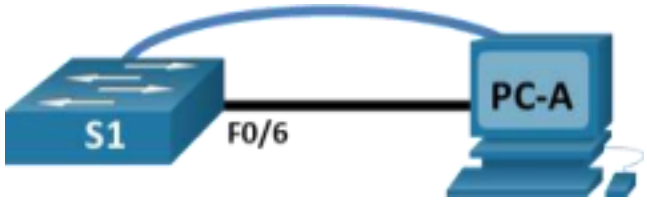
Lab - Basic Switch Configuration

Topology



Addressing Table

Device	Interface	IP Address / Prefix
S1	VLAN 99	192.168.1.2 /24
		2001:db8:acad:1::2 /64
		fe80::2
PC-A	NIC	192.168.1.10 /24
		2001:db8:acad:1::10 /64

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.

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.

Lab - Basic Switch Configuration

Background / Scenario

Cisco switches can be configured with a special IP address known as the switch 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 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, and static MAC address. You will also demonstrate 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 switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.2(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 switches have been erased and have no startup configurations. If you are unsure, contact your instructor. Refer to Appendix A for the procedures to initialize and reload a switch.

The **default bias** template used by the Switch Database Manager (SDM) does not provide IPv6 address capabilities. Verify that SDM is using either the **dual-ipv4-and-ipv6** template or the **lanbase-routing** template. The new template will be used after reboot even if the configuration is not saved.

```
S1# show sdm prefer
```

Use the following commands to assign the **dual-ipv4-and-ipv6** template as the default SDM template.

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
  reload
S1#
```

Required Resources

• 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable) •

1 PC (Windows with terminal emulation program, such as Tera Term)

• 1 Console cable to configure the Cisco IOS device via the console port

• 1 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. Connect the console cable as shown in the topology. Do not connect the PC-A Ethernet cable at this

time.

b. Connect 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.

♥ 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.

a. Assuming the switch had no configuration file stored in nonvolatile random-access memory (NVRAM), A console connection using Tera Term or other terminal emulation program will place you 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 that there is a clean default configuration file on the switch by issuing the **show running-config** privileged EXEC mode command. If a configuration file was previously saved, it must be removed. Depending on the 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 a switch.

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?

0-4 and 5-15 or 0-15

c. Examine the startup configuration file in NVRAM.

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

Why does this message appear?

No configurations have been saved to NVRAM

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

```
Switch# show interface vlan1
```

♥ 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

Is there an IP address assigned to VLAN 1?

NO

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

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

f. Connect an Ethernet cable from PC-A 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.

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

What output do you see?

Vlan1 is administratively down, line protocol is down

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?

Version 15.0(2)SE4

What is the system image filename?

2960-lanbasek9-mz.150-2.SE4.bin

What is the base MAC address of this switch?

00:60:70:00:24:A0

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?

What is the MAC address of the interface?

Connecting a host or other device

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.

♥ 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

Which ports are in VLAN 1?

all ports; F0/1 – F0/24; G0/1, G0/2

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?

2960-lanbasek9-mz.150-2.SE4.bin

Part 2: Configure Basic Network Device Settings

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

Step 1: Configure basic switch settings.

a. Copy the following basic configuration and paste it into S1 while in global configuration mode.

```
no ip domain-lookup
hostname S1
service password-encryption
```

```
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
1st
configure terminal
```

b. 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. IPv6 address can also be configured on the SVI interface. Use the IPv6 addresses listed in the Addressing Table.

```
S1# configure terminal
```

♥ 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public


```
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)# ipv6 address 2001:db8:acad:1::2/64
Exit press Enter to return to S1(config)#
sdm prefer dual-ipv4-and-ipv6 default
End
Reload
Yes
Enable
Pass: class
configure terminal
interface vlan 99
S1(config-if)# ipv6 address 2001:db8:acad:1::2/64
S1(config-if)# ipv6 address fe80::2 link-local
S1(config-if)# no shutdown
S1(config-if)# exit
```

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.

c. 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.

d. Issue the **show vlan brief** command to verify that all 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
```

e. Configure the 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. 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
```

♥ 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

f. Console port access should also be restricted with a password. Use **cisco** as the console login password in this activity. 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)# logging synchronous
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
```

g. Configure the virtual terminal (vty) lines for the switch to allow telnet access. If you do not configure a vty password, you will not be able 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

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** and **fe80::1** to simulate a router attached to S1.

1) Navigate to the **Control Panel**.
2) In the Category view, select **View network status and tasks**.
3) Click **Change adapter settings** on the left panel.
4) Right-click an **Ethernet** interface, and choose **Properties**.
5) Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
6) Click the **Use the following IP address** radio button and enter the IP address and subnet mask and click **OK**.
7) Select **Internet Protocol Version 6 (TCP/IPv6)** and click **Properties**.
8) Click the **Use the following IPv6 address** radio button and enter the IPv6 address and prefix and click **OK** to continue
9) Click **OK** to exit the Properties window.

