Continue

Show startup-config Which information does the show startup-config command display?Show startup-config shows the router or switch complete configuration saved on the nonvolatile RAM, Information present on the non-volatile RAM is saved even after the device restarts so this configuration is present at the time of the device start-up.Show start-up config is one of the most common commands by the network administrators as it shows all the config that is useful while checking the device and checking what is configured on the device.This command can be used for troubleshooting, whenever there is an issue with the device we can copy the complete configuration and flash that on the new device. The new device can be configured instantly using this command so its a best practice to always have a backup of the start-up config.In case of hardware failure, we can quickly use the saved startup-config and configure the new device same as the old one in a few minutes.We can also delete the start-up config however once deleted, we cannot retrieve the configuration so backing up the config is highly important on the production network or high-traffic network.The startup-config file is very small in size so backing up the config does not take much space. It is just a text file with configuration data.By default, on a new Cisco device, thestart-up config is not present so we have to save the startup-config on the new device then only it will show up when we will use the command show startup-config.To save the running config, we can use the command write and to delete it we can use the command write eraseBelow is the output of the show running-config commandRouter#show startup-configUsing 608 bytes!version 15.1no service timestamps logdatetimemsecno service timestamps debugdatetimemsecno service password-encryption!hostname Router!!!!!!!!ip cefno ipv6 cef!!!!license udi pid CISCO1941/K9 sn FTX1524P93Q-!!!!!!!!!!!spanning-tree mode pvst!!!!!!interface GigabitEthernet0/0no ip addressduplex autospeed autoshutdown!interface GigabitEthernet0/1no ip addressduplex autospeed autoshutdown!interface Vlan1no ip addressshutdown!ip classless!ip flow-export version 9!!!!!!!line con 0!line aux 0!linevty0 4login!!!EndThe above output is from the new router, we can see that nothing much is configured on the router however, after configuring the router and saving the startup-config, we will see the configuration in the startup-config.We can use the pipe symbol to filter out the configuration that we want to seeFor example, if we want to see the VTY line configuration, we can use the pipe symbol to check the VTY lines.Show startup-config | beginvtyWe can use this command to check any specific configuration present on the device. 2.5.5 Packet Tracer Configure Initial Switch Settings Part 1: Verify the Default Switch ConfigurationPart 2: Configure a Basic Switch Configuration Part 3: Configure a MOTD BannerPart 4: Save Configuration Files to NVRAMPart 5: Configure In this activity, you will perform basic switch configurations. You will secure access to the command-line interface (CLI) and console ports using encrypted and plain text passwords. You will also learn how to configure messages for users logging into the switch. These banners are also used to warn unauthorized users that access is prohibited. You can access all switch commands from privileged mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use.The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the configure command through which access to the remaining command modes are gained.a. Click S1 and then the CLI tab. Press Enterb. Enter privileged EXEC mode by entering the enable command:Switch> enableSwitch#Notice that the prompt changed in the configuration to reflect privileged EXEC mode. a. Enter the show running-config command.Switch# show running-configb. Answer the following questions:How many FastEthernet interfaces does the switch have? 24 How many Gigabit Ethernet interfaces does the switch have?2What is the range of values shown for the vty lines? 0 -15 Which command will display the current contents of non-volatile random-access memory (NVRAM)?show startup-configuration Why does the switch respond with startup-config is not present? It displays this message because the configuration file was not saved to NVRAM. Currently it is only located in RAM. To configure parameters on a switch, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the switch.Switch# configure terminalSwitch(config)# hostname S1S1(config)# exitS1# To secure access to the console line, access config-line mode and set the console password to letmein.S1# configure terminalEnter configuration commands, one per line. End with CNTL/Z.S1(config)# line console 0S1(config-line)# password letmeinS1(config-line)# loginS1(config-line)# exitS1(config)# exit%SYS-5-CONFIG_I: Configured from console by consoleS1#Why is the login command required?In order for the password checking process to work, it requires both thelogin and password commands Exit privileged mode to verify that the console port password is in effect.S1# exitSwitch con0 is now availablePress RETURN to get started.User Access VerificationPassword:S1>Note: If the switch did not prompt you for a password, then you did not configure the login parameter in Step 2. Set the enable password to c1$c0. This password protects access to privileged mode.Note: The 0 in c1$c0 is a zero, not a capital O. This password will not grade as correct until after you encrypt it in Step 8.S1> enableS1# configure terminalS1(config)# enable password c1$c0S1(config)# exit%SYS-5-CONFIG_I: Configured from console by consoleS1# a. Enter the exit command again to log out of the switch.b. Press and you will now be asked for a password:User Access VerificationPassword:c. The