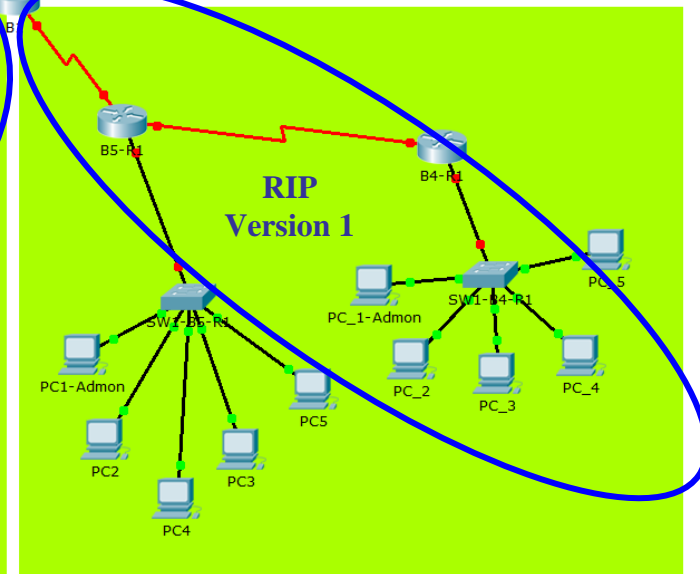


Diagrama de **TOPOLOGÍA**

Región R1



RIP Version 1



Región R2

REDES DE COMPUTADORAS: Caso de estudio

Objetivos de aprendizaje

- Realizar un cálculo eficiente de direccionamiento.
- Configurar VLAN.
- Configurar enrutamiento entre VLAN.
- Filtrar tráfico.
- Configurar DHCP.
- Configurar protocolo de enrutamiento dinámico RIPv.1 y RIPv.2
- Configurar NAT estática y dinámica para el acceso a Internet.
- Configurar el enrutamiento estático y predeterminado
- Configurar el servicio Syslog
- Configurar el servicio NTP
- Configurar los servicios, WEB, DNS, FTP, TFTP Y MAIL.

Situación

Usted es un técnico de red que trabaja para una compañía que decidió migrar de IPv4 a IPv6. Mientras tanto, debe admitir ambos protocolos (**dual stack**) en la Región 1. En este caso realizará la implementación de la configuración de IPv4 e IPv6 para los dispositivos. La Región 2 utiliza solo IPv4

Se necesita configurar la topología propuesta, para lo cual deberá realizar los siguientes pasos.

Paso 1: Creación de un esquema de direccionamiento IPv4.

Aunque se usarán direcciones privadas (RFC 1928), la empresa aprecia la eficiencia y la conservación de direcciones en el diseño. Para minimizar el desperdicio en el espacio de direcciones, han pedido que se utilicen máscaras de subred de longitud variable en la Región 1.

- Diseñar y documentar un esquema de direccionamiento según los requisitos que se muestran en la topología y en las tablas, tomando en cuenta lo siguiente:
 1. Utilice el espacio de dirección **10.128.0.0/15**
 2. Determinar primero el segmento necesario para la **Región** (R1)
 3. Asigne a partir de los **ULTIMOS** bloques disponibles de subredes de la red que se le ha asignado.
 4. Determinar el segmento necesario para cada **BxR1**.
 5. Determinar el segmento necesario para cada **Vlan, LAN y WAN** para cada **BxR1**.

6. Asigne la **última** dirección IP utilizable de cada subred a cada interfaz o subinterfaz de router o switch.

Paso 2: Creación de un esquema de direccionamiento IPv6.

- Diseñar y documentar un esquema de direccionamiento según los requisitos que se muestran en las tablas, tomando en cuenta lo siguiente:
 1. Utilice el espacio de dirección **2001:0DB0:ABCD::/48**
 2. Los espacios de direcciones IPv6 divídalos en subredes para admitir el diseño lógico jerárquico de la red armando una jerarquía de direccionamiento. Por motivos de seguridad para crear menos hosts por subred realizar la división en subredes en el límite de cuartetos.
 3. Determinar primero el segmento necesario para la **Región** (R1)
 4. Asigne a partir de las **PRIMERAS** subredes disponibles de la red que se le ha asignado.
 5. Determinar el segmento necesario para cada **BxR1**.
 6. Determinar el segmento necesario para cada **Vlan, LAN y WAN** para cada **BxR1**.
 7. Asigne la **última dirección** IP utilizable de cada subred a cada interfaz o subinterfaz de router o switch que lo requiera.
 8. Dejar que las direcciones link-local se generen de manera automática.

