April 15, 2018 12:52 PM

Setup device configuration

Set Device Name to "student123"

1. Enter privileged Exec
   enable
2. Access Global Configuration
   configure terminal
3. Enter command hostename followed by the name of the switch
   hostename student123

Secure User EXEC mode with password "class"

1. Access Global Config
   Configure terminal
2. Access Console Configuration
   Enable secret "*class*"

Secure Console lines using password "cisco"

VTY lines provide remote access. Very useful, but unprotected, this poses a LARGE security risk

1. Access Global Config
   Configure terminal
2. Access Console Configuration
   Line console 0
3. Enter password command, followed by the specific password
   Password cisco
4. Enable VTY access using the login command
   Login

Secure VTY lines using password "cisco"

VTY lines provide remote access. Very useful, but unprotected, this poses a LARGE security risk

1. Access Global Config
   Configure terminal
2. Access VTY Line Configuration
   Line vty 0 15
3. Enter password command, followed by the specific password
   Password cisco
4. Enable VTY access using the login command
   Login
5. Enable login from out of band access
   Login local

Encrypt Passwords

Hide above set passwords in Startup-config and running-config files

1. Access Global Config
   Configure terminal
2. Use the service password-encryption command
   Service password-encryption
3. (optional) confirm encryption in running config from the privileged EXEC menu
   show running config

Enable Banner Messages warning against unauthorized access

1. Access Global Config
   configure terminal
2. User banner motd command, with delimiting characters (#, ^ etc).
   Banner motd ^Authorized Access Only^

Set up IP address and Subnet Gateway on switch

1. The IP of a switch is related to a virtual line VLAN 1
   Interface vlan 1
   for Router interface FastEthernet0/0
2. Apply the IP address
   ip address *"ip address" "subnet-mask"*
3. Enable the ip address (get rid of the default "off" setting
   No shutdown

Save the Running Config File

Always remember there are two configs (startup and running). We have configured running config, but now must save it to startup

1. Copy running-config startup-config

Create SSH Server

1. Create Username and Password (encrypted)

(config)#Username username secret 5 cisco

2. Create Domain Name (be sure to have configured telnet on vty lines

(config)#ip domain-name domain.com

3. Make crypto key

(config)#crypto key generate rsa

4. SSH version 2

(config)#ip ssh version 2

VLAN set up (repeat for each VLAN range)

(config)#vlan 10

(config-vlan)#name students

(config)#int vlan 99
(config-int)#ip address 192.168.1.1 255.255.255.252

(config)#interface range fa0/1-10

(config-if-range)#Switchport mode access

(config-if-range)#Switch port-security

(config-if-range)#Swit port.. Max (max number)

(config-if-range)#Swit port... violation (type)

(config-if-range)#Swi port... mac sticky b

Trunking

Interface
Sw mo trunk
Sw trunk encapsulation dot1q
Sw trunk native vlan 99
Swi trun allowed vlan 1,2,3

ACLS

Create named ACL RFC1918

(config)#ip access-list standard RFC1918

Block 10.0.0.0/8; block 172.16.0.0/12; permit all other

(config-std-nacl)#deny 10.0.0 0.255.255.255
(config-std-nacl)#deny 172.16.0.0 0.15.255.255
(config-std-nacl)#permit any

Apply ACL to int s0/0/0

(config-if)#ip access-group RFC1918 out

Port Forwarding

Permit remote ssh to switch 172.16.1.58 from global public 20.30.40.1 (port 22)

(config)#ip nat inside source static tcp 172.16.58 22 20.30.40.1 22

Apply to interfaces (ip nat in / ip nat out)

PAT

Allow private address translated to s0/0/0 public access via numbered ACL 1

(config-if)#ip access-list standard 1
(config-std-nacl)#permit 10.0.0.0 0.255.255.255
(config-std-nacl)#permit 172.16.0.0 0.0.255.255

(config-if)#ip nat inside source list 1 interface s0/0/0 overload