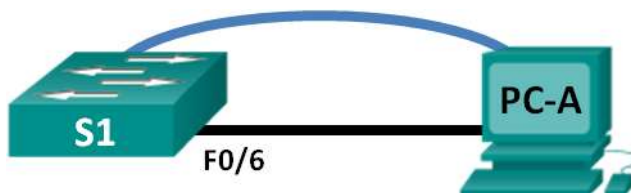


Lab – Configuring Basic Switch Settings (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Cable the Network and Verify the Default Switch Configuration

Part 2: Configure Basic Network Device Settings

- Configure basic switch settings.
- Configure the PC IP address.

Part 3: Verify and Test Network Connectivity

- Display device configuration.
- Test end-to-end connectivity with ping.
- Test remote management capabilities with Telnet.
- Save the switch running configuration file.

Part 4: Manage the MAC Address Table

- Record the MAC address of the host.
- Determine the MAC addresses that the switch has learned.
- List the **show mac address-table** command options.
- Set up a static MAC address.

Background / Scenario

Cisco switches can be configured with a special IP address known as Switched Virtual Interface (SVI). The SVI or management address can be used for remote access to the switch to display or configure settings. If the VLAN 1 SVI is assigned an IP address, by default, all ports in VLAN 1 have access to the SVI management IP address.

In this lab, you will build a simple topology using Ethernet LAN cabling and access a Cisco switch using the console and remote access methods. You will examine default switch configurations before configuring basic switch settings. These basic switch settings include device name, interface description, local passwords,

message of the day (MOTD) banner, IP addressing, setting up a static MAC address, and demonstrating the use of a management IP address for remote switch management. The topology consists of one switch and one host using only Ethernet and console ports.

Note: The switch used is a Cisco Catalyst 2960 with Cisco IOS Release 15.0(2) (lanbasek9 image). Other 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.

Note: Make sure that the switch has been erased and has no startup configuration. Refer to Appendix A for the procedures to initialize and reload devices.

Required Resources

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term, and Telnet capability)
- Console cable to configure the Cisco IOS device via the console port
- Ethernet cable as shown in the topology

Part 1: Cable the Network and Verify the Default Switch Configuration

In Part 1, you will set up the network topology and verify default switch settings.

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

- a. Cable the console connection as shown in the topology. Do not connect the PC-A Ethernet cable at this time.

Note: If you are using Netlab, you can shut down F0/6 on S1 which has the same effect as not connecting PC-A to S1.

- b. Create a console connection to the switch from PC-A using Tera Term or other terminal emulation program.

Why must you use a console connection to initially configure the switch? Why is it not possible to connect to the switch via Telnet or SSH?

No IP addressing parameters are configured yet. A Cisco 2960 switch first placed into service has no networking configured.

Step 2: Verify the default switch configuration.

In this step, you will examine the default switch settings, such as current switch configuration, IOS information, interface properties, VLAN information, and flash memory.

You can access all the switch IOS commands in privileged EXEC mode. Access to privileged EXEC mode should be restricted by password protection to prevent unauthorized use because it provides direct access to global configuration mode and commands used to configure operating parameters. You will set passwords later in this lab.

The privileged EXEC mode command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes is gained. Use the **enable** command to enter privileged EXEC mode.

Lab – Configuring Basic Switch Settings

- a. Assuming the switch had no configuration file stored in nonvolatile random-access memory (NVRAM), you will be at the user EXEC mode prompt on the switch with a prompt of Switch>. Use the **enable** command to enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Verify a clean configuration file with the **show running-config** privileged EXEC mode command. If a configuration file was previously saved, it must be removed. Depending on switch model and IOS version, your configuration may look slightly different. However, there should be no configured passwords or IP address. If your switch does not have a default configuration, erase and reload the switch.

Note: Appendix A details the steps to initialize and reload the devices.

- b. Examine the current running configuration file.

```
Switch# show running-config
```

How many FastEthernet interfaces does a 2960 switch have? _____ 24

How many Gigabit Ethernet interfaces does a 2960 switch have? _____ 2

What is the range of values shown for the vty lines? _____ 5-15

- c. Examine the startup configuration file in NVRAM.

```
Switch# show startup-config
startup-config is not present
```

Why does this message appear? _____

Nothing yet has been saved to NVRAM.

