CISCO

Lab Manual

Switched Networks

ciscopress.com

Cisco | Networking Academy®
Mind Wide Open™

Switched Networks Lab Manual

Cisco Networking Academy

Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240

Switched Networks Lab Manual

Cisco Networking Academy

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing December 2013

ISBN-13: 9781587133275

ISBN-10: 158713327X

Warning and Disclaimer

This book is designed to provide information about Switched Networks. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, please visit www.cisco.com/edu.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher	**Paul Boger**
Associate Publisher	**Dave Dusthimer**
Business Operations Manager, Cisco Press	**Jan Cornelssen**
Executive Editor	**Mary Beth Ray**
Managing Editor	**Sandra Schroeder**
Project Editor	**Seth Kerney**
Editorial Assistant	**Vanessa Evans**
Cover Designer	**Mark Shirar**
Compositor	**TnT Design, Inc.**

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Contents

About This Lab Manual

Switched Networks Lab Manual contains all the labs and class activities from the Cisco Networking Academy course of the same name. It is meant to be used within this program of study.

More Practice

If you would like more practice activities, combine your Lab Manual with the new *CCNA Routing and Switching Practice and Study Guide* ISBN: 9781587133442

Other Related Titles

CCNA Routing and Switching Portable Command Guide ISBN: 9781587204302 (or eBook ISBN: 9780133381368)

Switched Networks Companion Guide ISBN: 9781587133299 (or eBook ISBN: 9780133476460)

Switched Networks Course Booklet ISBN: 9781587133268

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Chapter 1 — Introduction to Switched Networks

1.0.1.2 Class Activity – Sent or Received

Objectives

Describe convergence of data, voice, and video in the context of switched networks.

Scenario

Individually, or in groups (per the instructor's decision), discuss various ways hosts send and receive data, voice, and streaming video.

- Develop a matrix (table) listing network data types that can be sent and received. Provide five examples.

Your matrix table might look something like this:

Sent	Received
Client requests a web page from a web server.	Web server send web page to requesting client.

Save your work in either hard- or soft-copy format. Be prepared to discuss your matrix and statements in a class discussion.

Resources

Internet connectivity

Reflection

1. If you are receiving data, how do you think a switch assists in that process?

____

2. If you are sending network data, how do you think a switch assists in that process?

____

1.1.3.6 Lab – Selecting Switching Hardware

Objectives

Part 1: Explore Cisco Switch Products

Part 2: Select an Access Layer Switch

Part 3: Select a Distribution/Core Layer Switch

Background / Scenario

As a Network Engineer, you are part of a team that selects appropriate devices for your network. You need to consider the network requirements for the company as they migrate to a converged network. This converged network supports voice over IP (VoIP), video streaming, and expansion of the company to support a larger customer base.

For a small- to medium-sized company, Cisco hierarchical network design suggests only using a two-tier LAN design. This design consists of an access layer and a collapsed core/distribution layer. Network switches come in different form factors, and with various features and functions. When selecting a switch, the team must choose between fixed configuration or modular configuration, and stackable or non-stackable switches.

Based on a given set of requirements, you will identify the Cisco switch models and features to support the requirements. The scope of this lab will limit the switch models to campus LAN only.

Required Resources

PC with Internet access

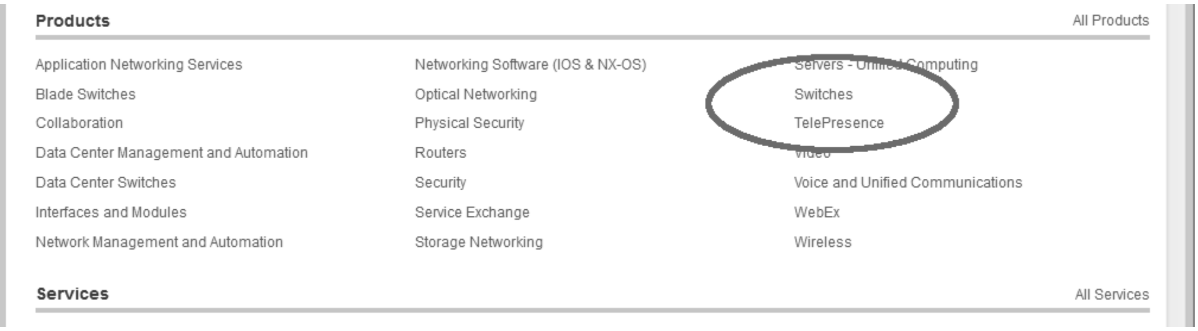
Part 1: Explore Cisco Switch Products

In Part 1, you will navigate the Cisco website and explore available switch products.

