Project 4

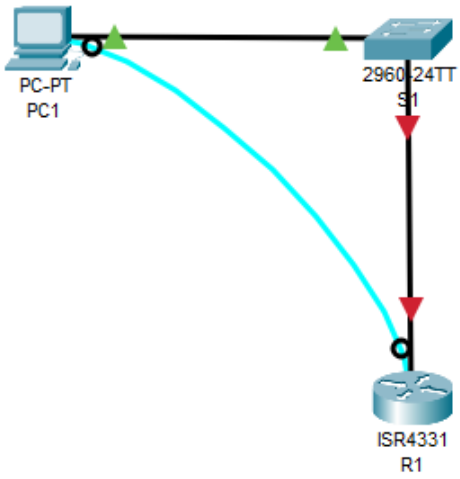
Basic network device security

Project description:

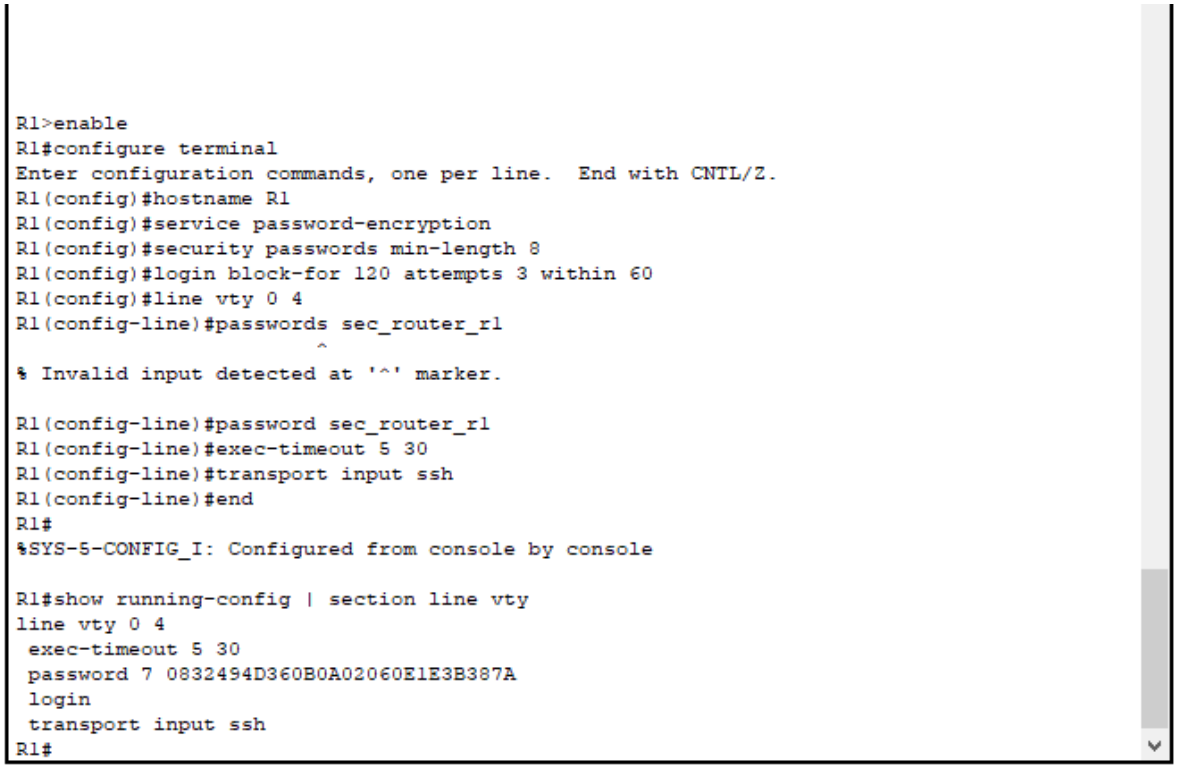
To ensure the basic security of a network device using the example of a Cisco router.

Steps:

- Create a topology of LAN



- Configure the basic security of the router
  1. Encrypt all open passwords
  2. Setting the minimum password length
  3. Setting a lock on multiple login attempts
  4. Setting up session logout after inactivity
  5. Setting up user disconnection on VTY lines
  6. Check the settings