- d. Examine the characteristics of the SVI for VLAN 1.

```
Switch# show interface vlan1
```

Is there an IP address assigned to VLAN 1? _____ No

What is the MAC address of this SVI? Answers will vary. _____

0CD9:96E2:3D40 in this case.

Is this interface up?

Cisco switches have the **no shutdown** command configured by default on VLAN 1, but VLAN 1 won't reach the up/up state until a port is assigned to it and this port is also up. If there is no port in the up state in VLAN 1, then the VLAN 1 interface will be up, line protocol down. By default, all ports are assigned initially to VLAN 1.

- e. Examine the IP properties of the SVI VLAN 1.

```
Switch# show ip interface vlan1
```

What output do you see?

```
Vlan1 is up, line protocol is down
Internet protocol processing disabled
```

Lab – Configuring Basic Switch Settings

- f. Connect PC-A Ethernet cable to port 6 on the switch and examine the IP properties of the SVI VLAN 1. Allow time for the switch and PC to negotiate duplex and speed parameters.

Note: If you are using Netlab, enable interface F0/6 on S1.

Switch# **show ip interface vlan1**

What output do you see?

Vlan1 is up, line protocol is up
Internet protocol processing disabled

- g. Examine the Cisco IOS version information of the switch.

Switch# **show version**

What is the Cisco IOS version that the switch is running? _____

Answers may vary. c2960-lanbasek9-mz.150-2-SE.bin

What is the system image filename? _____

Answers may vary. c2960-LANBASEK9-MZ

What is the base MAC address of this switch? Answers will vary.

Answers will vary. 0C:D9:96:E2:3D:00.

- h. Examine the default properties of the FastEthernet interface used by PC-A.

Switch# **show interface f0/6**

Is the interface up or down? _____ It should be up unless there is a cabling problem.

What event would make an interface go up? _____

Connecting a host or other device

What is the MAC address of the interface? _____ 0CD9:96E2:3D06 (Varies)

What is the speed and duplex setting of the interface? _____ Full-duplex, 100Mb/s

- i. Examine the default VLAN settings of the switch.

Switch# **show vlan**

What is the default name of VLAN 1? _____ default

Which ports are in this VLAN? _____

all ports; Fa0/1 – Fa0/24; Gi0/1, Gi0/2

Is VLAN 1 active? _____ Yes

What type of VLAN is the default VLAN? _____ enet (Ethernet)

- j. Examine flash memory.

Issue one of the following commands to examine the contents of the flash directory.

Switch# **show flash**

Switch# **dir flash:**

Files have a file extension, such as .bin, at the end of the filename. Directories do not have a file extension.

What is the filename of the Cisco IOS image? _____
c2960-lanbasek9-mz.150-2.SE.bin (may vary)

Part 2: Configure Basic Network Device Settings

In Part 2, you configure basic settings for the switch and PC.

Step 1: Configure basic switch settings including hostname, local passwords, MOTD banner, management address, and Telnet access.

In this step, you will configure the PC and basic switch settings, such as hostname and an IP address for the switch management SVI. Assigning an IP address on the switch is only the first step. As the network administrator, you must specify how the switch is managed. Telnet and SSH are the two most common management methods. However, Telnet is not a secure protocol. All information flowing between the two devices is sent in plain text. Passwords and other sensitive information can be easily looked at if captured by a packet sniffer.

- a. Assuming the switch had no configuration file stored in NVRAM, verify you are at privileged EXEC mode. Enter **enable** if the prompt has changed back to Switch>.

```
Switch> enable
Switch#
```

- b. Enter global configuration mode.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

The prompt changed again to reflect global configuration mode.

- c. Assign the switch hostname.

```
Switch(config)# hostname S1
S1(config)#
```

- d. Configure password encryption.

```
S1(config)# service password-encryption
S1(config)#
```

- e. Assign **class** as the secret password for privileged EXEC mode access.

```
S1(config)# enable secret class
S1(config)#
```

- f. Prevent unwanted DNS lookups.

```
S1(config)# no ip domain-lookup
S1(config)#
```

- g. Configure a MOTD banner.

```
S1(config)# banner motd #
Enter Text message. End with the character '#'.
Unauthorized access is strictly prohibited. #
```

- h. Verify your access settings by moving between modes.

```
S1(config)# exit
S1#
```

Lab – Configuring Basic Switch Settings

```
*Mar  1 00:19:19.490: %SYS-5-CONFIG_I: Configured from console by console
S1# exit
S1 con0 is now available
```

Press RETURN to get started.

```
Unauthorized access is strictly prohibited.
S1>
```

Which shortcut keys are used to go directly from global configuration mode to privileged EXEC mode?