Step 1: Navigate the Cisco website.

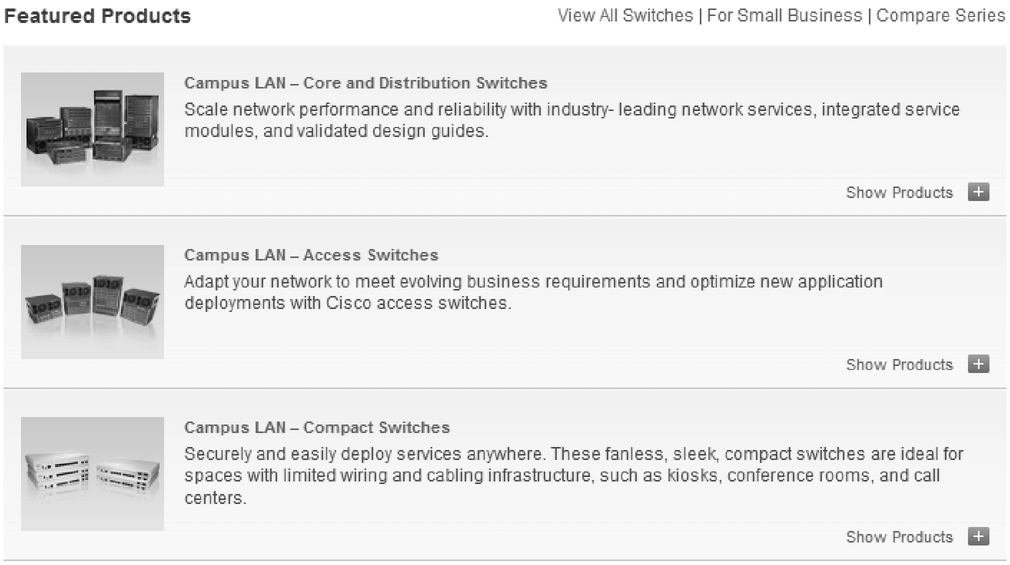
At www.cisco.com, a list of available products and information about these products is available.

a. From the home page, click **Products & Services** > **Switches**.



Step 2: Explore switch products.

In the Feature Products section, a list of different categories of switches is displayed. In this lab, you will explore the campus LAN switches. You can click different links to gather information about the different switch models. On this page, the information is organized in different ways. You can view all available switches by clicking **View All Switches**. If you click **Compare Series**, the switches are organized by types: modular vs. fixed configuration.



Featured Products

View All Switches | For Small Business | Compare Series

Campus LAN – Core and Distribution Switches

Scale network performance and reliability with industry- leading network services, integrated service modules, and validated design guides.

Show Products +

Campus LAN – Access Switches

Adapt your network to meet evolving business requirements and optimize new application deployments with Cisco access switches.

Show Products +

Campus LAN – Compact Switches

Securely and easily deploy services anywhere. These fanless, sleek, compact switches are ideal for spaces with limited wiring and cabling infrastructure, such as kiosks, conference rooms, and call centers.

Show Products +

a. Click the heading **Campus LAN – Core and Distribution Switches**.

List a few models and some of features in the table below.

Model	Uplink Speed	Number of Ports/Speed	Other Features

b. Click the heading **Campus LAN – Access Switches**.

List a few models and some of features in the table below.

Model	Uplink Speed	Number of Ports/Speed	Other Features

c. Click the heading **Campus LAN – Compact Switches**.