first password is the console password you configured for line con 0. Enter this password to return to user EXEC mode.d. Enter the command to access privileged mode.e. Enter the second password you configured to protect privileged EXEC mode.f. Verify your configurations by examining the contents of the running-configuration file:S1# show running-configurationNotice how the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder. The enable password should be replaced with the newer encrypted secret password using the enable secret command. Set the enable secret password to itsasecret.S1# config tS1(config)# enable secret itsasecretS1(config)# exitS1#Note: The enable secret password overrides the enable password. If both are configured on the switch, you must enter the enable secret password to enter privileged EXEC mode. a. Enter the show running-configuration command again to verify the new enable secret password is configured. Note: You can abbreviate show running-configuration asS1# show runb. What is displayed for the enable secret password? 1mERr$ILwq/b7kc.7X/ejA4Aosn0 c. Why is the enable secret password displayed differently from what we configured?The enable secret is shown in encrypted form, whereas the enable password is in plain text. As you noticed in Step 7, the enable secret password was encrypted, but the enable and console passwords were still in plain text. We will now encrypt these plain text passwords using the service password-encryption command.S1# config tS1(config)# service password-encryptionS1(config)# exitIf you configure any more passwords on the switch, will they be displayed in the configuration file as plain text or in encrypted form? Explain why?The service password-encryption command encrypts all current and future passwords. The Cisco IOS command set includes a feature that allows you to configure messages that anyone logging onto the switch sees. These messages are called message of the day, or MOTD banners. Enclose the banner text in quotations or use a delimiter different from any character appearing in the MOTD string.S1# config tS1(config)# banner motd "This is a secure system. Authorized Access Only!"S1(config)# exit%SYS-5-CONFIG_I: Configured from console by consoleS1#When will this banner be displayed? The message will be displayed when someone enters the switch through the console port. Why should every switch have a MOTD banner? Every switch should have a banner to warn unauthorized users that access is prohibited but can also be used for sending messages to network personnel/technicians (such as impending system shutdowns or who to contact for access) You have completed the basic configuration of the switch. Now back up the running configuration file to NVRAM to ensure that the changes made are not lost if the system is rebooted or loses power.S1# copy running-config startup-configDestination filename [startup-config]?[Enter]Building configuration...[OK]What is the shortest, abbreviated version of the copy running-config startup-config command? cop r s Which command will display the contents of NVRAM? show startup-config Are all the changes that were entered recorded in the file? Yes, it is the same as the running configuration. You have completed the configuration on S1. You will now configure S2. If you cannot remember the commands, refer to Parts 1 to 4 for assistance.Configure S2 with the following parameters:a. Name device: S2b. Protect access to the console using the letmein password.c. Configure an enable password of c1$c0 and an enable secret password of itsasecret.d. Configure a message to those logging into the switch with the following message:Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.e. Encrypt all plain text passwords.f. Ensure that the configuration is correct.g. Save the configuration file to avoid loss if the switch is powered down.Switch> enableSwitch# config tEnter configuration commands, one per line. End with CNTL/Z.Switch(config)# hostname S2S2(config)# line console 0S2(config-line)# password letmeinS2(config-line)# loginS2(config-line)# enable password c1$c0S2(config)# enable secret itsasecretS2(config)# banner motd $any text here$S2(config)# service password-encryptionS2(config)# do copy running-config startup-config Switch 1 S1enableconfigure terminalhostname S1line console 0password letmeinloginenable password c1$c0enable secret itsasecretservice password-encryptionbanner motd #This is a secure system. Authorized Access Only!#endcopy running-config startup-configSwitch 2 S2enableconfigure terminalhostname S2line console 0password letmeinloginenable password c1$c0enable secret itsasecretservice password-encryptionbanner motd #Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.#endcopy running-config startup-config Next Lab 2.7.6 Packet Tracer Implement Basic ConnectivityYour phone rings; it is not the news you want to hear.The network is down, and it is your job to fix it.What Youll LearnHow to investigate config register-related issuesHow to solve config register-related issuesHow to verify the network is back upWhat Youll NeedCisco Packet TracerInitial Packet Tracer Lab FileFirst, load the Packet Tracer file that has the initial topology.The network that we need to fix has three routers:After a power outage, the network has stopped working. All three of these routers have problems that we need to fix.Important: To simulate the power outage, click the Power Cycle Devices button in Packet Tracer in the bottom left-hand corner.After the devices reboot, you will then see the problems in the network. The goal is to fix all the issues and restore the configurations so that the routers can ping all loopbacks. You need to restore the configurations, without configuring the network.Router R3 Initial InvestigationAfter