**Router Commands**

**Enter privilege mode**

Router> enable //Console into the router

Router# //Enter into privileged EXEC mode

**Enter config mode**

Router# conf t //Enter configuration for terminal

**Assign a device name to the router**

Router(config)# hostname R1 //Sets hostname for Router

**Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names**

R1(config)# no ip domain-lookup //Disable DNS lookup

**Assign class as the priviledge EXEC encrypted password**

R1(config)# enable secret class //Set encrypted enable password

**Assign cisco as the console password and enable login**

R1(config)# line con 0 //Enter line console

R1(config-line)# password cisco

R1(config-line)# login

R1(config-line)# exit

R1(config)#

**Assign cisco as the vty password and enable login**

R1(config-line)# line vty 0 4 //Enter line vty

R1(config-line)# password cisco

R1(config-line)# login

R1(config-line)# exit

R1(config)#

**Encrypt the clear text password**

R1(config)# service password-encryption

**Create a banner that warns anyone accessing the device that unauthorized access is prohibited**

R1(config)# banner motd # Unauthorized access prohibited! #

R1(config)#

**Configure and activate both interfaces on the router**

R1(config)# int g0/0

R1(config-if)# description Connection to PC-B.

R1(config-if)# ip address [ip] [subnet]

R1(config-if)# no shut

R1(config-if)#

R1(config-if)# int g0/1

R1(config-if)# description Connection to S1.

R1(config-if)# ip address [ip] [subnet]

R1(config-if)# no shut

R1(config-if)# exit

R1(config)#

**Save the running configuration to the startup file**

R1# copy run start

**Set the clock on the router**

R1# clock set [hour:minutes:seconds] [date month year]

**Erase the startup configuration file from NVRAM**

Router# erase startup-config

**Reload the router**

Router# reload

**Configure the Router for SSH Access**

**//Configure device name**

Router(config)# hostname R1

**//Change the privileged EXEC encrypted password**

R1(config)# enable secret Enablep@55

**//Require that a minimum of 10 characters be used for all passwords**

R1(config)# security passwords min-length 10

**//Configure the domain for the device**

R1(config)# ip domain-name ccna-lab.com

**//Configure the encryption key method**

R1(config)# crypto key generate rsa modulus 1024

**//Configure a local database username**

R1(config)# username admin privilege 15 secret adminpass

**//Enable Telnet and SSH on the inbound VTY lines using the transport input command**

R1(config)# line vty 0 4

R1(config-line)# transport input telnet ssh

R1(config-line)# login local

R1(config-line)# end

R1#

R1# copy r s

**//Secure the console and VTY lines**

R1(config)# line console 0

R1(config-line)# exec-timeout 5 0

R1(config-line)# line vty 0 4

R1(config-line)# exec-timeout 5 0

R1(config-line)# exit

R1(config)#

**//To impede brute force login attempts**

R1(config)# login block-for 30 attempts 2 within 120

**//Entering telnet from PC**

Open Teraterm or Putty and select ssh

**//Entering SSH from PC**

Open Teraterm or Putty and select ssh

REMEMER: use version 1 SSH for teraterm

**Switch Commands**

**Connect to the switch**

Switch> enable

Switch#

**Determine if there have been any VLANs created**

Switch# show flash

**Delete the VLAN file**

Switch# delete vlan.dat

**Erase the startup configuration file from NVRAM**

Switch# erase startup-config

**Reload the switch**

Switch# reload

**Enter config mode**

Switch# conf t

**Assign a device name to the switch**

Switch(config)# hostname S1

**Disable DNS lookup to prevent the switch from attempting to translate incorrectly entered commands as though they were host names**

S1(config)# no ip domain-lookup

**Assign class as the priviledge EXEC encrypted password**

S1(config)# enable secret class

**Assign cisco as the console password and enable login**

S1(config)# line con 0

S1(config-line)# password cisco

S1(config-line)# login

S1(config-line)# exit

S1(config)#

**Assign cisco as the vty password and enable login**

S1(config-line)# line vty 0 15

S1(config-line)# password cisco

S1(config-line)# login

S1(config-line)# exit

S1(config)#

**Encrypt the clear text passwords**

S1(config)# service password-encryption

**Create a banner that warns anyone accessing the device that unauthorized access is prohibited**

S1(config)# banner motd # Unauthorized access prohibited! #

S1(config)#

**Configure and activate both interfaces on the switch**

S1(config)# int vlan 1

S1(config-if)# ip address [ip] [subnet]

S1(config-if)# no shut

S1(config-if)# exit

S1(config)#

**Configure Default Gateway**

S1(config)# ip default-gateway [ip address]

**Save the running configuration to the startup file**

S1# copy run start

**Configure the Switch for SSH Access**

**//Configure device name**

Switch(config)# hostname S1

**//Strength passwords**

S1(config)# enable secret Enablep@55

**//password min-length not available on switch**

**//Configure the domain for the device**

S1(config)# ip domain-name CCNA-lab.com

**//Configure the encryption key method**

S1(config)# crypto key generate rsa modulus 1024

**//Configure a local database username**

S1(config)# username admin privilege 15 secret adminpass

**//Enable Telnet and SSH on the inbound VTY lines using the transport input command**

S1(config)# line vty 0 15

S1(config-line)# transport input telnet ssh

S1(config-line)# login local

S1(config-line)# end

S1#

S1# copy r s

**//Secure the console and VTY lines**

S1(config)# line con 0

S1(config-line)# exec-timeout 10 0

S1(config-line)# line vty 0 15

S1(config-line)# exec-timeout 10 0

S1(config-line)# exit

S1(config)#

**//To impede brute force login attempts**

S1(config)# login block-for 30 attempts 2 within 120

S1(config)# end

**//Entering telnet from PC**

Open Teraterm or Putty and select ssh

**//Entering SSH from PC**

Open Teraterm or Putty and select ssh

REMEMER: use version 1 SSH for teraterm

**Show Commands:**

show ip interface brief  
show run  
show version

Show cdp neighbor

Show flash