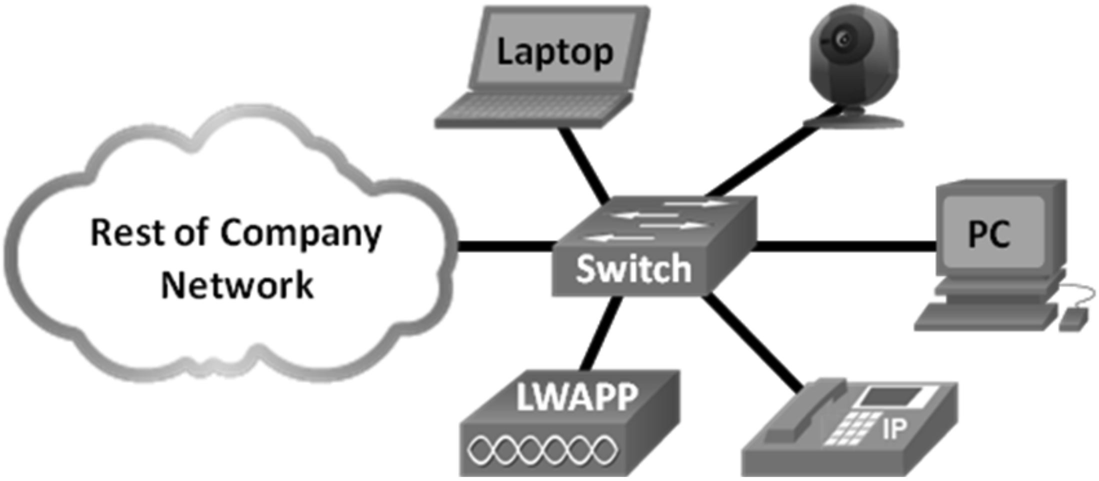
List a few models and some of features in the table below.

Model	Uplink Speed	Number of Ports/Speed	Other Features

Part 2: Select an Access Layer Switch

The main function of an access layer switch is to provide network access to end user devices. This switch connects to the core/distribution layer switches. Access switches are usually located in the intermediate distribution frame (IDF). An IDF is mainly used for managing and interconnecting the telecommunications cables between end user devices and a main distribution frame (MDF). There are typically multiple IDFs with uplinks to a single centralized MDF.

An access switch should have the following capabilities: low cost per switch port, high port density, scalable uplinks to higher layers, and user access functions and resiliency. In Part 2, you will select an access switch based on the requirements set by the company. You have reviewed and become familiar with Cisco switch product line.



a. Company A requires a replacement access switch in the wiring closet. The company requires the switch to support VoIP and multicast, accommodate future growth of users and increased bandwidth usage. The switch must support a minimum of 35 current users and have a high-speed uplink. List a few of models that meet those requirements.

____

____

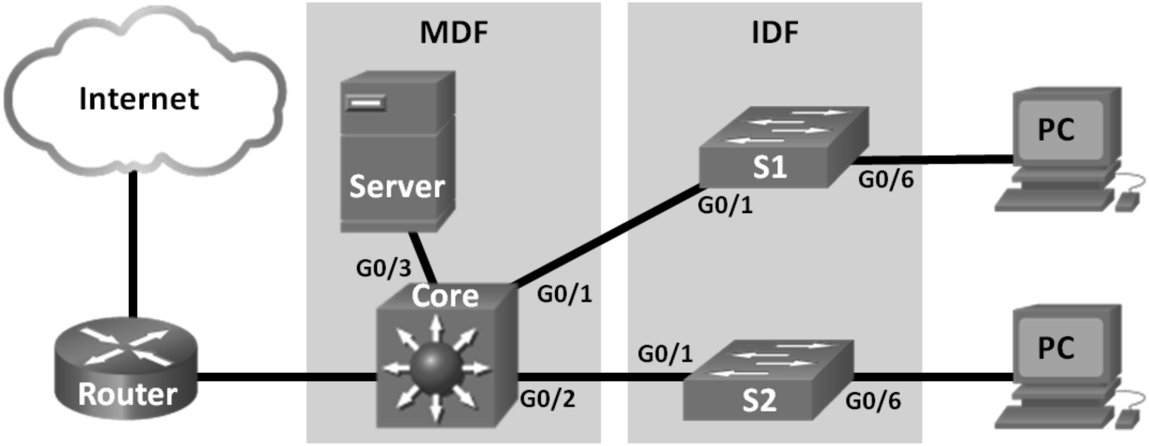
b. Company B would like to extend services to a conference room on an as-needed basis. The switch will be placed on the conference room table, and switch security is a priority.

____

____

Part 3: Select a Distribution/Core Layer Switch

The distribution/core switch is the backbone of the network for the company. A reliable network core is of paramount importance for the function of the company. A network backbone switch provides both adequate capacity for current and future traffic requirements and resilience in the event of failure. They also require high throughput, high availability, and advanced quality of service (QoS). These switches usually reside in the main wiring closet (MDF) along with high speed servers, routers, and the termination point of your ISP.



a. Company C will replace a backbone switch in the next budget cycle. The switch must provide redundancy features to minimize possible downtime in the event that an internal component fails. What features can accommodate these requirements for the replacement switch?