power cycling the routers, look at the CLI for R3; you will notice it has the error message no valid BOOT image found. It then attempts to boot from the default boot device. We then get the error that test.bin is not accessible and cannot be loaded.For some reason, the router R3 is trying to load test.bin and fails. It then tries to boot from the default boot device, which bootsthe isr4300-...SPA.bin operating system, and then the router boots up.Why is the router trying to boot from the test.bin boot file and defaulting to another one?Router R2 Initial InvestigationRouter R2 is in ROMMON mode, which is a major issue. If you look at the prompt for the device, it says rommon 1. There are only a few options in ROMMON mode. Because the router has not booted from a valid operating system, it defaulted to ROMMON.If we look at the topology, all the interfaces are down, which is a big problem.Router R1 Initial InvestigationRouter R1 prompts to enter the initial configuration dialogue. If you say no and enter into the routers CLI, the routers name is now simply Router instead of R1, and the show running-configuration has nothing but the default configuration of a new installation. The interfaces have no IP address and are shut down.Can you fix the network without configuring anything, but just restoring what is already there?We are now going to walk through how to fix the issues on router R1. When we rebooted the devices, R1 did not boot correctly. It ends up in the initial configuration dialogue with no configuration.Start by answering no to the initial configuration dialogue. We want the router to boot with the correct configuration.Enter enable mode and check the running configuration with a show run command. We can see the router has a default configuration and no routing protocol.Issue a show version command on R1; note that the system image file is fine. Hit the space bar a few more times to see at the bottom of the output that the configuration register of the router is 0x2142. That is a problem. Lets see why:There are a lot of documents on the Cisco website, such as Understand Configuration Register Usage on all Routers. This will help us understand why, because you will see the sample output for show version, and the output says configuration register is 0x2102 is the hexadecimal location we want for a normal router. Our router has it set to 0x2142.0x means a hexadecimal number. In binary, 0x2142 is 0010 0001 0100 0010 (2 = 0010, 1 = 0001, 4 = 0100, 2 = 0010).This document tells us the configuration register numbers that should be expected. There are several other normal hexadecimal locations that the router could expect. Each one has various features to provide, such as console baud rates or what kind of boot to do. Ours is currently set to 0x2142, which the document says ignores the contents of NVRAM (ignoring configuration).Issue a show startup-config command and compare the size of bytes (768 bytes) to the show running-configuration (564 bytes). The startup configuration has the original configuration that we need to restore the device to be fixed. You can review the configuration to verify it, but it is much larger, with the interface configuration, hostname R1, and EIGRP running.Because the configuration register is incorrect, it is not loading the correct configuration, ignoring the NVRAM configuration (startup configuration), and boots as if it is a brand-new router. Using 0x2142 is useful if you need to do password recovery because you are able to boot in to the device and ignore that startup configuration. In this case, we do not need to do password recovery, so we want to set it back to 0x2102 to boot normally.Enter configuration mode with conf t, and configure config-register 0x2102 and end.Verify the config register is updated by issuing show version again and looking at the bottom of the output. It should update at the next reload.Reload the device with the reload command, but do not answer yes (as you usually do) to saving the configuration before the reload. We want to replace the running config with the startup config in this case. Configuration registers are stored in a separate location, so you do not need to save before reloading; it will load from the new config register on reload.After the reload, you can verify that the configuration is there (password is cisco). If you issue a show ip interface brief command to verify, you will see the interfaces are UP / DOWN. That is because we have not restored the other routers yet.When the router R2 rebooted, it entered ROMMON mode. Lets see what that looks like.Use the ? to see the commands available.Note that every time you type a command, the number next to the ROMMON prompt will increment by one. We have a command called confreg to help set the configuration register and reset to reboot the router.Note: After the reload, check the topology and see the interfaces go green and a new EIGRP adjacency on R2.Enter enable mode in R2, and issue a show ip interface brief command to check the status of the network. Notice that the interfaces are UP (for the device that has been fixed on the other side). Issue a show ip eigrp neighbor to see the neighbor relationships coming up with R1.Test the connection to R1 by issuing a ping to the loopback of R1 with ping 1.1.1.1. The ping should be successful at this point.To simulate the problem we just saw, you can configure config-register 0x2100 to have the router boot in to ROMMON mode (after a reload and without saving the configuration).Logging in to router R3 has the correct name at the prompt, but there is no password, which is incorrect.Issue a show ip interface brief and see that all the interfaces are down (ADMIN DOWN / DOWN) and there are no IP addresses assigned. Also, issue a show ip protocol