Paso 3: Completar la documentación de las tablas de direccionamiento.

Tabla de direccionamiento para Región R1 e ISP-R1

La siguiente tabla es solo un **EJEMPLO**, no corresponde al direccionamiento que se requiere en todo el caso. Deberá llenar una tabla con el siguiente formato con los dispositivos, interfaces, direcciones, etc., requeridos

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		No. de dispositivos
R1	S0/0/0	209.165.201.2	255.255.255.252	No aplicable
		2001:DB8:ACAD:1::2/64		No aplicable
	S0/0/1			No aplicable
		2001:0DB0:ABCD . . ./		No aplicable

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
		Dirección/Prefijo IPv6		No. de dispositivos
	S0/1/0			No aplicable
		2001:0DB0:ABCD . . ./		No aplicable
	S0/1/1			No aplicable
		2001:0DB0:ABCD . . ./		No aplicable
ISP-R1	S0/0/0	209.165.201.1	255.255.255.252	No aplicable
		2001:DB8:ACAD:1::1/64		No aplicable
	Fa0/0	209.165.200.225	255.255.255.252	No aplicable
		2001:DB8:ACAD:2::1/64		No aplicable
	Fa0/1	209.165.200.229	255.255.255.252	No aplicable
		2001:DB8:ACAD:3::1/64		No aplicable
Servidor DNS	NIC	209.165.200.226	255.255.255.252	
		2001:DB8:ACAD:2::2/64		
Servidor Web	NIC	209.165.200.230	255.255.255.252	
		2001:DB8:ACAD:3::2/64		
Simular Internet	Loopback 0	207.248.160.1	255.255.255.255	No aplicable
		2005:DB8:CAFE::1/64		No aplicable

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado/
		Dirección/Prefijo IPv6		No. de dispositivos
B1-R1	S0/0/0			No aplicable
		2001:0DB0:ABCD . . ./		No aplicable
	S0/0/1			No aplicable
		2001:0DB0:ABCD . . ./		No aplicable
	Fa0/0			12
		2001:0DB0:ABCD . . ./		
SW1-B1-R1				
		2001:0DB0:ABCD . . ./		
Servidor FTP/TFTP	NIC			
		2001:0DB0:ABCD . . ./		
Servidor de correo y NTP	NIC			
		2001:0DB0:ABCD . . ./		
Servidor DNS, Syslog	NIC			
		2001:0DB0:ABCD . . ./		

Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado/
		Dirección/Prefijo IPv6		No. de dispositivos
Servidor Web Interno Servidor Web público	NIC			
		2001:0DB0:ABCD . . . /		
Lap-Admon	NIC			
		2001:0DB0:ABCD . . . /		

En cada lugar se indica la cantidad de dispositivos que pertenecen a cada VLAN.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	No. de dispositivos
B2-R1 S1-S2-S3-S4-S5	VLAN 10			2000
	VLAN 20			800
	VLAN 30			1000
	VLAN 100			30

Dispositivo	Interfaz	Dirección IP	Máscara de subred	No. de dispositivos
B3-R1 S1-S2-S3	VLAN 10			1200
	VLAN 20			500
	VLAN 30			640
	VLAN 100			64

Tabla de direccionamiento para Región R2

- La Región R2 solo utiliza direccionamiento IPv4

Dispositivo	Interfaz	Dirección IP	Máscara de subred	No. de dispositivos
B4-R1	LAN			1800

Dispositivo	Interfaz	Dirección IP	Máscara de subred	No. de dispositivos
B5-R1	LAN			1000

Paso 4: Configuración básica de dispositivos.

- Nombre de dispositivo.
- Desactivación de la búsqueda del **DNS**
- Configuración del **logging synchronous**
- Mensaje **MOTD** que incluya la palabra warning (advertencia)
- Usuario y contraseña de puerto de consola.
- Contraseña del modo privilegiado.
- Configuración para acceso **SSH** a todos los routers y switches.

