SEDE XYZ

La sede cuenta con 5 VLANs configuradas de la siguiente manera:

- VLAN 10, nombre: RRHH, 192.168.20.0/24
- VLAN 20, nombre: SOPORTE, 192.168.30.0/24
- VLAN 40, nombre: GUEST, 192.168.40.0/24
- VLAN 99, nativa

El router realiza el enrutamiento inter-VLAN para la sede, utilizando la primera IP disponible en cada segmento como gateway.

Nota: La VLAN nativa se usa exclusivamente para troncales y no tiene una subred asociada. Las PCs que utilizan las direcciones .10 de cada segmento se encuentran en VLAN 10 y VLAN 20.

Todos los enlaces troncales deben permitir el paso de las VLANs 10, 20, 30, 40 y 99. La conexión entre switches se realiza utilizando agregación de enlaces (EtherChannel), y en caso de utilizar modo dinámico, ambos extremos deben estar configurados para negociar la formación del troncal.

Se han configurado las siguientes relaciones de enlace entre switches:

- Entre SW10 y SW12 se utiliza LACP en el grupo 1.
- Entre SW10 y SW20 se configura manualmente en el grupo 3.
- Entre SW12 y SW20 se utiliza PAGP en el grupo 2.

El switch SW10 actúa como el puente raíz para las VLANs 10 y 30, mientras que el switch SW20 es el puente raíz para las VLANs 20 y 40.

La VLAN 30 está reservada para la administración de los switches, cuyas direcciones IP deben ser accesibles desde otras VLANs. Las direcciones son: SW10 (.10), SW20 (.20) y SW12 (.12).

Nota: Los puertos de acceso deben activarse de inmediato y no deben esperar los timers de STP para entrar en funcionamiento.

SEDE ABCD

La sede cuenta con dos gateways configurados utilizando HSRP. El router principal, R1, tendrá una prioridad ajustada a 10 puntos por encima de la prioridad por defecto y deberá recuperar automáticamente su rol principal después de un fallo. El router secundario, R2, tendrá una prioridad ajustada a 10 puntos por debajo de la prioridad por defecto. La IP virtual utilizada será la “.3”.

El router R0 actuará como el servidor DHCP con un pool denominado "RED LOCAL" para la subred 192.168.1.0/24. Las direcciones IP desde la .1 hasta la .100 deben ser excluidas del pool DHCP. Además, se configurarán agentes de relay DHCP en los routers R1 y R2.

Asignación de IPs:

- **Impresora**: Debe tener una IP estática.
- **Laptop y PC**: Deben tener IPs dinámicas asignadas por DHCP.

Configuración de seguridad en el switch:

Configuración para el puerto del switch que conecta la impresora y la PC:

- **Port-Security**:
- Permitir una sola dirección MAC.
- La dirección MAC debe ser estática (sticky).
- No bloquear el puerto, pero no permitir otra dirección MAC.
- No enviar logs.

Configuración del puerto del switch que conecta al punto de acceso (AP):

- **Port-Security**:
- Permitir hasta 10 direcciones MAC dinámicas.
- No bloquear el puerto, pero no permitir más direcciones MAC adicionales.
- Enviar logs.

Configuración del punto de acceso (AP):

- **SSID**: skillexam
- **Clave WPA2**: 12345678

ENRUTAMIENTO

Configuración de rutas:

- **R1**: Configurar una ruta por defecto hacia R0.
- **R2**: Configurar una ruta por defecto hacia R0.
- **R0**:
- Configurar una ruta específica hacia R1 para la red 192.168.1.0/24 con una distancia administrativa (AD) de 5.
- Configurar una ruta específica hacia R2 para la red 192.168.1.0/24.
- Configurar una ruta por defecto hacia el ISP.
- **ISP**: Configurar rutas específicas hacia cada red interna.
- **R3**: Configurar una ruta por defecto hacia el ISP.

Pruebas

1. Realizar un ping entre las PC remotas y los switches de la red XYZ.
2. Verificar la navegación hacia `ccna.pka` desde cualquier PC.

Notas Finales

Para que esta evaluación sea aceptada como válida, asegúrate de lo siguiente:

1. En el menú "Opciones > Perfiles de usuario", tu nombre completo y correo electrónico deben estar registrados.
2. Guarda tu trabajo periódicamente y verifica que el archivo a enviar (formato *.pka) sea el correcto.