____

____

b. Which Cisco Catalyst switches would you recommend?

____

c. As Company C grows, high speed, such as 10 GB Ethernet, up to 8 uplink ports, and a modular configuration for the switch will become necessary. Which switch models would meet the requirement?

____

Reflection

What other factors should be considered during the selection process aside from network requirements and costs?

____

____

1.3.1.1 Class Activity – It's Network Access Time

Objectives

Describe features available for switches to support requirements of a small- to medium-sized business network.

Scenario

Use Packet Tracer for this activity. Work with a classmate to create two network designs to accommodate the following scenarios:

Scenario 1 – Classroom Design (LAN)

- 15 student end devices represented by 1 or 2 PCs.
- 1 instructor end device; a server is preferred.
- Device capability to stream video presentations over LAN connection. Internet connectivity is not required in this design.

Scenario 2 – Administrative Design (WAN)

- All requirements as listed in Scenario 1.
- Add access to and from a remote administrative server for video presentations and pushed updates for network application software.

Both the LAN and WAN designs should fit on to one Packet Tracer file screen. All intermediary devices should be labeled with the switch model (or name) and the router model (or name).

Save your work and be ready to justify your device decisions and layout to your instructor and the class.

Reflection

1. What are some problems that may be encountered if you receive streaming video from your instructor's server through a low-end switch?

   ____

2. How would the traffic flow be determined: multicast or broadcast – in transmission?

   ____

3. What would influence your decision on the type of switch to use for voice, streaming video and regular data transmissions?

   ____

4. As you learned in the first course of the Academy, video and voice use a special TCP/IP model, transport layer protocol. What protocol is used in this layer and why is it important to voice and video streaming?

   ____

Chapter 2 — Basic Switching Concepts and Configuration

2.0.1.2 Class Activity – Stand By Me

Objective

Describe the role of unicast, broadcast, and multicast in a switched network.

Scenario

When you arrived to class today, you were given a number by your instructor to use for this introductory class activity.

Once class begins, your instructor will ask certain students with specific numbers to stand. Your job is to record the standing students' numbers for each scenario.

Scenario 1

Students with numbers **starting** with the number **5** should stand. Record the numbers of the standing students.

Scenario 2

Students with numbers **ending** in **B** should stand. Record the numbers of the standing students.

Scenario 3

The student with the number **505C** should stand. Record the number of the standing student.

At the end of this activity, divide into small groups and record answers to the Reflection questions on the PDF for this activity.

Reflection

1. Why do you think you were asked to record the students' numbers when and as requested?

   ____

2. What is the significance of the number 5 in this activity? How many people were identified with this number?

   ____

3. What is the significance of the letter B in this activity? How many people were identified with this number?

   ____

4. Why did only one person stand for 505C?

   ____

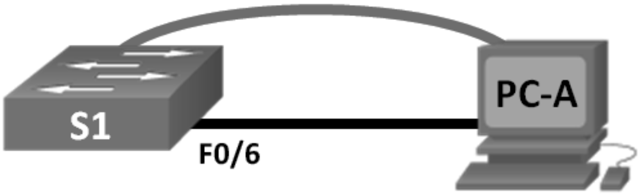
5. How do you think this activity represents data travelling on local area networks?

   ____

Save your work and be prepared to share it with another student or the entire class.

2.1.1.6 Lab – Configuring Basic Switch Settings

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 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 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?

   ____

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), 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? ________

How many Gigabit Ethernet interfaces does a 2960 switch have? ________

What is the range of values shown for the vty lines? ________

c. Examine the startup configuration file in NVRAM.

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

Why does this message appear? ____

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

```
Switch# show interface vlan1
```

Is there an IP address assigned to VLAN 1? ________

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

Is this interface up?

____

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

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

What output do you see?

____

____

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?

____

____

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

```
Switch# show version
```

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

What is the system image filename? ____

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

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

```
Switch# show interface f0/6
```

Is the interface up or down? ______________________

What event would make an interface go up? ____

What is the MAC address of the interface? ____________________________

What is the speed and duplex setting of the interface? _______________________

i. Examine the default VLAN settings of the switch.

```
Switch# show vlan
```

What is the default name of VLAN 1? ____________

Which ports are in this VLAN? ____

Is VLAN 1 active? ____________

What type of VLAN is the default VLAN? _______________

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? ____

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#
*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?

