|  |  |
| --- | --- |
| **DOCUMENT RULES:** | |
| **Task Number / Name:** | **Task / CISCO SWITCH SF300** |
| **Group name:** | **696.21ES** |
| **Student name and surname:** | **Perviz Ceferov** |
| **E-mail:** | **Ceferovperviz5757@gmail.com** |
| **WhatsApp number:** | **+994 51-530-80-70** |

|  |  |  |
| --- | --- | --- |
| **#** | **Task names** | **Command steps and outputs** |
| **1** | Name:  Model: | SF300-24P  SF300-24P - Cisco Small Business 300 Series Managed Switches |
| **2** | Detail: | 24 10/100 PoE ports with 180W power budget, 2 10/100/1000 ports - 2 combo mini-GBIC ports |
| **3** | Ports | 24 x 10/100 + 2 x combo Gigabit SFP + 2 x 10/100/1000 |
| **4** | What is Cisco SF300 | The Cisco 300 Series is broad portfolio of fixed-configuration managed Ethernet switches. Models are available with 8 to 48 ports of Fast Ethernet and 10 to 52 ports of Gigabit Ethernet connectivity, providing optimal flexibility to create exactly the right network foundation for your business. |
| **5** | Initial Configuration on 200/300 Series Managed Switches | Objective:  At its most basic definition, the job of a network switch is to receive messages from one connected device and forward them to another connected device. The 200/300 Series switches are capable of many more specialized and complicated tasks. One way to configure your switch is with the graphical user interface or GUI. This article explains how to access the GUI and configure the IP address of a 200/300 Series Managed Switch.  Applicable Devices   * SF/SG 200 and SF/SG 300 Series Managed Switches   Software Version   * v1.2.7.76 |
| **6** | Access the Graphical User Interface (GUI) | Step 1. Connect the switch to a power supply to turn it on. The switch accepts voltage in the range of 100-240V.  Step 2. Connect one end of an Ethernet cable to your computer and the other end to an available port on the switch.  Step 3. Configure your computer with an IP address in the same subnet as the IP address of the switch by one of two methods.   * Static —Assign your computer a static IP address in the same subnet as the switch.  The default IP address of the switch is 192.168.1.254, which means you must choose an IP address that is not in use and between 192.168.1.2 - 192.168.1.253. * Dynamic —Use a DHCP server that is connected to both the switch and your computer.  The DHCP server will assign the computer and the switch IP addresses.   Step 4. Open a web browser window.  Step 5. Enter the IP address of the switch in the address bar and press **Enter**. The Managed Switch Login page opens:    Step 6. Enter the username in the Username field. The default username is **cisco**.  Step 7. Enter the password in the Password field. The default password is **cisco**. Passwords are case sensitive.  Step 8. Choose the desired language from the Language drop-down list.  Step 9. Click **Log In** to log in to the device. Change the IP Address of the Switch |
|  | LAN Configuration on the 200/300 Series Managed Switches | Objective In scenarios where the division of traffic and security are priority, VLANs can be created to enhance the security of your network with the separation of traffic. Only users that belong to a VLAN are able to access and manipulate data traffic in the VLAN. This is also needed in scenarios where multiple subnets need to pass through an uplink for the device. This article explains how to configure a VLAN on the 200/300 Managed Switches. Applicable Devices  * SF/SG 200 and SF/SG 300 Series Managed Switches  Software Version  * 1.3.0.62  VLAN Configuration Step 1. Log in to the web configuration utility and choose **VLAN Management > Create VLAN**. The Create VLAN page opens:    Step 2. Click **Add**. The Add VLAN window appears.    There are two ways to create a VLAN. You can create a single VLAN or you can set a range of new VLANs.    Step 3. To create a single VLAN, click the **VLAN** radio button. Then enter the following information:   * VLAN ID — The ID of the new VLAN. * VLAN Name — The name of the new VLAN.     Step 4. To create a range of VLANs, click the **Range** radio button. Then enter the following information:   * VLAN Range — The range, according to the number of VLANs you want to create. For example, if you want to create 10 VLANs, then enter a range that will fit your needs (In this case, from 10 to 20)   Step 5. Click **Apply** to save your configuration. Configuration of Port to VLAN Once the VLANs are created, you need to assign the ports you wish to the appropriate VLAN. The next steps explain how to assign ports to VLANs on the 200/300 Series Managed Switches.  