LAB 3: SETTING PASSWORD

THEORY

Setting passwords is crucial for computer networking in order to safeguard hardware such as switches and routers. Only authorized users can access or modify a network device thanks to passwords. Passwords in networking assist safeguard the configuration and settings of network devices, much like we do with our computers or phones to protect personal data. We learned how to create various passwords in this lab to make routers and switches more secure.

Unencrypted Password

A straightforward, plain-text password is known as an unencrypted password. This indicates that there is no protection and the password is saved and shown in its original format. Someone can quickly view the unencrypted password by looking at the device's setup. Although it is simple to set up, it is not secure, particularly in actual networks where security is crucial. This kind of password is typically used in tiny networks where security is not a major concern or for basic learning.

Encrypted Password

Because an encrypted password is stored in a coded or jumbled format, it is more safe. The actual password cannot be read, even if someone checks the setup. To secure the password, the device employs encryption techniques. This keeps unwanted users away from the device. The enable secret command is typically used to set an encrypted password on Cisco devices. It is advised to use this kind of password to secure the device's key access points.

Console Password

When someone uses a console cable to connect directly to the router or switch, a console password is used. This physical connection was made when the device was first set up. We ensure that only those who are aware of the password can access the device via this direct connection by establishing a console password. It provides an additional degree of protection, particularly in settings where numerous people have physical access to equipment.

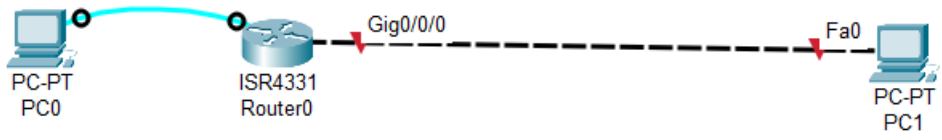
Telnet Password

When someone uses a console cable to connect directly to the router or switch, a console password is used. This physical connection was made when the device was first set up. We ensure that only those who are aware of the password can access the device via this direct connection by establishing a console password. It provides an additional degree of protection, particularly in settings where numerous people have physical access to equipment.

Setting up device for setting password

Using a single router and two PCs running Cisco Packet Tracer, a simple network configuration was established in this experiment.

Initially, two PCs and a router were set up on the workstation. The router was accessed via the console port on one PC, and network connectivity was accomplished via a crossover cable on the second PC. The first PC's console wire was connected to the router's console port. The router's command-line interface (CLI), where the password configurations were made, was accessed via this connection. A crossover cable was then used to link the second PC to one of the router's FastEthernet ports. Telnet remote access to the router was made possible by this connection. The second was given an IP address in order for it to connect to the router via the network. The router was accessed via the console connection after the connections were finished and the IP address was added.



Accessing router using the PC0

1. Two PCs and a router were set up in the Cisco Packet Tracer workspace.
2. The first PC was linked to the router's console port using a console cable.
3. The second PC was linked to the router's Gigabit Ethernet0/0/0 port using a crossover connection.
4. The second PC was given an IP address so that it could communicate with the router.

5. The Terminal was opened from the Desktop tab on the console-connected PC to gain access to the router.
6. The following commands were entered to configure the router interface:

   Router> en

   Router# config t

   Router(config)# int Gig 0/0/0

   Router(config-if)# ip address 192.168.1.1 255.255.255.0

   Router(config-if)# no sh

   Router(config-if)# exit

   Router(config)# exit

   Router# exit

   Router> ping 192.168.1.2

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig 0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no sh

Router(config-if)#
```

```
Router>ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

The router was accessible via PC0's terminal after being connected to PC0 via a console connector and to PC1 via a crossover cable. Configuration t entered global configuration mode, and privileged mode was entered using the enable command. After choosing the gig0/0/0 interface, the ip address command was used to assign the IP address 192.168.1.1 with subnet mask 255.255.255.0. The interface was activated with the no sh command. Following setting, a ping to PC1's IP address, 192.168.1.2, was performed to verify connectivity. The successful ping verified that everything was set up correctly.

When the PC connected by the crossover cable typed in the telnet 192.168.1.1 command, the message "Connection closed by foreign host" appeared. Consequently, the router connection was refused right away. This occurred because the router's Telnet service was improperly configured. Setting the login command and configuring the vty (virtual terminal) lines with a

