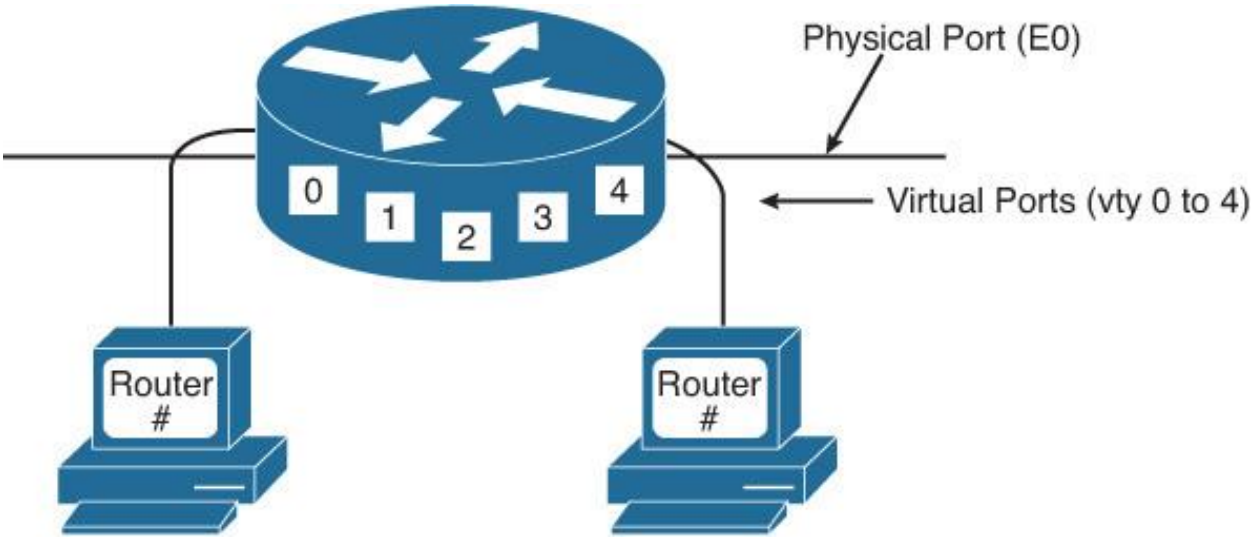
Cisco Routers Security:

- Cisco Routers are not security device and it is made for Routing.
- There are many features present in Cisco Routers, which can be misused.
- Attacker can easily gain access to router and can take control over the network.
- Network infrastructure devices routers are the assets of an enterprise.
- Router play an important role & thus need to be protected & configured accordingly.
- Cisco routers can be secure using many methods such as Physical Security.
- Router Hardening, Operating System Security and Administrative Access Security.
- Enterprises focus on protecting data, servers; applications etc but forget about Router.
- A compromised router can be devastating to the whole security of the enterprise.
- Hardening Routers is essential for enhancing the whole security of the enterprise.

Enable Mode Passwords
R1(config)# enable password cisco
R1(config)# do show running-config | include password
R1(config)# service password-encryption
https://www.ifm.net.nz/cookbooks/passwordcracker.html
R1(config)# enable secret cisco
R1(config)# do show running-config | include secret
https://www.ifm.net.nz/cookbooks/cisco-ios-enable-secret-password-cracker.html
R1(config)# enable algorithm-type sha256 secret cisco
R1(config)# do show running-config | include secret
R1(config)# enable algorithm-type scrypt secret cisco
R1(config)# do show running-config | include secret

VTY (Virtual Terminal Lines):

- VTY is stands for Virtual Terminal Lines or Virtual Teletype.
- VTY is a Command Line Interface (CLI) created in a cisco router.
- VTY is used to facilitate a connection to the daemon via Telnet.
- VTY is just a way of accessing the switches or routers CLI remotely.
- Virtual Terminals are logical connections from the network to the router.
- VTY are typically telnet connections to cisco witches or cisco routers.
- Telnet (Teletype Network) is used to manage routers or switches remotely.
- A Telnet client and server application ships with Cisco's IOS software default.
- Telnet (Teletype Network) commonly uses TCP port 23 to connect to devices.



Configure VTY Authentication R1	
Password Only	**Username & Password**
R1(config-)≠ line vty 0 4 R1(config-line)≠ password cisco R1(config-line)≠ login	R1(config-)≠ username admin password cisco R1(config-)≠ line vty 0 4 R1(config-line)≠ login local
AAA Local Database	
R1(config)# aaa new-model R1(config)# aaa authentication login default local R1(config)≠ username admin password 123 R1(config)# line vty 0 4 R1(config-line)# login authentication default	
R1(config)#access-list 1 permit host 1.1.1.10 R1(config)#line vty 0 4 R1(config-line)#access-class 1 in	

SSH (Secure Shell):

- SSH is network term, which is stands for Secure Shell.
- SSH provides secure remote access connection to network devices.
- SSH (Secure Shell) are two versions SSH Version 1 and SSH Version 2.
- Communication between client & server is encrypted in both SSH version.
- SSH (Secure Shell), version 2 is more secure than version SSH Version 1.
- SSH (Secure Shell) commonly uses TCP port 22 to connect to devices.
- SSH, as the preferred management protocol under the VTY interfaces.
- SSH provides a secure and reliable mean of connecting to remote devices.
- SSH (Secure Shell), Version 2 is the more secure and commonly used version.
- SSH (Secure Shell), require an IOS image that supports crypto features.
- SSH is a more secure way to configure routers, switches or firewalls.

SSH for Secure Management	
R1(config)# ip domain-name ksa.com	
R1(config)# crypto key generate rsa modulus 1024	
R1(config)# ip ssh timeout 60	
R1(config)# ip ssh authentication-retries 3	
R1(config)#crypto key zeroize rsa	
R1(config)#ip ssh version 2	
R1(config)#username admin privilege 15 secret cisco	
R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#transport input ssh R1(config-line)# exec-timeout 5 0	
R1#show ssh	R1#show ip ssh
R1#show crypto key mypubkey rsa	R1#debug ip ssh

Allow Specific Hosts for Remote Management
R1(config)#access-list 1 permit host 1.1.1.10
R1(config)#line vty 0 4 R1(config-line)#access-class 1 in