and see that there are no routing protocols enabled on the router.Note: If you remember from our initial troubleshooting, R3 was trying to load test.bin as the operating system image and failed.Lets look at the boot images in storage with a show flash command. There is an isr4300...SPA.bin file in flash memory and no test.bin file. Trying to get the router to boot from test.bin will not work because there is no file with that name in storage.The router was able to boot because once it failed booting, it did a final autoboot attempt from default boot device. It looked for the first file in flash and was able to boot from it, so the router came up.Look at the configuration with show run, and note the config has only one boot statement with boot system flash test.bin.Look at the show startup-config output interface configuration. Notice that the configuration for the interfaces have no IP addresses and no routing protocol.First, lets check the config register with the show version command, looking at the end of the output.Note: The config register is set to 0x2101, which is a config register used in the old days, booting in to bootstrap mode (a mini-IOS).Look at this old Cisco 2500 Series Router. It has asynchronous ports on the left to connect to the consoles of multiple devices (as a terminal server), and there are two serial interfaces on the right. This old device would have a bootstrap mode (mini-IOS), but that does not exist on modern routers. The bootstrap mode is irrelevant for this router in Packet Tracer and any modern router.Change the config register by issuing the conf t and config-register 0x2102 commands. Reload the router to change the config register location. Do not save the changes to the boot location we fixed earlier; we will need to fix them a different way.Remember that to solve the issues, we are not allowed to make any configuration changes to the device, so simply configuring the interfaces is not an option in this scenario.Issue a show flash command and note that the flash storage has a file called live-config. This might be a backup configuration we could use. Lets look at what is inside, using the more flash:live-config command to read the contents of the file. Note that the config has the incorrect boot statement but does have the EIGRP and interface configuration.To restore the configuration, issue at enable level copy flash running-config. The CLI will prompt you for a filename; we will use the filename live-config that we saw in the flash storage. The destination is the running config. Now we will see the interfaces come up and the routing come up.Issue a show ip interface brief command to verify that the interfaces and IP addresses are up. Also, issue a show ip protocol to see the EIGRP info. A show run still has the incorrect boot statement, but everything else is there.When you restore configuration like we did here, interfaces are shut down. So we will need to enable those interfaces.Turn the interfaces back up by entering the following commands (to bring the interface and EIGRP up):conf tint gig 0/0/0no shutdown .Verify that we can ping the loopback of routers R1 and R2 with ping 1.1.1.1 and ping 2.2.2.2 at enable mode.Remove the bad boot statement with the conf t and no boot system flash test.bin commands. Verify that it is gone with a show run. Make sure to update the startup-config by issuing a copy running-config startup-config, and reload the router.Power-cycle all the devices using the button on the bottom left to verify that everything is fixed. The network will go down, but they should come back up after the reload with our fixes.The fixed topology file is here.Congrats! Please continue your learning through our communitys many other resources, helping folks get started on their CCNA journey.Training ResourcesCCNA E-LearningCCNA Study MaterialsCCNA Exam TopicsMore From David Bombal Share copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt remix, transform, and build upon the material for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms. Attribution You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. No additional restrictions You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits. You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation . No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material. In this packet tracer lab, We will back up and restore the files using the following commands.copy running-config tftpcopy startup-config tftpcopy flash tftpcopy tftp flashFirst of all, we will configure the TFTP server in the packet tracer that we are using to transfer the files. DownloadFTP and TFTP servers provide file transferability so using this server, we can back up and restore various files between end devices like PC to PC and we can also use these servers to back and restore running-config, startup-config, and Cisco IOS.It is always a good practice to save the Cisco device configuration and IOS to the external server so, in the case of hardware failure; we can easily restore the configuration and reduce the significant downtime.Configuring TFTP and FTP servers in packet tracer is fairly easy. In this lab, we will configure the TFTP server however FTP server can also be configured in the same way.Step 1We have to attach the server endpoint in our network, packet tracer has provided us with many endpoint devices and one of them is the server, this server provides many services including FTP and TFTP.Step2Assign an IP address to the server, the IP address should be of the reachable network; test the connectivity to the server via ping command.Step3Make sure that the TFTP service is running, although it is enabled by default however we can double-check it for confirmation.That is all required to configure the server, now we will save running-config, startup-config, and IOS to the TFTP server.If we want to backup and restore the switchs files then we have to configure VLAN 1 interface with an IP address.We have to use the following commandsUse copy running-config tftp to backup running-configSwitch#copy running-config tftp:Address or name of remote host []? 