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.

Use the console connection on PC-A to display and verify the 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 is shown here. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

♥ 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

```
S1# show run
Building configuration...

Current configuration : 2206 bytes
!
version 15.2
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 5
```

```
$1$mtvC$6NC.1VKr3p6bj7YGE.jNg0 !
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
<output omitted>
!
interface FastEthernet0/24
 switchport access vlan 99
!
interface GigabitEthernet0/1
 switchport access vlan 99
!
interface GigabitEthernet0/2
 switchport access vlan 99
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan99
 ip address 192.168.1.2
 255.255.255.0 ipv6 address FE80::2
 link-local
 ipv6 address 2001:DB8:ACAD:1::2/64
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
banner motd ^C
```

♥ 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lab - Basic Switch Configuration

```
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password 7 00071A150754
 logging synchronous
 login
line vty 0 4
 password 7 121A0C041104
 login
line vty 5 15
 password 7 121A0C041104
 login
!
end
```

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 runts, 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

♥ 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

```
C:\> ping 192.168.1.10
C:\> ping 2001:db8:acad:1::10
```

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

```
C:\> ping 192.168.1.2
C:\> ping 2001:db8:acad: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. Check both the physical cabling and logical addressing.

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.

a. Open Tera Term or other terminal emulation program with Telnet capability.

b. Select the Telnet server and provide the SVI management address to connect to S1. The password is **cisco**.

c. After entering the password **cisco**, you will be at the user EXEC mode prompt. Access privileged EXEC mode using the **enable** command and providing the secret password **class**.

d. Save the configuration.

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

e. Type **exit** to end the Telnet session.

Part 4: Manage the MAC Address Table

In Part 4, you will determine the MAC addresses 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.

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

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

♥ 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

How many MAC addresses are there in total?

24

Does the dynamic MAC address match the MAC address of PC-A?

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?

3

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

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 dynamic** command in 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

How many dynamic addresses are there?

0

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 of 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. 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 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?

1

How many static addresses are there?

1

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 PC-A.

```
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?

1

Reflection Questions

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

You configure a vty password primarily to enable and secure remote management. The lab explicitly notes that if you do not configure a vty password, you will not be able to telnet to the switch. Furthermore, it ensures that only authorized administrators can access the switch's command-line interface over the network.

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

This is a major security best practice. By default, every single port on a Cisco switch belongs to VLAN 1. If you assign your switch's management IP address (SVI) to VLAN 1, any user plugging into any default port instantly has network access to the switch's management interface. Changing it to a different VLAN (like VLAN 99) logically separates your administrative traffic from regular user data.

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

Across the network: You should use SSH instead of Telnet for remote access. The lab states that with Telnet, all information, including passwords and commands, is sent across the session in plain text.

In the configuration files: To prevent passwords from being easily read by someone looking at the show running-config output, you use the service password-encryption command to encrypt them within the switch's database.

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

Configuring a static MAC address is a fundamental way to enforce port security. As the lab mentions, one option to specify which ports a host can connect to is to create a static mapping of the host MAC address to a port. This prevents someone from unplugging your authorized PC, plugging in their own rogue laptop, and successfully accessing the network.

Appendix A: Initialize and Reload a 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)
```

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.

You are prompted to confirm deletion of this file. Press Enter to confirm.

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

e. 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#
```

f. Reload the switch to remove any old configuration information from memory. You will then receive a prompt to confirm reloading of 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
```

g. 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
```

♥ 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lab - Basic Switch Configuration

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 5 $1$mtvC$6NC.1VKr3p6bj7YGE.jNg0
!
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
 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
 !
interface FastEthernet0/22
 switchport access vlan 99
 !
 interface FastEthernet0/23
  switchport access vlan 99
```


Lab - Basic Switch Configuration

```
 !
interface FastEthernet0/24
  switchport access vlan 99
 !
interface GigabitEthernet0/1
  switchport access vlan 99
 !
interface GigabitEthernet0/2
  switchport access vlan 99
 !
interface Vlan1
  no ip address
 !
interface Vlan99
  ip address 192.168.1.2 255.255.255.0
  ipv6 address FE80::2 link-local
  ipv6 address 2001:DB8:ACAD:1::2/64
 !
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 00071A150754
  logging synchronous
  login
line vty 0 4
  password 7 121A0C041104
  login
line vty 5 15
  password 7 121A0C041104
```

```
 login
!
end
```

♥ 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public