____

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.

l. 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? ____

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 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? ____________________

What is the VLAN 99 state? ___________

What is the line protocol state? ___________

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.

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.

____

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? ____________

How many MAC addresses are there in total? ____________

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

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? ____________

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? ____________

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 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? ____

How many dynamic addresses are there? ____

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? _________

Why did this change from the last display? ____

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? __________

How many static addresses are there? _____________

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.

```
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? ____________

Reflection

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

   ____

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

   ____

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

   ____

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

   ____

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#
```

a. 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#
```

b. 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
```

c. 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
```

d. 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.

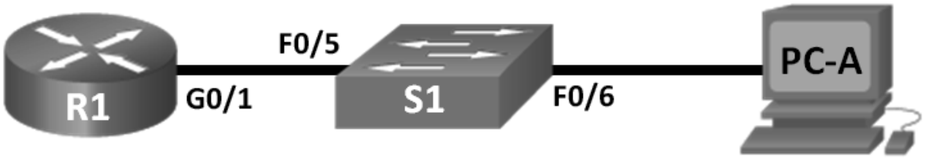
```
System configuration has been modified. Save? [yes/no]: no
```

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>
```

2.2.4.11 Lab – Configuring Switch Security Features

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Basic Device Settings and Verify Connectivity

Part 3: Configure and Verify SSH Access on S1

- Configure SSH access.
- Modify SSH parameters.
- Verify the SSH configuration.

Part 4: Configure and Verify Security Features on S1

- Configure and verify general security features.
- Configure and verify port security.

Background / Scenario

It is quite common to lock down access and install good security features on PCs and servers. It is important that your network infrastructure devices, such as switches and routers, are also configured with security features.

In this lab, you will follow some best practices for configuring security features on LAN switches. You will only allow SSH and secure HTTPS sessions. You will also configure and verify port security to lock out any device with a MAC address not recognized by the switch.

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

Note: Make sure that the router and switch have been erased and have no startup configurations. If you are unsure, contact your instructor or refer to the previous lab for the procedures to initialize and reload devices.

Required Resources

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

Part 1: Set Up the Topology and Initialize Devices

In Part 1, you will set up the network topology and clear any configurations if necessary.

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

Step 2: Initialize and reload the router and switch.

If configuration files were previously saved on the router or switch, initialize and reload these devices back to their basic configurations.

Part 2: Configure Basic Device Settings and Verify Connectivity

In Part 2, you configure basic settings on the router, switch, and PC. Refer to the Topology and Addressing Table at the beginning of this lab for device names and address information.

Step 1: Configure an IP address on PC-A.

Step 2: Configure basic settings on R1.

a. Configure the device name.

b. Disable DNS lookup.

c. Configure interface IP address as shown in the Addressing Table.

d. Assign **class** as the privileged EXEC mode password.

e. Assign **cisco** as the console and vty password and enable login.

f. Encrypt plain text passwords.

g. Save the running configuration to startup configuration.

Step 3: Configure basic settings on S1.

A good security practice is to assign the management IP address of the switch to a VLAN other than VLAN 1 (or any other data VLAN with end users). In this step, you will create VLAN 99 on the switch and assign it an IP address.

a. Configure the device name.

b. Disable DNS lookup.

c. Assign **class** as the privileged EXEC mode password.

d. Assign **cisco** as the console and vty password and then enable login.

e. Configure a default gateway for S1 using the IP address of R1.

f. Encrypt plain text passwords.

g. Save the running configuration to startup configuration.

h. Create VLAN 99 on the switch and name it **Management**.

```
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

i. Configure the VLAN 99 management interface IP address, as shown in the Addressing Table, and enable the interface.

```
S1(config)# interface vlan 99
S1(config-if)# ip address 172.16.99.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1#
```

j. Issue the **show vlan** command on S1. What is the status of VLAN 99? ______________________

k. Issue the **show ip interface brief** command on S1. What is the status and protocol for management interface VLAN 99?

____

Why is the protocol down, even though you issued the **no shutdown** command for interface VLAN 99?

____

l. Assign ports F0/5 and F0/6 to VLAN 99 on the switch.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# end
```

m. Issue the **show ip interface brief** command on S1. What is the status and protocol showing for interface VLAN 99? ____

Note: There may be a delay while the port states converge.