_____ **Ctrl-Z**

- i. Go back to privileged EXEC mode from user EXEC mode. Enter **class** as the password when prompted.

```
S1> enable
Password:
S1#
```

Note: The password does not display when entering.

- j. Enter global configuration mode to set the SVI IP address of the switch. This allows remote management of the switch.

Before you can manage S1 remotely from PC-A, you must assign the switch an IP address. The default configuration on the switch is to have the management of the switch controlled through VLAN 1. However, a best practice for basic switch configuration is to change the management VLAN to a VLAN other than VLAN 1.

For management purposes, use VLAN 99. The selection of VLAN 99 is arbitrary and in no way implies that you should always use VLAN 99.

First, create the new VLAN 99 on the switch. Then set the IP address of the switch to 192.168.1.2 with a subnet mask of 255.255.255.0 on the internal virtual interface VLAN 99.

```
S1# configure terminal
S1(config)# vlan 99
S1(config-vlan)# exit
S1(config)# interface vlan99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)#
```

Notice that the VLAN 99 interface is in the down state even though you entered the **no shutdown** command. The interface is currently down because no switch ports are assigned to VLAN 99.

- k. Assign all user ports to VLAN 99.

```
S1(config)# interface range f0/1 - 24,g0/1 - 2
S1(config-if-range)# switchport access vlan 99
S1(config-if-range)# exit
```

```
S1(config)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

To establish connectivity between the host and the switch, the ports used by the host must be in the same VLAN as the switch. Notice in the above output that the VLAN 1 interface goes down because none of the ports are assigned to VLAN 1. After a few seconds, VLAN 99 comes up because at least one active port (F0/6 with PC-A attached) is now assigned to VLAN 99.

- I. Issue **show vlan brief** command to verify that all the user ports are in VLAN 99.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
99	VLAN0099	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- m. Configure the IP default gateway for S1. If no default gateway is set, the switch cannot be managed from a remote network that is more than one router away. It does respond to pings from a remote network. Although this activity does not include an external IP gateway, assume that you will eventually connect the LAN to a router for external access. Assuming that the LAN interface on the router is 192.168.1.1, set the default gateway for the switch.

```
S1(config)# ip default-gateway 192.168.1.1
```

```
S1(config)#
```

- n. Console port access should also be restricted. The default configuration is to allow all console connections with no password needed. To prevent console messages from interrupting commands, use the **logging synchronous** option.

```
S1(config)# line con 0
```

```
S1(config-line)# password cisco
```

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

```
S1(config-line)# logging synchronous
```

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

```
S1(config)#
```

- o. Configure the virtual terminal (vty) lines for the switch to allow Telnet access. If you do not configure a vty password, you are unable to telnet to the switch.

```
S1(config)# line vty 0 15
```

```
S1(config-line)# password cisco
```

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

```
S1(config-line)# end
```

```
S1#
```

```
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

Why is the **login** command required? _____

Without the **login** command, the switch will not prompt for a password to be entered.

Step 2: Configure an IP address on PC-A.

Assign the IP address and subnet mask to the PC as shown in the Addressing Table. An abbreviated version of the procedure is described here. A default gateway is not required for this topology; however, you can enter **192.168.1.1** to simulate a router attached to S1.

- 1) Click the Windows **Start** icon > **Control Panel**.
- 2) Click **View By:** and choose **Small icons**.
- 3) Choose **Network and Sharing Center** > **Change adapter settings**.
- 4) Select **Local Area Network Connection**, right click and choose **Properties**.
- 5) Choose **Internet Protocol Version 4 (TCP/IPv4)** > **Properties**.
- 6) Click the **Use the following IP address** radio button and enter the IP address and subnet mask.

