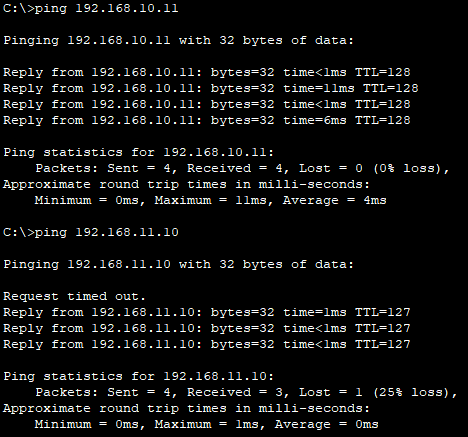
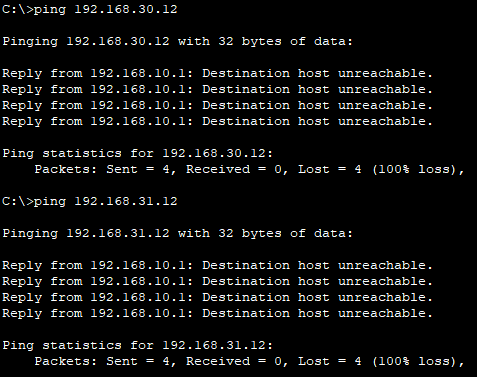
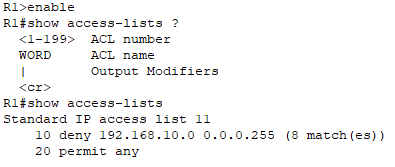
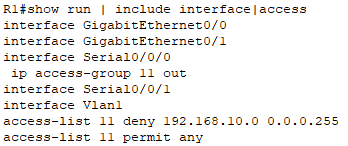
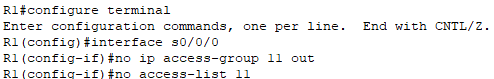
# PROPÓSITO DE LAS ACL

Preguntas de actividad

* ¿Por qué se realizaron de forma correcta los pings?
  + Porque las capas 1 a 3 funcionan correctamente y no existe una política que filtre los mensajes ICMP.
* ¿Por qué fallaron los pings? (pista: utilice el modo de simulación o vea las configuraciones del router para investigar).
  + Los pings fallan porque R1 está configurado con una ACL para denegar todo ping que salga de la interfaz serial 0/0/0.
* ¿A qué interfaz y en qué dirección se aplica la ACL?
  + Serial 0/0/0.

Bitácora

La finalidad de esta actividad es poder visualizar como funciona las ACL dentro de una red.

* Se realizo una prueba con la PC1, haciendo ping en los equipos PC2 y PC3, funcionando correctamente ya que no tiene alguna ACL configurada.
* Después, se realizó la prueba haciendo ping con los equipos PC4 y el servidor DNS, dando con ello un error y percatándonos que tiene una política de filtros para denegar todo ping que salga de la interfaz s0/0/0.
* Lo cual, para poder quitar el ACL tenemos que irnos directamente al Router R1 entrar al CLI y acceder. Ejecutamos el comando de show access-list para visualizar que cualquier paquete de origen de la red 192.168.10.0 esta denegada.
* Esto nos ayuda para identificar que cosas están dentro del ACL pero para poder checar un poco más especifico es utilizando el comando show run | include interface|access de lo cual nos da como resultado a que interfaz esta aplicada el ACL (serial0/0/0).
* Para poder quitar esa restricción, subimos al configure terminal y ejecutamos el comando interface s0/0/0 y no ip access-group 11 out lo cual hace de quitar el serial del grupo en donde esta aplicado el ACL al igual que eliminaremos por completo el ACL con el comando no access-list 11.
* Y por último, hacemos un ping en los equipos para corroborar que se corrigió el error.