192.168.1.5Destination filename [Switch-confg]? Test-config-1Once we have entered the command then the device will ask for the IP address of the server so we have to enter the IP address then press enter, and then the device will ask us to provide the destination file name, if we press enter without writing anything then the file will be saved with name Switch-config. However, we have given the file name Test-config-1 here so the file will be saved with this name.Use copy startup-config tftp to backup startup-configPlease note, to export startup-config, please make sure that startup-config is present on the router, and if not then please first save the startup-config.We have to use the following command.Switch#copy startup-config tftp:Address or name of remote host []? 192.168.1.5Destination filename [Switch-confg]? Test-config-2We have saved the startup-config file with the Test-config-2 name. Some of the newer Cisco devices also have USB ports that allow the backup of the Cisco IOS to USB storage however copying the IOS on the server is the best practice as servers are more stable and are configured with redundant storage.Use copy flash tftp to backup the IOSSwitch#copy flash: tftp:Source filename []? 2960-lanbasek9-mz.150-2.SE4.binAddress or name of remote host []? 192.168.1.5Destination filename [2960-lanbasek9-mz.150-2.SE4.bin]? (press enter)IOS of the Cisco device is stored in Flash so we have to copy from flash to the TFTP server. While backing up the IOS, we have to use the exact IOS name so we should copy the IOS name instead of typing it as you can see that IOS names are not easy to type.We can use the command show flash to find out and copy the name of the IOS.We have not given the destination name here and just used the default IOS name because the IOS name provides information about the IOS version so we should keep the name as default.After successfully transferring the file to the TFTP server, we will see the ok message on the Cisco device terminal as well.After the successful backup, we should be able to see the files in the TFTP server. You can see that all backed-up files are available on the TFTP server.To restore the files from the TFTP server, we just have to change the command a bit. We can restore using the copy tftp flash command in the following format.Switch#copy tftp: flash:Source filename []? 2960-lanbasek9-mz.150-2.SE4.binAddress or name of remote host []? 192.168.1.5Destination filename [2960-lanbasek9-mz.150-2.SE4.bin]? (press enter)Please note, while saving the running and startup-config, we have given them a different name in this lab however while copying it to a Cisco device, we must give them the default name as running-config and startup-config as a Cisco device only looks for these names while saving and loading configuration so if we will change the name then the device is not going to recognize it. This message is displayed, when the copy start tftp command is issued to backup the configuration files.In some cases, when the show startup-config command is issued, the %% Non-volatile configuration memory is not present was outputed error message is observed.ResolutionThe workaround is to issue a write memory command before you back up the configuration, in order to make sure the configuration is saved in non-volatile RAM (NVRAM). Aug 30, 2020 Last Updated: May 14, 2023 CCNA v7 Course #1 Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. 10.1.4 Packet Tracer Configure Initial Router Settings10.1.4 Packet Tracer Configure Initial Router Settings Part 1: Verify the Default Router ConfigurationPart 2: Configure and Verify the Initial Router ConfigurationPart 3: Save the Running Configuration File In this activity, you will perform basic router configurations. You will secure access to the CLI and console port using encrypted and plain text passwords. You will also configure messages for users logging into the router. These banners also warn unauthorized users that access is prohibited. Finally, you will verify and save your running configuration. a. Choose a Console cable from the available connections.b. Click PCA and select RS 232.c. Click R1 and select Console.d. Click PCA > Desktop tab > Terminal.e. Click OK and press ENTER. You are now able to configure R1. You can access all the router commands from privileged EXEC mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use.a. Enter privileged EXEC mode by entering the enable command.Router> enable Router#Notice that the prompt changed in the configuration to reflect privileged EXEC mode.b. Enter the show running-config command:Router# show running-configc. Answer the following questions:What is the routers hostname? RouterHow many Fast Ethernet interfaces does the Router have? 4How many Gigabit Ethernet interfaces does the Router have? 2How many Serial interfaces does the router have? 2What is the range of values shown for the vty lines? 