Part 3: Verify and Test Network Connectivity

In Part 3, you will verify and document the switch configuration, test end-to-end connectivity between PC-A and S1, and test the switch's remote management capability.

Step 1: Display the switch configuration.

From your console connection on PC-A, display and verify your switch configuration. The **show run** command displays the entire running configuration, one page at a time. Use the spacebar to advance paging.

- a. A sample configuration displays here. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

```
S1# show run
```

```
Building configuration...
```

```
Current configuration : 2206 bytes
```

```
!
```

```
version 15.0
```

```
no service pad
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service password-encryption
```

```
!
```

```
hostname S1
```

```
!
```

```
boot-start-marker
```

```
boot-end-marker
```

```
!
```

```
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
```

```
!
```

```
no aaa new-model
```

```
system mtu routing 1500
```



```
!  
!  
no ip domain-lookup  
!  
<output omitted>  
!  
interface FastEthernet0/24  
  switchport access vlan 99  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
  no ip address  
  no ip route-cache  
!  
interface Vlan99  
  ip address 192.168.1.2 255.255.255.0  
  no ip route-cache  
!  
ip default-gateway 192.168.1.1  
ip http server  
ip http secure-server  
!  
banner motd ^C  
Unauthorized access is strictly prohibited. ^C  
!  
line con 0  
  password 7 104D000A0618  
  logging synchronous  
  login  
line vty 0 4  
  password 7 14141B180F0B  
  login  
line vty 5 15  
  password 7 14141B180F0B  
  login  
!  
end  
  
S1#
```

- b. Verify the management VLAN 99 settings.

```
S1# show interface vlan 99  
Vlan99 is up, line protocol is up  
  Hardware is EtherSVI, address is 0cd9.96e2.3d41 (bia 0cd9.96e2.3d41)  
  Internet address is 192.168.1.2/24  
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
```

```
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:06, output 00:08:45, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  175 packets input, 22989 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
      0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    1 packets output, 64 bytes, 0 underruns
      0 output errors, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
What is the bandwidth on this interface? _____ 1000000 Kb/s (1 Gb/sec)
What is the VLAN 99 state? _____ up
What is the line protocol state? _____ up
```

Step 2: Test end-to-end connectivity with ping.

- a. From the command prompt on PC-A, ping your own PC-A address first.

```
C:\Users\User1> ping 192.168.1.10
```

- b. From the command prompt on PC-A, ping the SVI management address of S1.

```
C:\Users\User1> ping 192.168.1.2
```

Because PC-A needs to resolve the MAC address of S1 through ARP, the first packet may time out. If ping results continue to be unsuccessful, troubleshoot the basic device configurations. You should check both the physical cabling and logical addressing if necessary.

Step 3: Test and verify remote management of S1.

You will now use Telnet to remotely access the switch. In this lab, PC-A and S1 reside side by side. In a production network, the switch could be in a wiring closet on the top floor while your management PC is located on the ground floor. In this step, you will use Telnet to remotely access switch S1 using its SVI management address. Telnet is not a secure protocol; however, you will use it to test remote access. With Telnet, all information, including passwords and commands, are sent across the session in plain text. In subsequent labs, you will use SSH to remotely access network devices.

Instructor Note: Tera Term or other terminal emulation programs with Telnet capability may be used if Telnet from the Windows command prompt is not allowed at your institution.

Note: If you are using Windows 7, the administrator may need to enable the Telnet protocol. To install the Telnet client, open a cmd window and type **pkgmgr /iu:"TelnetClient"**. An example is shown below.

```
C:\Users\User1> pkgmgr /iu:"TelnetClient"
```

- a. With the cmd window still open on PC-A, issue a Telnet command to connect to S1 via the SVI management address. The password is **cisco**.

```
C:\Users\User1> telnet 192.168.1.2
```

- b. After entering the password **cisco**, you will be at the user EXEC mode prompt. Access privileged EXEC mode.
- c. Type **exit** to end the Telnet session.

Step 4: Save the switch running configuration file.

Save the configuration.