Step 1. Log in to the web configuration utility and choose **VLAN Management > Port to VLAN**. The *Port to VLAN* page opens:      Step 2. In the Filter field, from the VLAN ID Equals To drop-down list, choose the appropriate VLAN.    Step 3. In the Filter field, from the Interface Type Equals To drop-down list, choose the type of interface you would like to add to the VLAN. The available options are either a port or a LAG (Link Aggregation Group).    Step 4. Click **Go**.  Step 5. For each interface, click the radio button of the desired interface type. The available options are:   * Forbidden — The interface won't join the chosen VLAN manually, or through GVRP. Instead, the interface joins the internally used VLAN 4095 if the interface is not a member of any other VLANs. * Excluded — The interface is not a member of the chosen VLAN. If the chosen VLAN is the Default VLAN for this device, the Excluded radio button is not available. If every untagged VLAN is excluded from an interface, the interface joins automatically the Default VLAN. * Tagged — The interface is a member of the chosen VLAN and packets sent from this interface destined to the chosen VLAN will have the packet tagged with the VLAN ID. The Tagged radio button is not enabled for interfaces in Access mode if the chosen VLAN is the Default VLAN. If there are no untagged VLANs on an interface, the interface automatically joins the internally used VLAN 4095. * Untagged — The interface is a member of the chosen VLAN and packets sent from this interface destined to the chosen VLAN will not be tagged with the VLAN ID. If the interface is in Access or Trunk mode, the Default VLAN is automatically excluded when the interface joins the VLAN as Untagged. * Multicast TV VLAN — This option enables multicast transmission to users who are not in the same data VLAN. The users, which are connected to the switch with different VLAN ID, can share the same multicast stream if they join the ports to the same multicast VLAN ID.   Step 6 (Optional) The Port VLAN Identifier (PVID) identifies the Default VLAN for the interface. To set the PVID of the interface to the chosen VLAN, for each interface, check the **PVID** check box. If the interface is in Access or Trunk mode, the interface changes from Tagged to Untagged mode. On the other hand, if you uncheck the **PVID** check box and the interface is in Access or Trunk mode, the interface changes the tag mode of the VLAN to Tagged. Also if the interface is in Access or Trunk mode and if you click the **Untagged** radio button, then the **PVID** check box is checked, and if you click the **Tagged** radio button, then the **PVID** check box is unchecked.  Step 7. Click **Apply** save the settings for the chosen VLAN and interface type. |
|  | Telnet Service on 300 and 500 Series Managed Switches Enable | Telnet is a network protocol that allows a device to be controlled by a command line interface over the internet or a LAN.  When Telnet is enabled, an administrator can configure the switch through the use of a Telnet client application. However, since Telnet messages are not encrypted, it is recommended that you use SSH service.   This article explains how to enable Telnet services on SF/SG 300 and SF/SG 500 Series Managed Switches. Applicable Devices • SF/SG 300 Series Managed Switches • SF/SG 500 Series Managed Switches Software Version • v1.4.1.3 Enable Telnet Service Step 1. Log in to the web configuration utility and choose **Security > TCP/UDP Services**. The *TCP/UDP Services* page opens:    Step 2. Check **Enable** in the Telnet Service check box to enable access of the switch through the use of Telnet.    Step 3. Click **Apply** to immediately enable the Telnet service.    **Note:** For the Windows operating system, the telnet command is not available in CMD until it is enabled by through operating system. For more information refer to the [Windows Telnet: Frequently Asked Questions](http://windows.microsoft.com/en-us/windows/telnet-faq#1TC=windows-7) page.  Step 4. To access the switch through Telnet, open the command prompt and enter **telnet n.n.n.n**. Enter the same username and password used to access the graphical user interface. |