Step 4: Verify connectivity between devices.

a. From PC-A, ping the default gateway address on R1. Were your pings successful? _______________

b. From PC-A, ping the management address of S1. Were your pings successful? _______________

c. From S1, ping the default gateway address on R1. Were your pings successful? _______________

d. From PC-A, open a web browser and go to http://172.16.99.11. If it prompts you for a username and password, leave the username blank and use **class** for the password. If it prompts for secured connection, answer **No**. Were you able to access the web interface on S1? _______________

e. Close the browser session on PC-A.

Note: The non-secure web interface (HTTP server) on a Cisco 2960 switch is enabled by default. A common security measure is to disable this service, as described in Part 4.

Part 3: Configure and Verify SSH Access on S1

Step 1: Configure SSH access on S1.

a. Enable SSH on S1. From global configuration mode, create a domain name of **CCNA-Lab.com**.

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

b. Create a local user database entry for use when connecting to the switch via SSH. The user should have administrative level access.

Note: The password used here is NOT a strong password. It is merely being used for lab purposes.

```
S1(config)# username admin privilege 15 secret sshadmin
```

c. Configure the transport input for the vty lines to allow SSH connections only, and use the local database for authentication.

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

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

```
S1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

S1(config)#
S1(config)# end
```

e. Verify the SSH configuration and answer the questions below.

```
S1# show ip ssh
```

What version of SSH is the switch using? _______________________

How many authentication attempts does SSH allow? _______________________

What is the default timeout setting for SSH? _______________________

Step 2: Modify the SSH configuration on S1.

Modify the default SSH configuration.

```
S1# config t
S1(config)# ip ssh time-out 75
S1(config)# ip ssh authentication-retries 2
```

How many authentication attempts does SSH allow? _______________________

What is the timeout setting for SSH? _______________________

Step 3: Verify the SSH configuration on S1.

a. Using SSH client software on PC-A (such as Tera Term), open an SSH connection to S1. If you receive a message on your SSH client regarding the host key, accept it. Log in with **admin** for username and **cisco** for the password.

Was the connection successful? _________________________

What prompt was displayed on S1? Why?

____

____

____

b. Type **exit** to end the SSH session on S1.

Part 4: Configure and Verify Security Features on S1

In Part 4, you will shut down unused ports, turn off certain services running on the switch, and configure port security based on MAC addresses. Switches can be subject to MAC address table overflow attacks, MAC spoofing attacks, and unauthorized connections to switch ports. You will configure port security to limit the number of MAC addresses that can be learned on a switch port and disable the port if that number is exceeded.

Step 1: Configure general security features on S1.

a. Configure a message of the day (MOTD) banner on S1 with an appropriate security warning message.

b. Issue a **show ip interface brief** command on S1. What physical ports are up?

____

c. Shut down all unused physical ports on the switch. Use the **interface range** command.

```
S1(config)# interface range f0/1 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 - 2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

d. Issue the **show ip interface brief** command on S1. What is the status of ports F0/1 to F0/4?

____

e. Issue the **show ip http server status** command.

What is the HTTP server status? ____________________________

What server port is it using? ____________________________

What is the HTTP secure server status? ____________________________

What secure server port is it using? ____________________________

f. HTTP sessions send everything in plain text. You will disable the HTTP service running on S1.

```
S1(config)# no ip http server
```

g. From PC-A, open a web browser session to http://172.16.99.11. What was your result?

____

h. From PC-A, open a secure web browser session at https://172.16.99.11. Accept the certificate. Log in with no username and a password of **class**. What was your result?

____

i. Close the web session on PC-A.

Step 2: Configure and verify port security on S1.

a. Record the R1 G0/1 MAC address. From the R1 CLI, use the **show interface g0/1** command and record the MAC address of the interface.

```
R1# show interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia
3047.0da3.1821)
```

What is the MAC address of the R1 G0/1 interface?

____

b. From the S1 CLI, issue a **show mac address-table** command from privileged EXEC mode. Find the dynamic entries for ports F0/5 and F0/6. Record them below.

F0/5 MAC address: ____

F0/6 MAC address: ____

c. Configure basic port security.

Note: This procedure would normally be performed on all access ports on the switch. F0/5 is shown here as an example.

1) From the S1 CLI, enter interface configuration mode for the port that connects to R1.

```
S1(config)# interface f0/5
```

2) Shut down the port.

```
S1(config-if)# shutdown
```

3) Enable port security on F0/5.