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
S1#
```

Part 4: Manage the MAC Address Table

In Part 4, you will determine the MAC address that the switch has learned, set up a static MAC address on one interface of the switch, and then remove the static MAC address from that interface.

Step 1: Record the MAC address of the host.

From a command prompt on PC-A, issue **ipconfig /all** command to determine and record the Layer 2 (physical) addresses of the PC NIC.

PC-A: 00-50-56-BE-6C-89 (answers will vary)

Step 2: Determine the MAC addresses that the switch has learned.

Display the MAC addresses using the **show mac address-table** command.

```
S1# show mac address-table
```

How many dynamic addresses are there? _____ 1 (can vary)

How many MAC addresses are there in total? _____ 24 (can vary)

Does the dynamic MAC address match the PC-A MAC address? _____ Yes

Step 3: List the show mac address-table options.

- a. Display the MAC address table options.

```
S1# show mac address-table ?
```

How many options are available for the **show mac address-table** command? _____ 12 (can vary)

- b. Issue the **show mac address-table dynamic** command to display only the MAC addresses that were learned dynamically.

```
S1# show mac address-table dynamic
```

How many dynamic addresses are there? _____ 1 (can vary)

- c. View the MAC address entry for PC-A. The MAC address formatting for the command is xxxx.xxxx.xxxx.

```
S1# show mac address-table address <PC-A MAC here>
```

Step 4: Set up a static MAC address.

- a. Clear the MAC address table.

To remove the existing MAC addresses, use the **clear mac address-table** command from privileged EXEC mode.

```
S1# clear mac address-table dynamic
```

- b. Verify that the MAC address table was cleared.

```
S1# show mac address-table
```

How many static MAC addresses are there? _____

at least 20 (other static entries could have been manually created)

Instructor Note: The first 20 static addresses in the MAC address table are built-in.

How many dynamic addresses are there? _____

0 (may be 1, depending on how quickly addresses are re-acquired by the switch)

- c. Examine the MAC table again.

More than likely, an application running on your PC has already sent a frame out the NIC to S1. Look at the MAC address table again in privileged EXEC mode to see if S1 has relearned the MAC address for PC-A.

```
S1# show mac address-table
```

How many dynamic addresses are there? _____ 1

Why did this change from the last display? _____

The switch dynamically reacquired the PC MAC address.

If S1 has not yet relearned the MAC address for PC-A, ping the VLAN 99 IP address of the switch from PC-A, and then repeat the **show mac address-table** command.

- d. Set up a static MAC address.

To specify which ports a host can connect to, one option is to create a static mapping of the host MAC address to a port.

Set up a static MAC address on F0/6 using the address that was recorded for PC-A in Part 4, Step 1. The MAC address 0050.56BE.6C89 is used as an example only. You must use the MAC address of your PC-A, which is different than the one given here as an example.

```
S1(config)# mac address-table static 0050.56BE.6C89 vlan 99 interface  
fastethernet 0/6
```

- e. Verify the MAC address table entries.

```
S1# show mac address-table
```

How many total MAC addresses are there? _____ 21 (varies)

How many static addresses are there? _____

There are 22 static addresses. Total MAC addresses and static addresses should be the same because there are no other devices currently connected to S1.

- f. Remove the static MAC entry. Enter global configuration mode and remove the command by putting a **no** in front of the command string.

Note: The MAC address 0050.56BE.6C89 is used in the example only. Use the MAC address for your PC-A.

Lab – Configuring Basic Switch Settings

```
S1(config)# no mac address-table static 0050.56BE.6C89 vlan 99 interface
fastethernet 0/6
```

- g. Verify that the static MAC address has been cleared.

```
S1# show mac address-table
```

How many total static MAC addresses are there? _____ 20 (varies)

Reflection

1. Why should you configure the vty lines for the switch?

If you do not configure a vty password you will not be able to telnet to the switch.

2. Why change the default VLAN 1 to a different VLAN number?

For improved security.

3. How can you prevent passwords from being sent in plain text?

Issue the **service password-encryption** command.

4. Why configure a static MAC address on a port interface?

To specify which ports a host can connect to.

Appendix A: Initializing and Reloading a Router and Switch

Step 1: Initialize and reload the router.

- a. Console into the router and enable privileged EXEC mode.

```
Router> enable
Router#
```

- b. Enter the **erase startup-config** command to remove the startup configuration from NVRAM.

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

- c. Issue the **reload** command to remove an old configuration from memory. When prompted to Proceed with reload?, press Enter. (Pressing any other key aborts the reload.)

