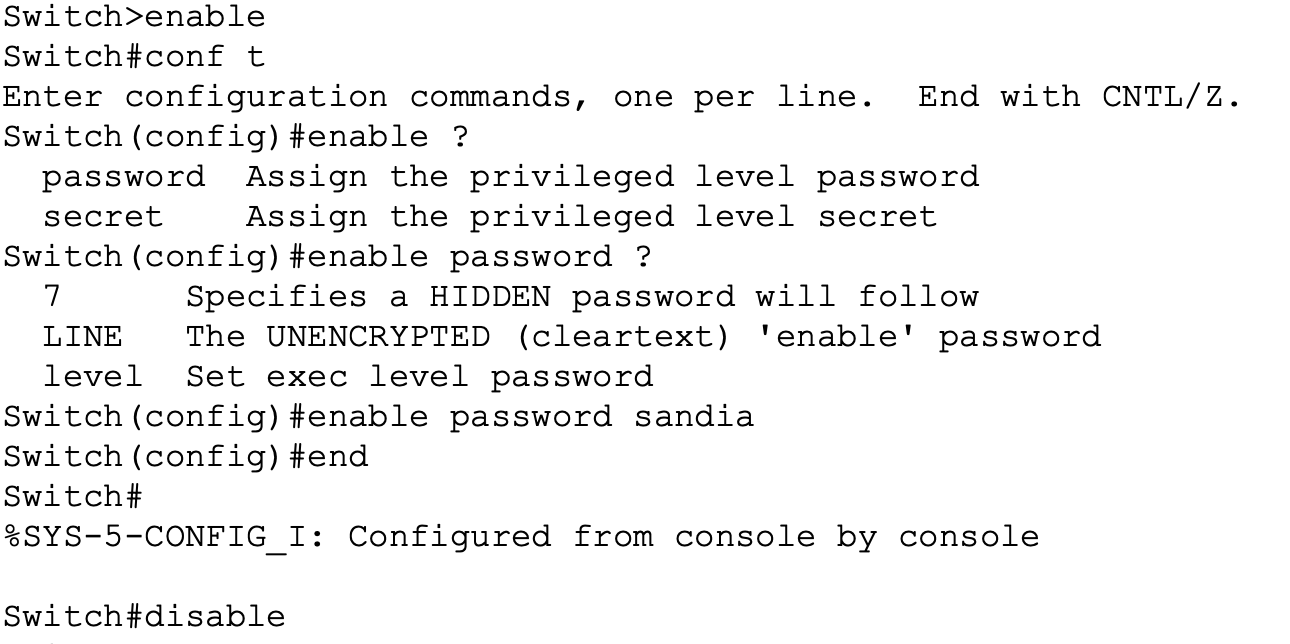
Agustin Salvador Quintanar de la Mora

A01636142

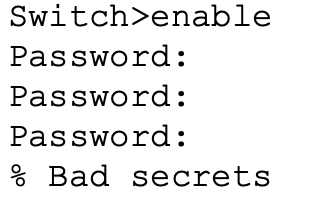
**Práctica 5**

**Proteger el acceso al modo privilegiado con una contraseña**

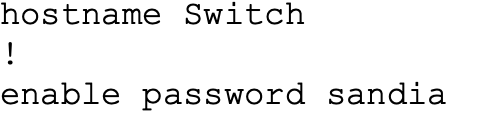


10. Teclee el comando para entrar al modo privilegiado y presione “enter” varias veces (no teclee ninguna contraseña):

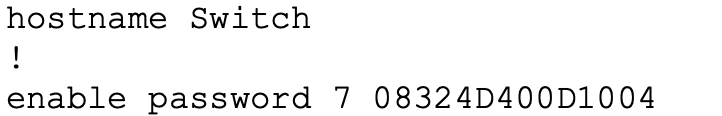
a. ¿Cuál es la respuesta del dispositivo?