```
S1(config-if)# switchport port-security
```

Note: Entering the **switchport port-security** command sets the maximum MAC addresses to 1 and the violation action to shutdown. The **switchport port-security maximum** and **switchport port-security violation** commands can be used to change the default behavior.

4) Configure a static entry for the MAC address of R1 G0/1 interface recorded in Step 2a.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

(xxxx.xxxx.xxxx is the actual MAC address of the router G0/1 interface)

Note: Optionally, you can use the `switchport port-security mac-address sticky` command to add all the secure MAC addresses that are dynamically learned on a port (up to the maximum set) to the switch running configuration.

5) Enable the switch port.

```
S1(config-if)# no shutdown
S1(config-if)# end
```

d. Verify port security on S1 F0/5 by issuing a **show port-security interface** command.

```
S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
```

```
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

What is the port status of F0/5?

e. From R1 command prompt, ping PC-A to verify connectivity.

```
R1# ping 172.16.99.3
```

f. You will now violate security by changing the MAC address on the router interface. Enter interface configuration mode for G0/1 and shut it down.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown
```

g. Configure a new MAC address for the interface, using **aaaa.bbbb.cccc** as the address.

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

h. If possible, have a console connection open on S1 at the same time that you do this step. You will see various messages displayed on the console connection to S1 indicating a security violation. Enable the G0/1 interface on R1.

```
R1(config-if)# no shutdown
```

i. From R1 privileged EXEC mode, ping PC-A. Was the ping successful? Why or why not?

j. On the switch, verify port security with the following commands shown below.

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
      Fa0/5            1           1                 1         Shutdown
----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192

S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : aaaa.bbbb.cccc:99
```

```
Security Violation Count   : 1

S1# show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>

S1# show port-security address
                Secure Mac Address Table
------------------------------------------------------------------------
Vlan     Mac Address       Type                 Ports      Remaining Age
                                                           (mins)
----     -----------       ----                 -----   -------------
  99     30f7.0da3.1821    SecureConfigured     Fa0/5         -
-----------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192
```

k. On the router, shut down the G0/1 interface, remove the hard-coded MAC address from the router, and re-enable the G0/1 interface.

```
R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown
R1(config-if)# end
```

l. From R1, ping PC-A again at 172.16.99.3. Was the ping successful? __________________

m. Issue the **show interface f0/5** command to determine the cause of ping failure. Record your findings.

____

n. Clear the S1 F0/5 error disabled status.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

Note: There may be a delay while the port states converge.