```
Router# reload
Proceed with reload? [confirm]
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Note: You may receive a prompt asking to save the running configuration prior to reloading the router. Respond by typing **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

- d. After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

- e. Another prompt asks to terminate autoinstall. Respond by typing **yes** press Enter.

```
Would you like to terminate autoinstall? [yes]: yes
```

Step 2: Initialize and reload the switch.

- a. Console into the switch and enter privileged EXEC mode.

```
Switch> enable  
Switch#
```

- b. Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash  
Directory of flash:/
```

2	-rwx	1919	Mar 1 1993 00:06:33 +00:00	private-config.text
3	-rwx	1632	Mar 1 1993 00:06:33 +00:00	config.text
4	-rwx	13336	Mar 1 1993 00:06:33 +00:00	multiple-fs
5	-rwx	11607161	Mar 1 1993 02:37:06 +00:00	c2960-lanbasek9-mz.150-2.SE.bin
6	-rwx	616	Mar 1 1993 00:07:13 +00:00	vlan.dat

```
32514048 bytes total (20886528 bytes free)
```

```
Switch#
```

- c. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat  
Delete filename [vlan.dat]?
```

- d. You are prompted to verify the filename. If you have entered the name correctly, press Enter; otherwise, you can change the filename.

- e. You are prompted to confirm to delete this file. Press Enter to confirm.

```
Delete flash:/vlan.dat? [confirm]  
Switch#
```

- f. Use the **erase startup-config** command to erase the startup configuration file from NVRAM. You are prompted to remove the configuration file. Press Enter to confirm.

```
Switch# erase startup-config  
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]  
[OK]  
Erase of nvram: complete  
Switch#
```

- g. Reload the switch to remove any old configuration information from memory. You will then receive a prompt to confirm to reload the switch. Press Enter to proceed.

```
Switch# reload  
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Respond by typing **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

- h. After the switch reloads, you should see a prompt to enter the initial configuration dialog. Respond by entering **no** at the prompt and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Device Configs

Switch S1

```
S1#sh run
Building configuration...
Current configuration : 2359 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!interface FastEthernet0/1
  switchport access vlan 99
!
interface FastEthernet0/2
  switchport access vlan 99
!
interface FastEthernet0/3
  switchport access vlan 99
!
interface FastEthernet0/4
  switchport access vlan 99
!
interface FastEthernet0/5
```

Lab – Configuring Basic Switch Settings

```
switchport access vlan 99
!
interface FastEthernet0/6
switchport access vlan 99
!
interface FastEthernet0/7
switchport access vlan 99
!
interface FastEthernet0/8
switchport access vlan 99
!
interface FastEthernet0/9
switchport access vlan 99
!
interface FastEthernet0/10
switchport access vlan 99
!
interface FastEthernet0/11
switchport access vlan 99
!
interface FastEthernet0/12
switchport access vlan 99
!
interface FastEthernet0/13
switchport access vlan 99
!
interface FastEthernet0/14
switchport access vlan 99
!
interface FastEthernet0/15
switchport access vlan 99
!
interface FastEthernet0/16
switchport access vlan 99
!
interface FastEthernet0/17
switchport access vlan 99
!
interface FastEthernet0/18
switchport access vlan 99
!
interface FastEthernet0/19
switchport access vlan 99
!
interface FastEthernet0/20
switchport access vlan 99
!
interface FastEthernet0/21
switchport access vlan 99
```


Lab – Configuring Basic Switch Settings

```
!  
interface FastEthernet0/22  
  switchport access vlan 99  
!  
interface FastEthernet0/23  
  switchport access vlan 99  
!  
interface FastEthernet0/24  
  switchport access vlan 99  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
  no ip address  
!  
interface Vlan99  
  ip address 192.168.1.2 255.255.255.0  
!  
ip default-gateway 192.168.1.1  
ip http server  
ip http secure-server  
!  
!  
banner motd ^C  
Unauthorized access is strictly prohibited. ^C  
!  
line con 0  
  password 7 0822455D0A16  
  logging synchronous  
  login  
line vty 0 4  
  password 7 01100F175804  
  login  
line vty 5 15  
  password 7 01100F175804  
  login  
!  
end
```