Monday, June 30, 2025 11:01 PM

📜 1. Set Password for Privileged EXEC Mode (enable)

🔐 Using enable password (plain text)

Router(config)# enable password cisco123

🔐 Using enable secret (encrypted - recommended)

Router(config)# enable secret strongpass

✅ *Note:* enable secret **overrides** enable password and is **encrypted in config**.

📜 2. Set Console Access Password

So that no one can access CLI via direct connection without login.

Router(config)# line console 0
Router(config-line)# password user123
Router(config-line)# login
Router(config-line)# exit

📜 3. Set VTY (Telnet/SSH) Access Password

Protects remote access via Telnet or SSH.

Router(config)# line vty 0 4
Router(config-line)# password remote456
Router(config-line)# login
Router(config-line)# exit

💡 line vty 0 4 = 5 simultaneous remote sessions (0 to 4)

📜 4. Encrypt All Plain Text Passwords

Router(config)# service password-encryption
This will encrypt all passwords in the config (except enable secret, which is already encrypted).

📜 5. Verify Your Passwords

Router# show running-config
You should see passwords like this:

```
enable secret 5 $1$...
line con 0
 password 7 070C285F4D06
 login
```

✅ Summary Table

Access Type	Command Example

Privileged EXEC Mode	enable secret strongpass
Console Access	line console 0 + password + login
VTY (Telnet/SSH)	line vty 0 4 + password + login
Encrypt All Passwords	service password-encryption