0 4d. Display the current contents of NVRAM.Router# show startup-configstartup-config is not presentWhy does the router respond with the startup-config is not present message? It displays this message because the configuration file was not saved to NVRAM. Currently it is only located in RAM. To configure parameters on a router, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the router. Note: If you have difficulty remembering the commands, refer to the content for this topic. The commands are the same as you configured on a switch.a. Configure R1 as the hostname.b. Configure Message of the day text: Unauthorized access is strictly prohibited.c. Encrypt all plain text passwords.Use the following passwords:1) Privileged EXEC, unencrypted: cisco2) Privileged EXEC, encrypted: itsasecret3) Console: letmein a. Verify the initial settings by viewing the configuration for R1.What command do you use?show running-configb. Exit the current console session until you see the following message:R1 con0 is now availablePress RETURN to get started.c. Press ENTER; you should see the following message:Unauthorized access is strictly prohibited.User Access VerificationPassword:Why should every router have a message-of-the-day (MOTD) banner?Every router should have a banner to warn unauthorized users that access is prohibited. MOTD Banners can also be used to send messages to network personnel (such as impending system shutdowns or who to contact for access). If you are not prompted for a password before reaching the user EXEC prompt, what console line command did you forget to configure?R1(config-line)# logind. Enter the passwords necessary to return to privileged EXEC mode.Why would the enable secret password allow access to the privileged EXEC mode and the enable password no longer be valid?The enable secret password overrides the enable password. If both are configured on the router, you must enter the enable secret password to enter privileged EXEC mode.If you configure any more passwords on the router, are they displayed in the configuration file as plain text or in encrypted form? Explain.The service password-encryption command encrypts all current and future passwords. a. You have configured the initial settings for R1. Now back up the running configuration file to NVRAM to ensure that the changes made are not lost if the system is rebooted or loses power.What command did you enter to save the configuration to NVRAM? copy running-config startup-configWhat is the shortest, unambiguous version of this command? copy r sInstructor Note: This can vary by platform and IOS version. Which command displays the contents of the NVRAM? show startup-configuration or show startb. Verify that all of the parameters configured are recorded. If not, analyze the output and determine which commands were not done or were entered incorrectly. You can also click Check Results in the instruction window. Although you will be learning more about managing the flash storage in a router in later chapters, you may be interested to know now that , as an added backup procedure , you can save your startup configuration file to flash. By default, the router still loads the startup configuration from NVRAM, but if NVRAM becomes corrupt, you can restore the startup configuration by copying it over from flash.Complete the following steps to save the startup configuration to flash.a. Examine the contents of flash using the show flash command:R1# show flashHow many files are currently stored in flash? 3Which of these files would you guess is the IOS image?c1900-universalk9-mz.SPA.151-4.M4.binWhy do you think this file is the IOS image? Answers may vary, but two clues are the file length compared to the others and the .bin at the end of the file name.b. Save the startup configuration file to flash using the following commands:R1# copy startup-config flashDestination filename [startup-config]The router prompts to store the file in flash using the name in brackets. If the answer is yes, then press ENTER; if not, type an appropriate name and press ENTER.c. Use the show flash command to verify the startup configuration file is now stored in flash. enableconfigure terminalhostname R1line console 0password letmeinloginexitenable password ciscoenable secret itsasecretservice password-encryptionbanner motd $Unauthorized access is strictly prohibited.$exitcopy running-config startup-configcopy startup-config flash: Previous Lab9.3.4 Packet Tracer IPv6 Neighbor DiscoveryNext Lab 10.3.4 Packet Tracer Connect a Router to a LAN Oct 26, 2020 Last Updated: May 15, 2023 CCNA 2 Labs - Packet Tracer Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice. 2.2.3.4 Packet Tracer Configuring Initial Switch Settings Part 1: Verify the Default Switch Configuration Part 2: Configure a Basic Switch ConfigurationPart 3: Configure a MOTD BannerPart 4: Save Configuration Files to NVRAMPart 5: Configure S2 In this activity, you will perform basic switch configurations. You will secure access to the command-line interface (CLI) and console ports using encrypted and plain text passwords. You will also learn how to configure messages for users logging into the switch. These banners are also used to warn unauthorized users that access is prohibited. You can access all switch commands from privileged mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use.The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the configure command through which access to the remaining command modes are gained.a. Click S1 and then the CLI tab. Press Enterb. Enter privileged EXEC mode by entering the enable command:Switch> enableSwitch#Notice that the prompt changed in the configuration to reflect privileged EXEC mode. a. Enter the show running-config command.Switch# show running-configb. Answer the following questions:1) How many FastEthernet interfaces does the switch have? 2) How many Gigabit Ethernet interfaces does the switch have?3) What is the range of values shown for the vty lines?4) Which command will display the current contents of non-volatile random-access memory (NVRAM)?show startup-configuration5) Why does the switch respond with startup-config is not present?It displays this message because the configuration file was not saved to NVRAM. Currently it is only located in RAM. To configure parameters on a