password are necessary for Telnet to function. Without these configurations, the connection is refused because the router automatically ends the Telnet session.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
C:\>
```

Setting Unencrypted Password

1. Enter privileged EXEC mode on the router by logging in via the console:

   Router> en

2. Enter global configuration mode:

   Router# config t

3. Set the unencrypted password using the enable password command:

   Router(config)# enable password password_name

4. Exit to save configuration:

   Router(config)# exit

   Router#

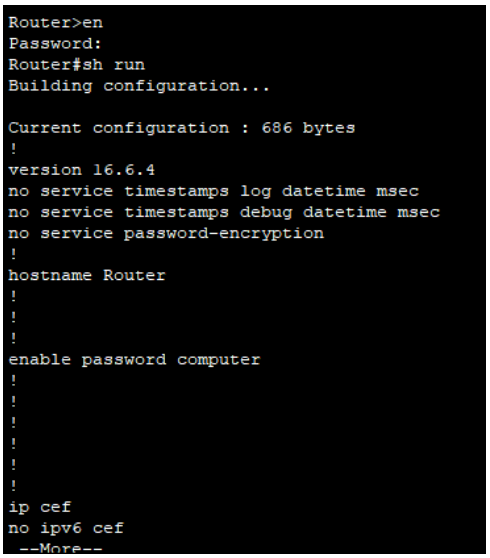
```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable password computer
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Going to privilege mode will now require password

```
Router>en
Password:
Router#
```

When the sh run command was entered in privileged EXEC mode (Router#), the router's current configuration was displayed. In this output, the unencrypted password appeared in plain text, making it visible to anyone with access to the terminal. The reason for this is that the

password was created with the enable password command, which does not encrypt it. This draws attention to a security issue because private data may be revealed. To avoid this, all plaintext passwords in the configuration file should be encrypted using the service password-encryption command..



Setting Encrypted password

1. Access the router and enter privileged EXEC mode:

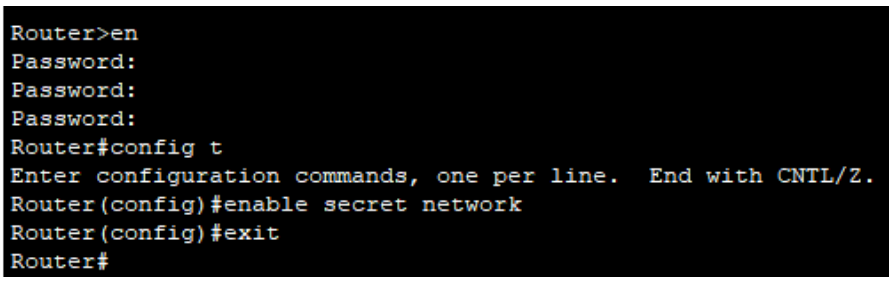
   Router> en

2. Enter global configuration mode:

   Router# config t

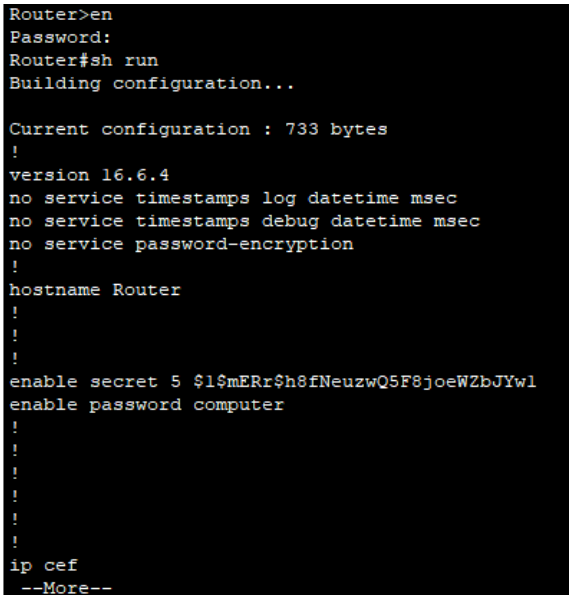
3. Set the encrypted password using enable secret:

   Router(config)# enable secret password_name



Checking password

When the sh run (short for show running-config) command was used in privileged mode (Router#), the router displayed its current configuration. In this output, the password set using the enable secret command appeared in an encrypted form, meaning it was not shown in plain text.



Setting console password

1. Put yourself in privileged EXEC mode:

   Router> en

2. Enter global configuration mode:

   Router# config t

3. Access console line configuration:

   Router(config)# line console 0

4. Set the console password:

   Router(config-line)# password password_name

5. Enable login using the password:

   Router(config-line)# login

6. Exit configuration mode:

   Router(config-line)# exit

   Router(config)# exit

   Router#

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password console
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Checking password

Even when accessing user mode (i.e., at the Router> prompt) after configuring the console password with the line console 0, password, and login instructions, a password prompt showed up. This implies that a password must now be entered before a user can access even the user EXEC mode whenever they attempt to access the router via the console port. This adds a basic layer of protection before any commands can be typed and helps shield the router from unwanted physical access.

```
User Access Verification

Password:

Router>
```