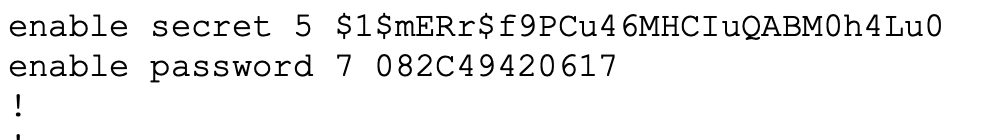
Show running-config antes del service password-encryption



Show running-config después del service password-encryption



Show running-config del secret



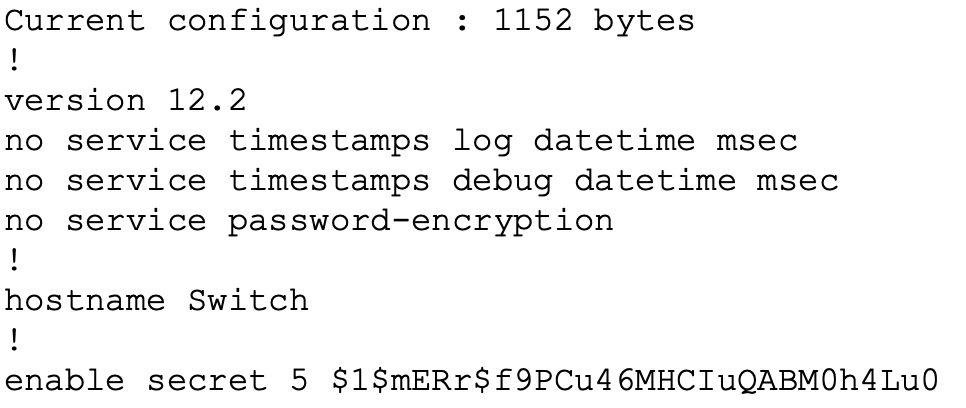
22. Compare como guardan las contraseñas los comandos de “enable secret” y “enable password”. ¿Cuál de las dos maneras de cifrar (proteger) contraseñas es la más segura?

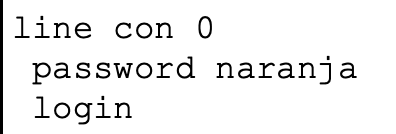
La secret porque utiliza mas caracteres y tiene una mayor longitud.

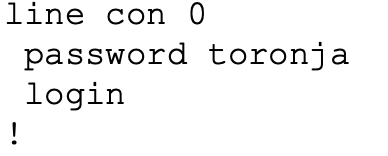
23. Salga del modo privilegiado y pruebe ambas contraseñas, primero “melon” y luego “manzana”. ¿Cuál de las dos acepta el dispositivo?

Manzana

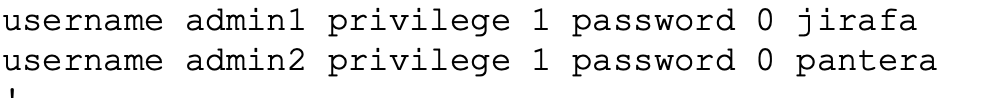
**Proteger el acceso al puerto de consola con una contraseña**

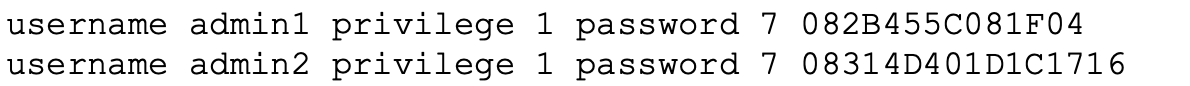






**Proteger el acceso al puerto de consola con un usuario y una contraseña**





45. Ejecute el comando para mostrar la configuración activa y busque las líneas de configuración de las cuentas de usuarios:

a. ¿Qué cambios observa en la forma en que se almacenan las contraseñas?

Sin encriptacion se guarda la contraseña tal como es, y con encriptacion se convierte a caracteres hexadecimales a simple vista.

b. ¿Cuál de las dos maneras de cifrar (proteger) contraseñas parece más segura?

La segunda (con encriptación).

Conclusion:

Se puede concluir que la encriptacion de contraseñas es una practica mas segura, asi como tambien es buena practica el manejo de usuarios.

Comando enable password/secret asigna una contraseña al modo de usuario privilegiado, password en line config 0 asigna una contraseña para inicializar la contraseña con un router, login local para habilitar la validacion por usuario y contraseña.