switch, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the switch.Switch# configure terminalSwitch(config)# hostname S1S1(config)# exitS1# To secure access to the console line, access config-line mode and set the console password to letmein.S1# configure terminalEnter configuration commands, one per line. End with CNTL/Z.S1(config)# line console 0S1(config-line)# password letmeinS1(config-line)# loginS1(config-line)# exitS1(config)# exit%SYS-5-CONFIG_I: Configured from console by consoleS1#Why is the login command required?In order for the password checking process to work, it requires both the login and password commands. Exit privileged mode to verify that the console port password is in effect.S1# exitSwitch con0 is now availablePress RETURN to get started.User Access VerificationPassword:S1>Note: If the switch did not prompt you for a password, then you did not configure the login parameter in Step 2. Set the enable password to c1$c0. This password protects access to privileged mode.Note: The 0 in c1$c0 is a zero, not a capital O. This password will not grade as correct until after you encrypt it in Step 8.S1> enableS1# configure terminalS1(config)# enable password c1$c0S1(config)# exit%SYS-5-CONFIG_I: Configured from console by consoleS1# a. Enter the exit command again to log out of the switch.b. Press and you will now be asked for a password:User Access VerificationPassword:c. The first password is the console password you configured for line con 0. Enter this password to return to user EXEC mode.d. Enter the command to access privileged mode.e. Enter the second password you configured to protect privileged EXEC mode.f. Verify your configurations by examining the contents of the running-configuration file:S1# show running-configurationNotice how the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder. The enable password should be replaced with the newer encrypted secret password using the enable secret command. Set the enable secret password to itsasecret. S1# config tS1(config)# enable secret itsasecretS1(config)# exitS1#Note: The enable secret password overrides the enable password. If both are configured on the switch, you must enter the enable secret password to enter privileged EXEC mode. a. Enter the show running-configuration command again to verify the new enable secret password is configured.Note: You can abbreviate show running-configuration asS1# show runb. What is displayed for the enable secret password?1mERr$ILwq/b7kc.7X/ejA4Aosn0c. Why is the enable secret password displayed differently from what we configured?The enable secret is shown in encrypted form, whereas the enable password is in plain text. As you noticed in Step 7, the enable secret password was encrypted, but the enable and console passwords were still in plain text. We will now encrypt these plain text passwords using the service password-encryption command.S1# config tS1(config)# service password-encryptionS1(config)# exitIf you configure any more passwords on the switch, will they be displayed in the configuration file as plain text or in encrypted form? Explain why?The service password-encryption command encrypts all current and future passwords. The Cisco IOS command set includes a feature that allows you to configure messages that anyone logging onto the switch sees. These messages are called message of the day, or MOTD banners. Enclose the banner text in quotations or use a delimiter different from any character appearing in the MOTD string.S1# config tS1(config)# banner motd "This is a secure system. Authorized Access Only!"S1(config)# exit%SYS-5-CONFIG_I: Configured from console by consoleS1#When will this banner be displayed? The message will be displayed when someone enters the switch through the console port. Why should every switch have a MOTD banner? Every switch should have a banner to warn unauthorized users that access is prohibited but can also be used for sending messages to network personnel/technicians (such as impending system shutdowns or who to contact for access) You have completed the basic configuration of the switch. Now back up the running configuration file to NVRAM to ensure that the changes made are not lost if the system is rebooted or loses power.S1# copy running-config startup-configDestination filename [startup-config]?[Enter]Building configuration...[OK]What is the shortest, abbreviated version of the copy running-config startup-config command? cop r s Which command will display the contents of NVRAM? show startup-config Are all the changes that were entered recorded in the file? Yes, it is the same as the running configuration. You have completed the configuration on S1. You will now configure S2. If you cannot remember the commands, refer to Parts 1 to 4 for assistance.Configure S2 with the following parameters:a. Name device: S2b. Protect access to the console using the letmein password.c. Configure an enable password of c1$c0 and an enable secret password of itsasecret.d. Configure a message to those logging into the switch with the following message:Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.e. Encrypt all plain text passwords.f. Ensure that the configuration is correct.g. Save the configuration file to avoid loss if the switch is powered down.Switch> enableSwitch# config tEnter configuration commands, one per line. End with CNTL/Z.Switch(config)# hostname S2S2(config)# line console 0S2(config-line)# password letmeinS2(config-line)# loginS2(config-line)# enable password c1$c0S2(config)# enable secret itsasecretS2(config)# banner motd $any text here$S2(config)# service password-encryptionS2(config)# do copy running-config startup-config Switch 1 S1enableconfigure terminalhostname S1line console 0password letmeinloginenable password c1$c0enable secret itsasecretservice password-encryptionbanner motd #This is a secure system. Authorized Access Only!