

Lab - Securing Network Device Setting Parties Device Setting Table 1

In Part 1, you will set up the network topology and configure basic settings, such as the interface IF Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1 _{o bereins}	G0/1	192,168.1 ₋₁₁₆ m	255.255.255.0	able DNS loolAMto
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings acres and phisesops encyns amew fait remaid a staeto

proPart 2: Configure Basic Security Measures on the Router shalm F\00 and efsolusions amplited

Part 3: Configure Basic Security Measures on the Switch Configure the default SVI on the switch with the IP address information according to the Addressing

Background / Scenario

It is recommended that all network devices be configured with at least a minimum set of best practice security commands. This includes end user devices, servers, and network devices, such as routers and switches.

In this lab, you will configure the network devices in the topology to accept SSH sessions for remote management. You will also use the IOS CLI to configure common, basic best practice security measures. You will then test the security measures to verify that they are properly implemented and working correctly.

Note: The routers used with CCNA hands-on labs are Cisco 1941 ISRs with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary table at the end of the lab for the correct interface identifiers. Similar to

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor. Note: Best practice guidelines require the use of strong passwords, such as those shown here, in a

Required Resources's bas obel and see that countries and all and a see that decome and controlled the countries and controlled the controlled the countries and controlled the controlled the countries and controlled the contro

- 1 Router (Cisco 1941 with Cisco IOS software, release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology



Addressing Table

Part 1: Configure Basic Device Settings alved showted gringed - dal

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the devices.

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology and cable as necessary.

Step 2: Initialize and reload the router and switch.

Step 3: Configure the router and switch.

- Console into the device and enable privileged EXEC mode.
- b. Assign the device name according to the Addressing Table.
- c. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.
- Assign class as the privileged EXEC encrypted password.
- e. Assign cisco as the console password and enable login.
- f. Assign cisco as the VTY password and enable login.
- g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- Configure and activate the G0/1 interface on the router using the information contained in the Addressing Table.
- i. Configure the default SVI on the switch with the IP address information according to the Addressing Table.
- j. Save the running configuration to the startup configuration file.

Part 2: Configure Basic Security Measures on the Router

management. You will also use the IOS CLI to configure common, basic best practice security in Step 1: Will Encrypt the clear text passwords are passwords.

EM(PR1 (config) #3 service password-encryption of no-shed AUOO day besu stolugg of T stol

(universatk9 image). The switches used are Clarco Catalyst 2950s with Clarco IOS Release 15.8(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Cabrowassq inehtgnerts! C2 qetS

An administrator should ensure that passwords meet the standard guidelines for strong passwords. These guidelines could include combining letters, numbers and special characters in the password and setting a minimum length.

Note: Best practice guidelines require the use of strong passwords, such as those shown here, in a production environment. However, the other labs in this course use the cisco and class passwords for ease in performing the labs.

- a. Change the privileged EXEC encrypted password to meet guidelines.

 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

Alf show in interface brief

Step 3: Enable SSH connections.

a. Assign the domain name as CCNA-lab.com.

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

- b. Create a local user database entry to use when connecting to the router via SSH. The password should meet strong password standards, and the user should have user EXEC access. If privilege level is not specified in the command, the user will have privileged EXEC (level 15) access by default. R1(config)# username SSHadmin privilege 1 secret Admin1p@55
- c. Configure the transport input for the VTY lines so that they accept SSH connections, but do not allow Telnet connections.

R1(config) # line vty 0 4

R1(config-line) # transport input sshinds Explain des transport input security Explain des transport des transport input security Explain des transport des

The VTY lines should use the local user database for authentication.

R1(config-line) # login local R1(config-line)# exit

e. Generate a RSA crypto key using a modulus of 1024 bits. Challesting HSS and generate a RSA crypto key using a modulus of 1024 bits.

R1(config)# crypto key generate rsa modulus 1024 s seau ani advisim vilanounaini .0

Step 4: Secure the console and VTY lines.