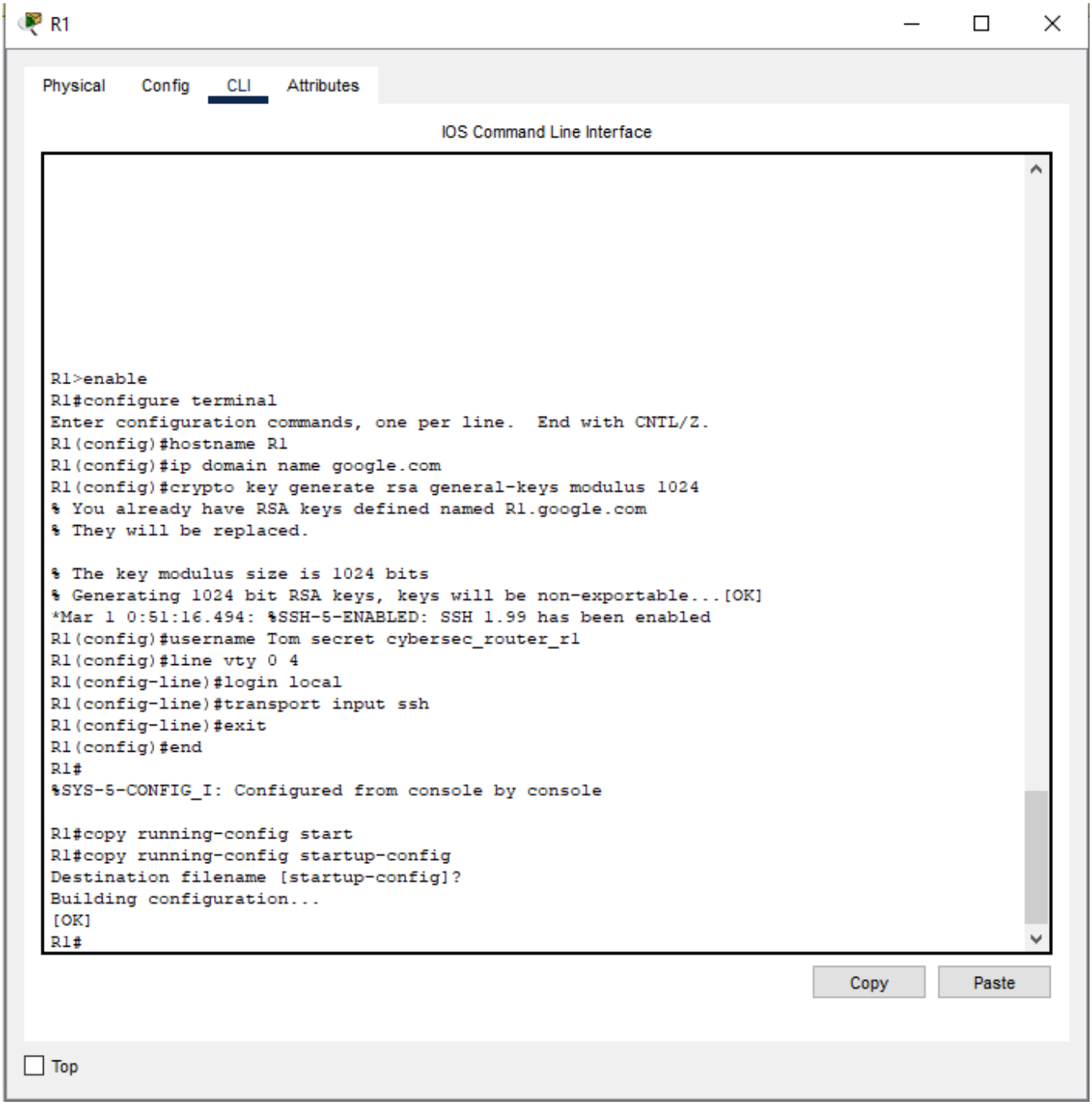


```
R1>enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname R1
R1(config)#service password-encryption
R1(config)#security passwords min-length 8
R1(config)#login block-for 120 attempts 3 within 60
R1(config)#line vty 0 4
R1(config-line)#passwords sec_router_r1
                        ^
% Invalid input detected at '^' marker.

R1(config-line)#password sec_router_r1
R1(config-line)#exec-timeout 5 30
R1(config-line)#transport input ssh
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show running-config | section line vty
line vty 0 4
 exec-timeout 5 30
 password 7 0832494D360B0A02060E1E3B387A
 login
 transport input ssh
R1#
```

- Activating SSH connection for secure remote access:
  1. Setting up a unique device name
  2. Configure the IP domain name
  3. Generate a key to encrypt SSH traffic
  4. Create a user and password
  5. Enable local database authentication
  6. Enable ssh session for vty lines
  7. Checking open ports
  8. Save configuration



Summary:

The basic security configuration of the router is configured. We need to understand that in order to fully ensure network security, we also need to use and configure: Firewall, VPN, Proxy, IPS/IDS, Wireshark + Siem for monitoring and analyzing logs.