#endcopy running-config startup-configSwitch 2 S2enableconfigure terminalhostname S2line console 0password letmeinloginenable password c1$c0enable secret itsasecretservice password-encryptionbanner motd #Authorized access only. Unauthorized access is prohibited and violators will be prosecuted to the full extent of the law.#endcopy running-config startup-config was just wondering if someone would kindly explain to me what config is loaded the first time a router is booted up, or even a swtich for that matter. Im using a packet tracer and whenever i use the commandshow startup-configon a new router or switch i get this responsestartup-config is not presentthanks 0 Share on FacebookShare on Twitter Network simulation softwareThis article relies excessively on references to primary sources. Please improve this article by adding secondary or tertiary sources. Find sources:"Packet Tracer"news newspapers books scholar JSTOR (January 2020) (Learn how and when to remove this message)Packet TracerDeveloper(s)Cisco SystemsStable release8.2.2[1] Operating systemLinux, Android 4.2+, iOS 8+, Microsoft Windows, macOS[2]PlatformWindows, Linux, Android (operating system), iOS, macOS[2]Size305 MB (Linux)265 MB (Windows)856 MB (macOS)Available inEnglishTypeNetwork simulationLicenseProprietaryWebsitewww.netacad.com/courses/packet-tracerPacket Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Cisco Networking Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.[2]Packet Tracer can be run on Linux, Microsoft Windows, macOS. Apps for mobile operating systems like Android[3] and iOS[4] were also available. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a 'cable' item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP, to the extents required by the current CCNA curriculum. As of version 5.3, Packet Tracer also supports the Border Gateway Protocol.[5]In addition to simulating certain aspects of computer networks, Packet Tracer can also be used for collaboration. As of Packet Tracer 5.0, Packet Tracer supports a multi-user system that enables multiple users to connect multiple topologies together over a computer network.[6] Packet Tracer also allows instructors to create activities that students have to complete.[citation needed] Packet Tracer is often used in educational settings as a learning aid.[7][8] Cisco Systems claims that Packet Tracer is useful for network experimentation.[9]Packet Tracer allows students to design complex and large networks, which is often not feasible with physical hardware, due to costs.[7] Packet Tracer is commonly used by NetAcad students, since it is available to download after creating a free account.[10] However, due to functional limitations, it is intended by Cisco to be used only as a learning aid, not a replacement for Cisco routers and switches.[9] The application itself only has a small number of features found within the actual hardware running a current Cisco IOS version. Thus, Packet Tracer is unsuitable for modelling production networks. It has a limited command set, meaning it is not possible to practice all of the IOS commands that might be required.[11] Packet Tracer can be useful for understanding abstract networking concepts, such as the Enhanced Interior Gateway Routing Protocol by animating these elements in a visual form.[7][11] Packet Tracer is also useful in education by providing additional components, including an authoring system, network protocol simulation and improving knowledge an assessment system.[9]In 2019, Cisco registered a new URI scheme with the IANA called "pttp". This protocol is used as part of Packet Tracer 7.2.2 capabilities to transmit data between Packet Tracer and Cisco's CSR routing platform.[12][13] As of mid-2022, little is known about this protocol or its functionality.[citation needed]GNS3^ "Download Cisco Packet Tracer 8.2.2 & GNS3". Retrieved 6 October 2024.^ a b c Michel Bakni; Yudith Cardinale; Luis Moreno (2018). "An Approach to Evaluate Network Simulators: An Experience with Packet Tracer". Revista Venezolana de Computacin. 5 (1): 2936. ISSN2244-7040. S2CID195800949. WikidataQ133866763.^ "Cisco Packet Tracer Mobile". Cisco Systems, Inc. 2017-05-12. Archived from the original on 2017-11-15. Retrieved 2017-11-15.^ "Cisco Packet Tracer Mobile on the App Store". App Store. Archived from the original on 2017-11-15. Retrieved 2017-11-15.^ "Cisco Packet Tracer 5.3" (PDF). Archived from the original (PDF) on 2012-09-14. Retrieved 26 August 2018.^ Andrew Smith (31 August 2011). "Development of a Simulated Internet for Education". Research in Learning Technology. Archived from the original on 2017-08-16.^ a b c Dennis C. Frezzo; John T. Behrens; Robert J. Mislevy. "Simulation-Based Environment for a Community of Instructors: Design Patterns for Learning and Assessment" (PDF). Archived from the original (PDF) on 2017-08-16. Retrieved 26 August 2018.^ Zhang, Yongbin; Liang, Ronghua; Ma, Huiling (2012). "Teaching Innovation in Computer Network Course for Undergraduate Students with Packet Tracer". IERI Procedia. 2: 504510. doi:10.1016/j.ieri.2012.06.124.^ a b c "Cisco Packet Tracer" (PDF). Cisco Networking Academy. Retrieved 26 August 2018.^ "Skills for All Resource Hub". Cisco Networking Academy. Retrieved 2024-09-12.^ a b Expsito, Jess; Trujillo, Valentina; Gamess, Eric (2022 October 2010). Using Visual Educational Tools for the Teaching and Learning of EIGRP (PDF). Proceedings of the World Congress on Engineering and Computer Science 2010 Vol I. CiteSeerX10.1.1.301.4894. ISBN978-988-17012-0-6. Retrieved 27 August 2018.^ Deng, Tony; Hoang, Tuan; Hinkle, Bob; Chen, Mark (24 June 2019). "pttp Resource Identifier Scheme". Internet Assigned Numbers Authority. Retrieved 24 May 2022.^