- Cifrar contraseñas de texto plano.
- Desactivar los puertos sin utilizar.
- Configurar el direccionamiento de los routers según los registros.
- Incluya una descripción adecuada para cada interfaz del router.
- Configure el direccionamiento de switches según los registros para realizar administración remota.

Paso 5: Configuración de VLAN y asignaciones de puertos.

- A los switches de la región que tienen VLANs, asignarles los puertos de acuerdo a la siguiente tabla.

Número de VLAN	Nombre de VLAN	Asignaciones de puertos
10	INVESTIGACIÓN/DESARROLLO	BxR1 - Sx, Fa0/2 – Fa0/4
20	PRODUCCIÓN	BxR1 - Sx, Fa0/5 – Fa0/7
30	VENTAS	BxR1 - Sx, Fa0/8 – Fa0/10
100	ADMOR	BxR1 - Sx, Fa0/11 – Fa0/20

- Asignar la VLAN 100 a los puertos activos en el switch del área de servidores. Deshabilitar los demás puertos.

Paso 6: Configuración de direccionamiento estático.

- Los dispositivos de la VLAN 100 se configuran todos de manera estática de acuerdo a los registros de las tablas de direccionamiento.

Paso 7: Configuración de switches.

- Configurar la interfaz VLAN y la Gateway predeterminada en cada switch.
- Configurar los enlaces troncales necesarios.
- La VLAN 99 es la nativa.

Paso 8: Configuración de seguridad de puerto.

Utilice la siguiente política para establecer la seguridad de puerto en los puertos de acceso de la VLAN 100.

- Permitir solo una dirección MAC
- Configurar la primera dirección MAC aprendida para que se “pegue” a la configuración.

-
- Configurar el puerto para que se desconecte si se produce una violación de seguridad.

Paso 9: Configuración de DHCP para IPv4 e IPv6.

Configurar el router **B1-R1** como servidor de **DHCP** para **IPv4**. Los pools de DHCP para las VLAN 10, 20 y 30 deben seguir los siguientes requisitos:

- Excluir las primeras 5 direcciones IP de cada pool para las LAN.
- El nombre del pool es R1_VLAN##, donde ## es el número de VLAN.
- Todos los dispositivos de las LAN o VLAN, reciben su IP del router R1. Deben poder acceder a la red de toda la empresa y a Internet.

Configurar los routers **B2-R1** Y **B3-R1** como servidores **DHCPv6** para todos los dispositivos de las VLAN 10, 20 Y 30.

Paso 10: Configuración de Servidores y PC

- Instalar y configurar los servidores indicados en la región.
- Deben estar registrados los servidores en el sistema público DNS. Utilice los nombres que desee para cada servicio.
- Configurar por lo menos una PC en cada VLAN.
- Configurar las PC para que utilicen DHCP
- Configure los router de la Región R1 como clientes NTP para que tengan los relojes sincronizados. Deben usar el servidor NTP.
- Habilitar el servicio de syslog en el servidor indicado en la topología.
- Configurar el switch del área de servidores y el router B1R1 para que utilicen el servicio de syslog.

Paso 11: Configuración enrutamiento entre VLAN.

- Utilice la tabla de direccionamiento de los routers para configurar el enrutamiento entre VLAN.
- Configurar las subinterfaces con la encapsulación **802.1Q**.
- Verificar la conectividad.

Paso 12: Configuración de enrutamiento dinámico tanto para IPv4 como para IPv6, considerando lo siguiente:

Configurar **RIPv2** en el área marcada de la región R1.

Configurar **RIPv1** en el área marcada de la región R2.

- La parte de la región marcada utiliza el protocolo RIPv1 en estas oficinas y por el momento desea seguir usando esta opción.

Deshabilite en toda la región las interfaces que no requieren enviar actualizaciones de enrutamiento.

Deberá investigar como redistribuir las rutas entre las dos regiones.

Verificar conectividad total en las regiones.

Paso 13: Configuración de ruta por defecto y su redistribución.

- Configurar en la región las rutas por defecto que se requieren para lograr conectividad externa con ambos protocolos IP.

Paso 14: Configuración del router ISP-R1 y sus dispositivos conectados.

