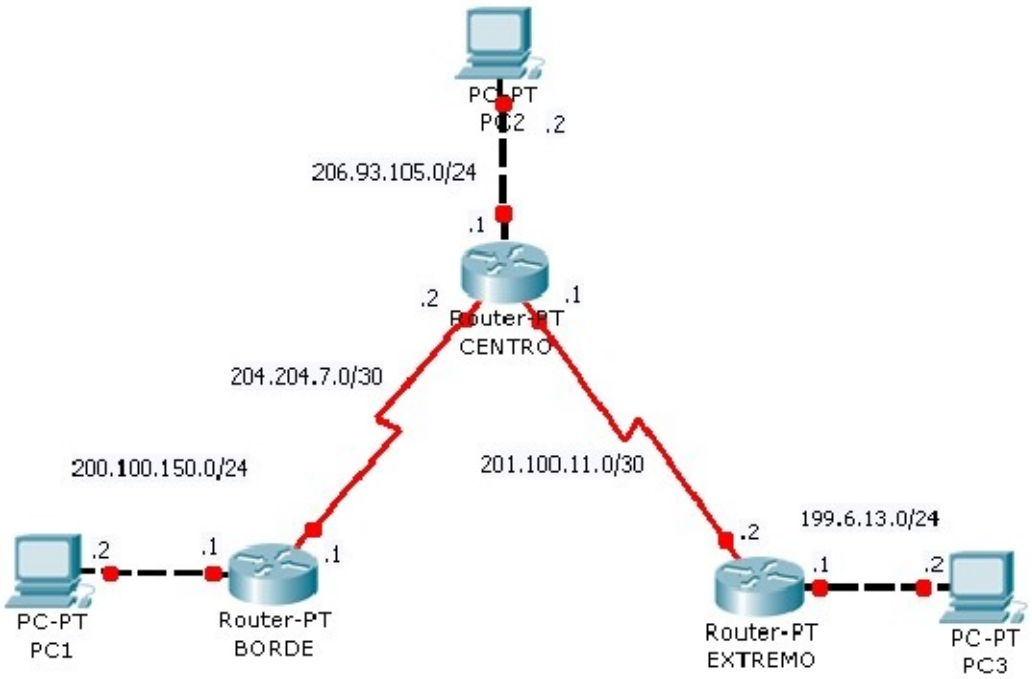
1. Diseña la siguiente topología.



2. Crea las rutas necesarias para tener conectividad total

3. Guarda la configuración de cada router en su NVRAM

4. Crear y aplicar una ACL estándar que bloquee el tráfico proveniente de PC-1 y con destino PC-3
a) Seleccionar el enrutador idóneo para crear la ACL. cualquier otro tráfico será permitido.
b) Escribir la ACL en el router seleccionado
c) Comprobar el funcionamiento de la ACL. Realizar un ping desde PC-1 hasta PC-3. Se debe dar una respuesta no exitosa.
d) Desactivar la ACL (no es lo mismo de eliminarla).
e) Realizar nuevamente pruebas de conectividad entre las PC-1 y PC-3.

5. Crear y aplicar una ACL estándar que bloquee el tráfico con origen PC-1 y destino PC-2, y que además permita el tráfico con origen PC-3 y destino PC-2. (Cualquier otro tráfico será negado).
a) Selección del enrutador: Más cerca del destino CENTRO
b) Escribir la ACL estándar
c) Realizar pruebas de ping desde PC-1 y PC3. Se obtendrán pruebas exitosas solo desde PC-3.
d) Desactivar la ACL en la interfaz Fastethernet0/0

6. Reescribir la ACL anterior para que permita o bloquee el tráfico de toda la red y no solo de un host en particular.
a) Escribir la ACL
b) Agregar un nuevo PC en el router BORDE (hacer uso de un Switch) y asignarle una IP diferente (que corresponda al rango de red)
c) Hacer pruebas de ping desde el nuevo PC
d) Desactivar la ACL

7. Configurar ACL's extendidas que denieguen las sesiones telnet desde cualquiera de las estaciones de trabajo (excepto de la PC-1) hacia BORDE. Cualquier otro tipo de tráfico será permitido.
a) **Opción 1:** Una sola ACL ubicada en BORDE (el tráfico atravesará toda la red y será detenido en la interfaz serial0/0 de BORDE).

b) Configuración y ubicación de la ACL
c) Intentar establecer sesiones telnet desde las estaciones PC-2 y PC-3. Los intentos deben fallar. Solamente desde PC-1 podrá establecer una conexión vía telnet exitosamente.
d) Desactivar la ACL de la interfaz serial0/0 de BORDE
e) **Opción 2:** ACL's independientes en CENTRO y EXTREMO (el tráfico será detenido lo más cerca posible del origen para no tener utilización innecesaria del ancho de banda en conexiones que serán denegadas).
f) Configuración y ubicación de ACL en CENTRO
g) Configuración y ubicación de ACL en EXTREMO
h) Nuevamente realizar pruebas intentando conectarse vía telnet con BORDE. Las conexiones desde PC-2 y PC-3 deben fallar.
i) Desactivar las ACL's de las interfaces fastethernet en los router CENTRO y EXTREMO

8. Configurar ACL's extendidas que permitan filtrar tráfico por tipo de servicios y por dirección de origen y destino.
a) Restringir el ping a los host con ip par dentro de la red LAN de EXTREMO
b) Realizar pruebas de ping con diferentes IP dentro de la red LAN de EXTREMO, las pruebas deberán ser exitosas si el ping es dirigido a una ip par.
c) Desactivar la ACL.
d) Colocar un servidor WEB en la red de CENTRO y permitirle solo a las últimas 3 IP de BORDE y EXTREMO que puedan acceder al servidor.
e) Realizar pruebas de navegación con diferentes ip desde cada red hacia el servidor web.
f) Desactivar las ACL's

9. Ejemplo de control de las líneas vty de CENTRO en una forma tradicional. Solo se permitirán las sesiones telnet iniciadas en la red correspondiente a la PC-2. Las redes a las que pertenecen las estaciones PC-1 y PC-3 serán denegadas. Todo el demás tráfico (que no sea telnet) será permitido.
a) Configuración de la ACL en CENTRO
b) Ubicación de la ACL
c) Realizar las pruebas necesarias para verificar el funcionamiento deseado de la ACL. Solo la PC-2 podrá exitosamente administrar CENTRO vía telnet.
d) Desactivar las ACL's

10. Alternativa usando control de las vty's
a) Configuración de la ACL (siempre en CENTRO)
b) Verificar nuevamente el funcionamiento de la ACL y comprobar que solamente PC-2 puede administrar CENTRO vía telnet.