Setting Telnet password

1. Enter privileged EXEC mode:

   Router> en

2. Enter global configuration mode:

   Router# config t

3. Access the VTY (virtual terminal) lines:

   Router(config)# line vty 0 4

4. Set the Telnet password:

   Router(config-line)# password yourpassword

5. Enable login using the password:

   Router(config-line)# login

6. Exit configuration mode:

   Router(config-line)# exit

   Router(config)# exit

   Router#

```
User Access Verification

Password:

Router>en
Password:
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password telnet
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Checking Password through PC1

The screen requested a password when PC1 was opened and the command telnet 192.168.1.1 was entered in the Command Prompt. This occurred as a result of the router being configured to need a password in order to access Telnet. Therefore, in order to remotely log in to the router, PC1 had to input the right password before connecting.

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
Router>
```

Removing unencrypted password

1. Enter privileged EXEC mode:

   Router> en

2. Enter global configuration mode:

   Router# config t

3. Remove the unencrypted enable password by using the no form of the command:

   Router(config)# no enable password

4. Exit configuration mode:

   Router(config)# exit

   Router#

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no enable password
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Remove Encrypted password

2. Enter privileged EXEC mode:

   Router> en

3. Enter global configuration mode:

   Router# config t

4. Remove the unencrypted enable password by using the no form of the command:

   Router(config)# no enable secret

5. Exit configuration mode:

   Router(config)# exit

   Router#

```
Router>en
Password:
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no enable secret
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Checking the removal of password

The router stopped requesting a password when logging into privileged EXEC mode (Router#) after the encrypted password was removed using the command no enable secret. This lowers the router's security since anyone could access the higher-level instructions without entering a password. The router does not prevent access to privileged mode if neither an enable password nor an enable secret is set.

```
User Access Verification

Password:

Router>en
Router#
```

Removing Console Password

1. Enter privileged EXEC mode:

   Router> en

2. Enter global configuration mode:

   Router# config t

3. Go to the console line configuration:

   Router(config)# line console 0

4. Remove the console password:

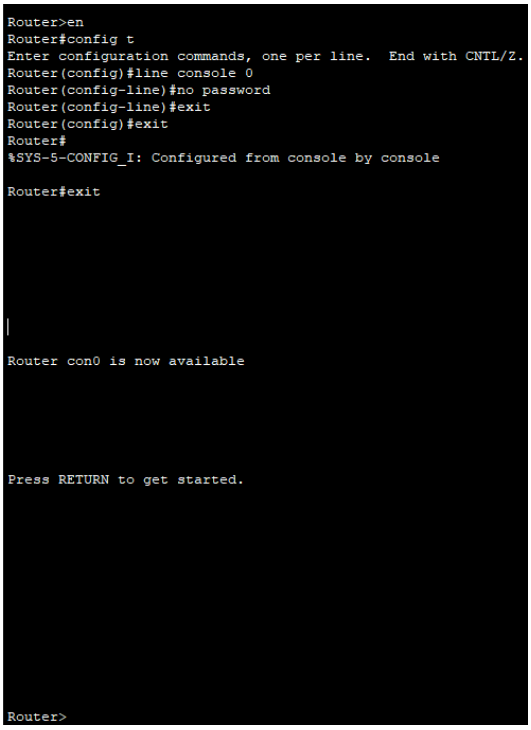
   Router(config-line)# no password

5. Exit configuration mode:

   Router(config-line)# exit

Router(config)# exit

Router#



No password was required to access the router via the console port once the console password was removed using the commands. This makes the router less secure because anyone might connect to it directly without entering a password.

Removing Telnet Password

1. Enter privileged EXEC mode:

   Router> en

2. Enter global configuration mode:

   Router# config t

3. Access the VTY lines:

   Router(config)# line vty 0 4

4. Remove the Telnet password:

   Router(config-line)# no password

5. Exit configuration mode:

   Router(config-line)# exit

   Router(config)# exit

   Router#

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#no password
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Checking password removal

The error message "Connection closed by foreign host" appeared when attempting to connect to the router using telnet 192.168.1.1 after the password was deleted using the no password command. This occurred because in order to grant Telnet access, the router needs a login method on the VTY lines. The router automatically terminates the Telnet connection if no password is entered and the login command is not enabled, blocking access.

```
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
C:\>
```

DISCUSSION

To prevent unwanted access, the router in this experiment was configured with a variety of passwords. Telnet passwords were set up for remote access, console passwords for direct access, and both encrypted and unencrypted passwords for privileged mode. Security was found to be impacted when passwords were eliminated. For instance, the connection was promptly terminated when the Telnet password was withdrawn, demonstrating that correct password configuration is necessary to permit remote access. It was shown how crucial password configuration is for limiting access to the router's settings.

CONCLUSION

To improve network security, the router was configured using passwords. Because encrypted passwords are hidden in the configuration, it has been demonstrated that they offer greater security than unencrypted ones. Passwords for the console and Telnet were used to secure local and remote access, respectively. Access to the router was left open when passwords were either forgotten or revoked, which might be dangerous. The importance of utilizing various password settings to enhance router security was comprehended through this experiment.