- De acuerdo a la topología y a la tabla de direccionamiento.
- Instalar y configurar los servidores DNS y WEB.
- Debe estar registrado el sitio WEB en el sistema público DNS. Utilice el nombre de dominio que desee.
- Configurar el enrutamiento estático necesario que permita la conectividad a la región R1.

Paso 15: Configuración de NAT estática y PAT para IPv4.

En la empresa el router R1 proporciona acceso al conjunto de servidores y a Internet a través de la NAT.

- Deberá configurar NAT estática para los servidores WEB público y FTP de la región.
- El servidor web público de la región debe poder ser accesado desde el exterior.

Todos los dispositivos al salir a internet deberán utilizar una IP pública, utilice **PAT**.

- Permita que se traduzcan todas las direcciones para el espacio de direcciones de la empresa.
- La empresa posee el siguiente espacio de direcciones públicas a utilizar:
209.165.200.224/27

Verificar que **NAT** haga traducciones.

Paso 16: Verificación de la conectividad entre todos los dispositivos en la topología completa. Tanto para IPv4 como para IPv6.

Ahora debe tener conectividad de extremo a extremo.

- Utilice el ping para probar la conectividad de extremo a extremo.

-
- Cada router debe poder realizar un ping a todas las otras interfaces de los otros routers y a los servidores.
 - Cada host o router debe poder realizar una sesión **telnet** y **ssh** a cualquier router y switch.
 - Cada host debe poder acceder a los servicios de todos los servidores.

Paso 17: Configuración de ACLs.

Debido a que el ISP representa la conectividad a Internet, configure una ACL nombrada, llamada **FIREWALL**, en el siguiente orden:

- Los dispositivos de ISP-R1 solo podrán ver el servidor web de la región.
- Los dispositivos del ISP deberán dar respuestas a cualquier ping que reciban. Pero ellos no podrán hacer pings a los dispositivos de la región.
- Bloquee explícitamente cualquier otro acceso entrante desde el ISP y cualquier otro origen más allá del ISP.
- Todos los dispositivos internos de las regiones podrán tener conectividad total con todos los demás dispositivos de las regiones, excepto con el servidor FTP/TFTP, al cual solo tienen acceso los dispositivos de la VLAN100
- Todos los dispositivos de las áreas RIPv1 y RIPv2 deberán tener comunicación total.
- Considere las siguientes restricciones de los dispositivos del área RIPv1:
 - Las PC1-Admon del área de RIPv2 serán los únicos dispositivos que podrán tener acceso a los servidores conectados al switch SW1-B1-R1 del área RIPv2.
 - Los demás dispositivos del área de RIPv1 solo podrán tener acceso a los servidores web interno y público y al servidor de correo del área RIPv2
- Todos los dispositivos de ambas regiones podrán tener acceso al servidor web conectado al ISP-R1
- El dispositivo Admon que es el del Administrador, tendrá control total de todos los dispositivos de región.

Paso 18: Verificar la conectividad desde hosts externos.

Los dispositivos externos no deben poder hacer ping al servidor web de la región. Sin embargo, deben poder solicitar una página web.

Paso 19: Simulación en Packet Tracer.

La simulación deberá realizarse aprovechando la funcionalidad que tiene de trabajar en **red**.

- Deberán utilizar dos computadoras mínimo para la presentación en Packet Tracer.

Paso 20: Entrega e implementación final.

- Deberá entregar toda la documentación generada al resolver el caso y la simulación del Packet Tracer en modo multiusuario en un disco **el día de su implementación real**.
- Ese día se le indicará qué parte de la topología implementará, considerando como interfaces lógicas las interfaces faltantes necesarias.
- Ese día se le indicará cuando presentará la simulación completa en modo multiusuario en Packet Tracer

EVALUACIÓN:

No.	EVALUACIÓN DE:	PUNTAJE
1	Direccionamiento IPv4	12
2	Direccionamiento IPv6	12
3	Configuración de y enrutamiento entre VLANs	12
4	Seguridad de puerto, TELNET y SSH a dispositivos (routers y switches)	10
5	Implementación de DHCP	12
6	Protocolo RIPv2	10
7	Implementación de NAT y PAT	10
8	Configuración de ACLs	12
9	Conectividad de extremo a extremo según las políticas de seguridad	10
	TOTAL	100