What happened after you falled to login the second tim a. You can set the router to log out of a connection that has been idle for a specified time. If a network administrator was logged into a networking device and was suddenly called away, this command automatically logs the user out after the specified time. The following commands cause the line to log out From your console session on the router, issue the show login do after five minutes of inactivity.

bas R1 (config) # line console 0 and w bases saw basemeno algo! works ent woled elements sbroom R1 (config-line) # exec-timeout 5 0w refun and about to in a latter and tent sworks

R1(config-line)# line vty 0 4

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

R1(config-linc)# exit

R1 (config) #

 The following command impedes brute force login attempts. The router blocks login attempts for 30 seconds if someone fails two attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

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

What does the 2 within 120 mean in the above command?

What does the block-for 30 mean in the above command?

Admin 1p@55 for the password. Step 5: Verify that all unused ports are disabled. Step 5: Verify that all unused ports are disabled.

Router ports are disabled by default, but it is always prudent to verify that all unused ports are in an administratively down state. This can be quickly checked by issuing the show ip interface brief command. Any unused ports that are not in an administratively down state should be disabled using the shutdown command in interface configuration mode.

	R1# show ip interface brief	: Enable SSH connections.	Step 3
	Enwedded-Serv_de-EngineU/U unassigned Y	K? Method Status ES NVRAM administratively down down ES NVRAM administratively down down	ocol
not not	Serial0/0/00	Es manual up souled less less estupo Es NVRAM administratively down down	d
Chanle			
	: Verify that your security measures have been	en implemented correctly.	
a.	Use Tera Term to telnet to R1.	Pl(contic) + Line vty 0 4	
	Does R1 accept the Telnet connection? Explain.dae	Ri(Ponfig-line) s transpost input	
NO	, become ne disable	The VTY lines should use the local User of	
b.	Use Tera Term to SSH to R1.	Richnide line; Flogin Rocal	
D.	The same of the sa		
		Generate a RSA crypto key using a modulu	
C.	Intentionally mistype the user and password informatic attempts.		
	What happened after you failed to login the second tin	k: Secure the console and VTY lines.	Step 4
	ction that has been idle for a specified time. If a netword day on 31 Outden W. Old aw. Oth 97 Outden W. Old aw. Oth 97 Outden W. Old aw. Other to to work commands cause the line to	You can set the router to log off of a conne	
	From your console session on the router, issue the sh example below, the show login command was issued shows that the router is in Quiet-Mode. The router will	ow login command to view the login status.	nd
	R1# show login	Biconfig-line) # line vty 0 4	oongo.
	A default login delay of 1 second is ap	el contlociono e exectimeo,bello	
	No Quiet-Mode access list has been conf	igured. sixe #(mil-pffmee)ff	
onrposs 0	Router enabled to watch for login Attac If more than 2 login failures occur in logins will be disabled for 30 seconds.	ks.	
	Router presently in Quiet-Mode.	Higgorial login block for 30 a	
	Will remain in Quiet-Mode for 1140 seconds		
	Denying logins from all sources.	Schlere Schooling S	
	R1#	What does the block-for 30 mean in the al	
e.	After the 30 seconds has expired, SSH to R1 again an Admin1p@55 for the password.	d login using the SSHadmin username and	
	After you successfully logged in, what was displayed?	The and amply land die shot	Step t
f.	Enter privileged EXEC mode and use Enablep@55 fo	r the password, and isolate all and at a real	o Cl
nand. Vn	If you mistype this password, are you disconnected fro within 120 seconds? Explain	m your SSH session after two failed attempt	S B
	180 because it was	minished in interface configuration mode.	
	enabled/conf	igured that	

g. Issue the show running-config command at the privileged EXEC prompt to view the security settings you have applied. Switch ports are enabled, by default. Shut down all ports that are not in use on the switch

Part 3: Configure Basic Security Measures on the Switch and Athen Associated as the Switch as

Step 1: Encrypt the clear text passwords.

S1(config) # service password-encryption

Step 2: Strengthen Passwords on the switch.

Change the privileged EXEC encrypted password to meet strong password guidelines.

```
S1(config) # enable secret Enablep@55
```

Note: The security password min-length command is not available on the 2960 switch.