| **7** | Method 1: Statically Assign TCP/IP Settings | Step 1.  Access the GUI of the switch and log in as described in the section *Access the Graphical User Interface (GUI)*.  Step 2. Click **Getting Started**. The *Getting Started*page opens:    Step 3. Click **Change Device IP Address**to change the IP address of the switch.  The *IPv4 Interface* page opens:    Step 4. Choose a VLAN number from the *Management VLAN* drop-down list. Only devices on the management VLAN will be able to access the GUI of the switch. The default management VLAN of the switch is VLAN1.  Refer to the article *VLAN Configuration on the 200/300 Series Managed Switches* for help with VLANs.  Step 3. Click the **Static** radio button in the *IP Address Type* field to manually assign an IP address.  Step 4. Enter the desired IP address of the switch in *IP Address* field.  Step 5. Click the radio button that corresponds to the method used to determine the subnet mask in the *Mask* field.  Step 6. Click the radio button that corresponds with the method used to determine the administrative default gateway in the *Administrative Default Gateway* field.   * Network Mask — Enter the IP address mask. * Prefix Length — Enter the IP address prefix length. * User Defined — Enter the IP address of the default gateway. * None — No default gateway will be configured. If no default gateway is chosen, the switch will not be able to communicate with devices that are outside of the IP subnet of the switch.   Step 7. Click **Apply** to save the settings. |
| **8** | Method 2: Dynamically Assign TCP/IP Settings | Step 1.  Access the GUI of the switch and log in as described in the section Access the Graphical User Interface (GUI).  Step 2. Click **Getting Started**. The Getting Started page opens:    Step 3. Click **Change Device IP Address**to change the IP address of the switch.  The IPv4 Interface page opens:    Step 4. Choose a VLAN number from the Management VLAN drop-down list. Only devices on the management VLAN will be able to access the GUI of the switch. The default management VLAN of the switch is VLAN1.  Refer to the article VLAN Configuration on the 200/300 Series Managed Switches for help with VLANs.  Step 5. Click the **Dynamic** radio button in the IP Address Type field to dynamically assign an IP address.  Step 6. (Optional) Check the **Enable**check box in the Renew IP Address Now field to renew the IP address of the switch.  The Auto Configuration via DHCP field shows the status of the Auto Configuration feature.  Refer to the article Dynamic Host Configuration Protocol (DHCP) Server Auto Configuration on the 200/300 Series Managed Switches for more information.  Step 7. Click **Apply** to save the settings. |
| **9** | Configure Basic Password Settings | Step 1. Log in to the switch console. The default username and password is *cisco*.    **Note:** The available commands or options may vary depending on the exact model of your device. In this example, the SG350X switch is used.  Step 2. You will be prompted to configure new password for better protection of your network. Press **Y** for Yes or **N** for No on your keyboard.    **Note:** In this example, Y is pressed.  Step 3. Enter the old password then press **Enter** on your keyboard.    Step 4. Enter and confirm the new password accordingly then press **Enter** on your keyboard.    Step 5. Enter Privileged EXEC mode with the **enable** command. In the Privileged EXEC mode of the switch, save the configured settings to the startup configuration file, by entering the following:  SG350X#**copy running-config startup-config**  Step 6. (Optional) Press **Y** for Yes or **N** for No on your keyboard once the Overwrite file [startup-config]… prompt appears.    You should now have configured the basic password settings on your switch through the CLI. |
| **10** | Configure Line Password Settings | Step 1. Log in to the switch console. The default username and password is *cisco*. If you have configured a new username or password, enter those credentials instead.    Step 2. In the Privileged EXEC mode of the switch, enter the Global Configuration mode by entering the following:  SG350X#**configure terminal**  Step 3. To configure a password on a line such as console, Telnet, Secure Shell (SSH), and so on, enter the password Line Configuration mode by entering the following:  SG350X(config)#**line [line-name]**  **Note:** In this example, the line used is Telnet.  Step 4. Enter the password command for the line by entering the following:  SG350X(config-line)#**password [password][encrypted]**  The options are:   * password — Specifies the password for the line. The length ranges from 0 to 159 characters. * encrypted — (Optional) Specifies that the password is encrypted and copied from another device configuration.   **Note:** In this example, the password Cisco123$ is specified for the Telnet line.    Step 5. (Optional) To return the line password to the default password, enter the following:  SG350X(config-line)#**no password**  Step 6. Enter the **end** command to go back to the Privileged EXEC mode of the switch.  SG350X(config)#**end**  Step 7. (Optional) In the Privileged EXEC mode of the switch, save the configured settings to the startup configuration file, by entering the following:  SG350X#**copy running-config startup-config**  Step 8. (Optional) Press **Y** for Yes or **N** for No on your keyboard once the Overwrite file [startup-config]… prompt appears.    You should now have configured the line password settings on your switch through the CLI. |
| **11** | Configure Enable Password Settings | Configure Enable Password Settings When you configure a new enable password, it is automatically encrypted and saved to the running configuration file. No matter how the password was entered, it will appear in the running configuration file with the keyword **encrypted** together with the encrypted password.  Follow these steps to configure the enable password settings on your switch through the CLI:  Step 1. Log in to the switch console. The default username and password is cisco. If you have configured a new username or password, enter those credentials instead.    Step 2. In the Privileged EXEC mode of the switch, enter the Global Configuration mode by entering the following:  SG350X#**configure terminal**  Step 3. To configure a local password on specific user access levels on your switch, enter the following:  SG350X(config)#**enable password [level privilege-level] [unencrypted-password | encrypted encrypted-password]**  The options are:   * **level** privilege-level — Specifies the level for which the password applies. The level ranges from 1 to 15. If not specified, the level is set to the default value of 15. The user levels are as follows:   - Read-Only CLI Access (1) — User cannot access the GUI, and can only access CLI commands that do not change the device configuration.  - Read/Limited Write CLI Access (7) — User cannot access the GUI, and can only access some CLI commands that change the device configuration. See the CLI Reference Guide for more information.  - Read/Write Management Access (15) — User can access the GUI, and can configure the device.  SG350X(config)#**enable password level 7 Cisco123$**  **Note:**In this example, the password Cisco123$ is set for the level 7 user account.   * unencrypted-password — The password for the username that you are currently using. The length ranges from 0 to 159 characters.   SG350X(config)#**enable password level Cisco123$**  **Note:**In this example, the password Cisco123$ is used.   * **encrypted** encrypted-password — Specifies that the password is encrypted. You can use this command to enter a password that is already encrypted from another configuration file of another device. This will allow you to configure the two switches with the same password.   SG350X(config)#**enable password encrypted 6f43205030a2f3a1e243873007370fab**  **Note:**In this example, the encrypted password used is 6f43205030a2f3a1e243873007370fab. This is the encrypted version of Cisco123$.    **Note:** In the above example, the enable password Cisco123$ is set for the level 7 access.  Step 4. (Optional) To return the user password to the default password, enter the following:  SG350X(config)#**no enable password**  Step 5. Enter the **exit** command to go back to the Privileged EXEC mode of the switch.  SG350X(config)#**exit**  Step 6. (Optional) In the Privileged EXEC mode of the switch, save the configured settings to the startup configuration file, by entering the following:  SG350X#**copy running-config startup-config**  Step 7. (Optional) Press **Y** for Yes or **N** for No on your keyboard once the Overwrite file [startup-config]… prompt appears.    You should now have configured the enable password settings on your switch through the CLI. |
| **12** | What is Cisco Telnet? | The Telnet protocol **enables you to set up TCP/IP connections to a host**. Telnet allows a user at one site to establish a TCP connection to a login server at another site and then pass the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address. |
| **13** | Prerequisites for Telnet | You have configured IP on a Layer 3 interface, out of band on the mgmt 0 interface. |
| **14** | Guidelines and Limitations for Telnet | • The Telnet server is disabled by default • Cisco NX-OS commands may differ from Cisco IOS commands. |