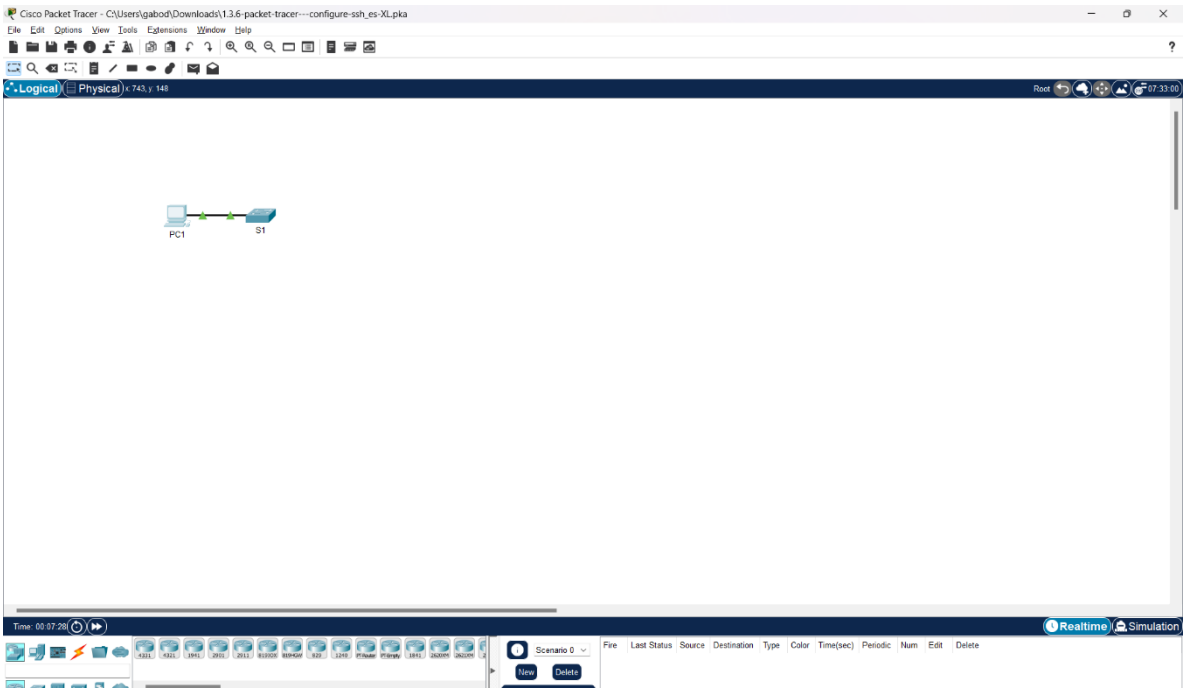

PT Activity: 00:07:31

c. Muestre la configuración actual y observe que las contraseñas están en texto no cifrado. Introduzca el comando para cifrar las contraseñas de texto no cifrado.

```
S1(config)# service password-encryption
```

d. Verifique que las contraseñas estén cifradas.

Parte 2: Cifrar conexiones

Paso 1: Establecer el nombre de dominio IP y generar claves seguras..

En general no es seguro utilizar Telnet, porque los datos se transfieren como texto no cifrado. Por lo tanto, utilice SSH siempre que esté disponible.

a. Configure el nombre de dominio **netacad.pka**.

b. Se necesitan claves seguras para cifrar los datos. Genere claves RSA con una longitud de clave de 1024.

Paso 2: Cree un usuario de SSH y reconfigure las líneas VTY para que solo admitan acceso por SSH.

a. Cree un usuario **administrador** con **cisco** como contraseña secreta.

b. Configure las líneas VTY para que revisen la base de datos local de nombres de usuario en busca de las credenciales de inicio de sesión y para que solo permitan el acceso remoto mediante SSH. Elimine la contraseña existente de la línea vty.

Paso 3: Verifique la implementación SSH

a. Cierre la sesión de Telnet e intente iniciar sesión nuevamente con Telnet. El intento debería fallar.

b. Intente iniciar sesión mediante SSH. Escriba **ssh** y presione la tecla **Enter** , sin incluir ningún parámetro que revele las instrucciones de uso de comandos. **Sugerencia**: La opción `-l` representa letter “L”, no el numero 1.

c. Cuando inicie sesión de forma correcta, ingrese al modo EXEC con privilegios y guarde la configuración. Si no pudo acceder de forma correcta al **S1**, reinicie y comience de nuevo en la parte 1.

Time Elapsed: 00:07:31 Completion: 100%

PC1

Physical Config Desktop Programming Attributes

SSH Client X

```
The name for the keys will be: S1.netacad.pka
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#netacad.pka
*Mar 1 1:3:13.101: %SSH-5-ENABLED: SSH 1.99 has been enabled
           ^
% Invalid input detected at '^' marker.

S1(config)#service passwo
S1(config)#service password-encryption
S1(config)#user name ad
S1(config)#user name admin
S1(config)#user name administrator secret cisco
                   ^
% Invalid input detected at '^' marker.

S1(config)#username administrator secret cisco
S1(config)#line vty 0 15
S1(config-line)#login 1
S1(config-line)#login local
S1(config-line)#tran
S1(config-line)#transport in
S1(config-line)#transport input ssh
S1(config-line)#no password cisco
S1(config-line)#exit
S1(config)#exit
S1#
```

Physical Config Desktop Programming Attributes

SSH Client X

```
Trying 10.10.10.2 ...Open


User Access Verification

Password:
S1>
S1>enable
Password:
S1#con
S1#conconfi
S1#conconfi t
           ^
% Invalid input detected at '^' marker.

S1#confi
S1#configure t
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip domain-name netacad.pka
S1(config)#crypto key generate rsa
The name for the keys will be: S1.netacad.pka
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#netacad.pka
*Mar 1 1:3:13.101: %SSH-5-ENABLED: SSH 1.99 has been enabled
           ^
```