Step 3: Enable SSH Connections.

a. Assign the domain-name as CCNA-lab.com

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

b. Create a local user database entry for use when connecting to the switch via SSH. The password should meet strong password standards, and the user should have user EXEC access. If privilege level is not specified in the command, the user will have user EXEC (level 1) access by default.

```
S1 (config) # username SSHadmin privilege 1 secret Admin1p@55
```

c. Configure the transport input for the VTY lines to allow SSH connections but not allow Telnet connections.

```
S1(config) # line vty 0 15
S1(config-line) # transport input ssh
```

d. The VTY lines should use the local user database for authentication.

```
S1(config-line) # login local
S1(config-line) # exit
```

e. Generate an RSA crypto key using a modulus of 1024 bits.

```
S1(config) # crypto key generate rsa modulus 1024
```

Step 4: Secure the console and VTY lines.

a. Configure the switch to log out a line that has been idle for 10 minutes.

```
S1(config) # line console 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)#
```

b. To impede brute force login attempts, configure the switch to block login access for 30 seconds if there are 2 failed attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

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

Step 5: Verify all unused ports are disabled. I and to be proposed and an exact

Switch ports are enabled, by default. Shut down all ports that are not in use on the switch.

a. You can verify the switch port status using the show ip interface brief command.

```
S1# show ip interface brief
                                                                                                      Step 1: Encrypt the clear text passwords ?NO Step 1: Step 1: Step 2: Step 2: Step 2: Step 3: S
               Interface
                                                                   P-Address
              Vlan1
                                                                   192. 68.1.11 no YFS/manual upwessq solving
                                                                                                                                                                     up
              FastEthernet0/1
                                                                  unassioned
                                                                                                      YES unset down
                                                                                                                                                                                down
              FastEthernet0/2
                                                                                                      Step 2: Shwapathen Passwords (nwabe seinuleav
                                                                  unassigned
              FastEthernet0/3
                                                                  unassigned
                                                                                                      YES unset
                                                                                                                              down
                                                                                                                                                                               Change awob
              FastEthernet0/4
                                                                  unassigned
                                                                                                      YES unset
                                                                                                                              down
                                                                                                                                                                                down
              FastEthernet0/5
                                                                                                     YFS unset up eldere
                                                                  unassioned
                                                                                                                                                                                up
              FastFithernet0/62 0882 arunassigned a lon
                                                                                                   Note: The queutly password min-lequit teams 23%s
              FastEthernet0/7
                                                                  unassigned
                                                                                                     YES unset down
                                                                                                                                                                                down
             FastEthernet0/8
                                                                                                     Step 3: Enword SSH Connections wob rearr SEY
                                                                 unassigned
              FastEthernet0/9
                                                                 unassigned
                                                                                                     YES unset down
                                                                                                                                                                               down and
              FastEthernet0/10
                                                                 unassigned
                                                                                                     YES unset down
                                                                                                                                                                               down
             FastEthernet3/11
                                                                 unassigned
                                                                                                     YFS unset
                                                                                                                             down
                                                                                                                                                                               down
blunda FastEthernet0/12 siv
                                                                Unassigned penno YES runset rodowne emwobst assulated wheel D
     ion FastEthernet0/13 80
                                                                 unassigneded blue YES unset bidown sonate blowering pridown lem
             FastEthernet0/14
                                                                 unassigned 0
                                                                                                    Sperment in the command, the moon and make my services
             FastEthernet0/15
                                                                unassigned
                                                                                                  DEYESvensetridown88 emanieau
             FastEthernet0/16
                                                                                                    YES unset down to much hopensy ent
                                                                unassigned
                                                                                                                                                                               down
             FastEthernet0/17
                                                                unassigned
                                                                                                    YFS unset
                                                                                                                            down
                                                                                                                                                                              down
             FastEthernet0/18
                                                                unassigned
                                                                                                    YES unset
                                                                                                                            down
                                                                                                                                                                               down
            FastEthernet0/19
                                                                unassigned
                                                                                                    YES unset
                                                                                                                             down
                                                                                                                                                                              down
            FastEthernet0/20
                                                                unassigned
                                                                                                    YES unset
                                                                                                                            down
            FastEthernet0/21
                                                                unassidnedly
                                                                                                   YES unsets a down and oak phiods soul down out?
            FastEthernet0/22
                                                                unassigned
                                                                                                    YES unset down
            FastEthernet0/23
                                                                unassigned
                                                                                                    YES unset
                                                                                                                            down
                                                                                                                                                                              down
            FastEthernet0/24
                                                                unassigned
                                                                                                    YES unset
                                                                                                                            down
            GigabitEthernet0/1
                                                                                                                            RSA crypto key uslinde
                                                                unassigned
                                                                                                   YES unset
            GigabitEthernet0/2
                                                               unassighedriubo YES unsets down
                                                                                                                                       nwob 114 drypto key
            S1#
```

b. Use the interface range command to shut down multiple interfaces at a time.

```
S1(config)# interface range f0/1-4 0.00/7-24 0.00/1-20 of dalway and amplication of slocation and application of slocation and application of slocation and slocation of sloca
```

5. To impede brute force login attempts, configure the switch to block login access for 30 seconds if there are 2 failed attempts within 120 seconds. This timer is sel especially low for the purpose of this lab.

login block-for 30 attempts 2 within 120

c. Verify that all inactive interfaces have been administratively shut down.

	S1# show ip interfac	a hring		,			-01	013391	
	Interface	IP-Address	00 00	I tot ben	co command was ente		SSWOY	nq.adŤ	1
	Viani	192.168.1.11			Status Boss blows		Proto	col	
	FastEthernet0/1			manual			up		
	FastEthernet0/2	unassigned		unsel	administratively o				
	FastEthernet0/3	unassigned		unset	administratively o				
	TO THE PARTY OF TH	unassigned		unset.	administratively o				
Pr 3 11	FastEthernet0/4	unassigned		unset	administratively o	iown	down		
	FastEthernet0/5	unassigned	YES	unset	up		up _c		
	FastEthernet0/6	unassigned	YES	unset	up		up		
	FastEthernet0/7	unassigned	YES	unsel	administratively d	lown	down		
	FastEthernet0/8	unassigned	YES	unset	administratively d				
	FastEthernet0/9	unassigned	YES	unset	administratively d				
	FastEthernet0/10	unassigned	YES	unset	administratively d			il setti	10.59
	FastEthernet0/11	unassigned	YES	unset	administratively d				-0.0
	FastEthernot0/12	unassigned nu2 o	YES	unset	administratively d				
	FastEthernet0/13	unassigned		unseL	administratively d				
ace #2	FastEthernet0/14 sonling			unset	administratively d				Ros
	FastEthernet0/15	unassigned		unset	administratively d				14/21
	FastEthernet0/160 03) 0	unassigned		unset	administratively d				
	FastEthernet0/17	unassigned		unset					
	FastFthernet0/18nmp	unassigned			administratively d				
	FastEthernet0/19	unassigned		unset	administratively d				
	FastEthernet0/20			unset	administratively d				
	rastEthernet0/21	unassigned		unset	administratively d				280
	FastEthernet0/22	unassigned		unset	administratively d				
		unassigned		unset	administratively d				
	FastFthernet0/23 08 0	unassigned		unset	administratively d	own	down		185
	FastEthernet0/24	unassigned		unset	administratively d				
	SigabitEthernet0/108) (unassigned	YES	unset	administratively d	own	down		
	SigabitEthernet0/2	unassigned	YES	unset	administratively de	own	down		
many	#12 the type of router and how	nierfaces for dentity							

Step 6: Verify that your security measures have been implemented correctly.

- a. Verify that Telnet has been disabled on the switch.
- b. SSH to the switch and intentionally mistype the user and password information to see if login access is blocked.
- c. After the 30 seconds has expired, SSH to S1 again and log in using the SSHadmin username and Admin1p@55 for the password.

Did the banner appear after you successfully logged in?

- d. Enter privileged EXEC mode using Enablep@55 as the password.
- e. Issue the show running-config command at the privileged EXEC prompt to view the security settings you have applied.

Reflection

The password cisco command was entered for the console and VTY lines in your basic configuration in Part
 When is this password used after the best practice security measures have been applied?

the password any longer

2. Are preconfigured passwords shorter than 10 characters affected by the security passwords min-length 10 command?

No, only passwords

the command u

Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/0/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

After the 30 seconds has expired, SSH to S1 again and log in using the SSHadmin username and Admin1p@55 for the password

Did the banner appear after you successfully logged an?

Enter privileged EXEC mode using Enablep@55 as the password

Issue the show running-config command at the provileged EXEC prompt to view the security settings
vou have scalled.