o. Issue the **show interface f0/5** command on S1 to verify F0/5 is no longer in error disabled mode.

```
S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

p. From the R1 command prompt, ping PC-A again. You should be successful.

Reflection

1. Why would you enable port security on a switch?

   ____

2. Why should unused ports on a switch be disabled?

   ____

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

2.3.1.1 Class Activity – Switch Trio

Objective

Verify the Layer 2 configuration of a switch port connected to an end station.

Scenario

You are the network administrator for a small- to medium-sized business. Corporate headquarters for your business has mandated that on all switches in all offices, security must be implemented. The memorandum delivered to you this morning states:

> *"By Monday, April 18, 20xx, the first three ports of all configurable switches located in all offices must be secured with MAC addresses — one address will be reserved for the printer, one address will be reserved for the laptop in the office, and one address will be reserved for the office server.*
>
> *If a port's security is breached, we ask you to shut it down until the reason for the breach can be certified.*
>
> *Please implement this policy no later than the date stated in this memorandum. For questions, call 1.800.555.1212. Thank you. The Network Management Team"*

Work with a partner in the class and create a Packet Tracer example to test this new security policy. Once you have created your file, test it with, at least, one device to ensure it is operational or validated.

Save your work and be prepared to share it with the entire class.

Reflection

1. Why would one port on a switch be secured on a switch using these scenario parameters (and not all the ports on the same switch)?

   ____

2. Why would a network administrator use a network simulator to create, configure, and validate a security plan, instead of using the small- to medium-sized business' actual, physical equipment?

   ____

Chapter 3 — VLANs

3.0.1.2 Class Activity – Vacation Station

Objective

Explain the purpose of VLANs in a switched network.

Scenario

You have purchased a three floor vacation home at the beach for rental purposes. The floor plan is identical on each floor. Each floor offers one digital television for renters to use.

According to the local Internet service provider, only three stations may be offered within a television package. It is your job to decide which television packages you offer your guests.

- Divide the class into groups of three students per group.
- Choose three different stations to make one subscription package for each floor of your rental home.
- Complete the PDF for this activity.

Share your completed group-reflection answers with the class.

Television Station Subscription Package – Floor 1		
Local News □	**Sports** □	**Weather** □
Home Improvement □	**Movies** □	**History** □
Television Station Subscription Package – Floor 2		
Local News □	**Sports** □	**Weather** □
Home Improvement □	**Movies** □	**History** □
Television Station Subscription Package – Floor 3		
Local News □	**Sports** □	**Weather** □
Home Improvement □	**Movies** □	**History** □

Reflection

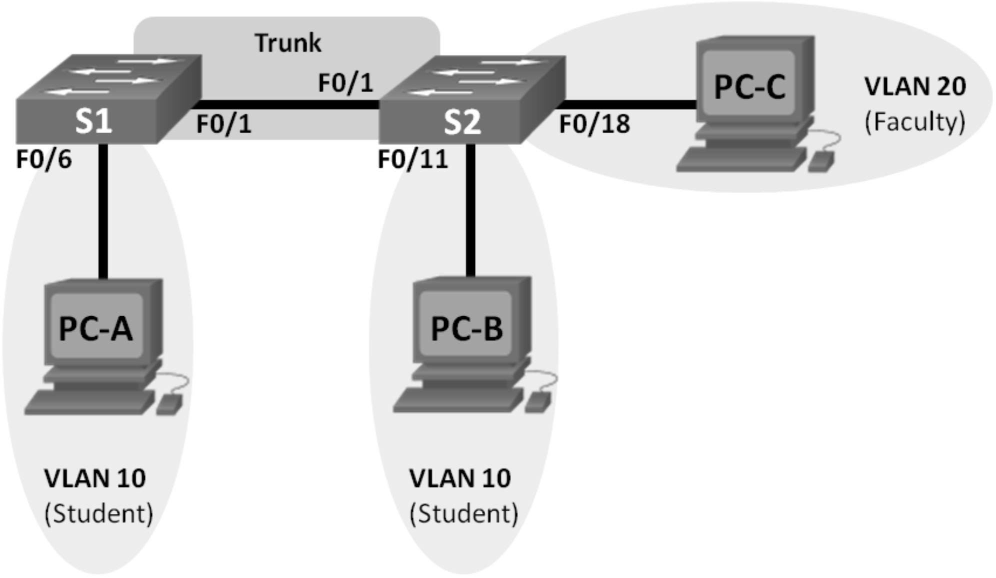
1. What were some of the criteria you used to select the final three stations?

2. Why do you think this Internet service provider offers different television station options to subscribers? Why not offer all stations to all subscribers?

3. Compare this scenario to data communications and networks for small- to medium-sized businesses. Why would it be a good idea to divide your small- to medium-sized business networks into logical and physical groups?

3.2.2.5 Lab - Configuring VLANs and Trunking

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Create VLANs and Assign Switch Ports

Part 3: Maintain VLAN Port Assignments and the VLAN Database

Part 4: Configure an 802.1Q Trunk between the Switches

Part 5: Delete the VLAN Database

Background / Scenario

Modern switches use virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones. VLANs can also be used as a security measure by controlling which hosts can communicate. In general, VLANs make it easier to design a network to support the goals of an organization.

VLAN trunks are used to span VLANs across multiple devices. Trunks allow the traffic from multiple VLANS to travel over a single link, while keeping the VLAN identification and segmentation intact.

In this lab, you will create VLANs on both switches in the topology, assign VLANs to switch access ports, verify that VLANs are working as expected, and then create a VLAN trunk between the two switches to allow hosts in the same VLAN to communicate through the trunk, regardless of which switch the host is actually attached to.

Note: The switches used are Cisco Catalyst 2960s 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: Ensure that the switches have been erased and have no startup configurations. If you are unsure contact your instructor.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and switches.

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

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

Step 2: Initialize and reload the switches as necessary.

Step 3: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure device name as shown in the topology.

c. Assign **class** as the privileged EXEC password.

d. Assign **cisco** as the console and vty passwords and enable login for console and vty lines.

e. Configure **logging synchronous** for the console line.

f. Configure a MOTD banner to warn users that unauthorized access is prohibited.

g. Configure the IP address listed in the Addressing Table for VLAN 1 on both switches.

h. Administratively deactivate all unused ports on the switch.

i. Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 5: Test connectivity.

Verify that the PC hosts can ping one another.

Note: It may be necessary to disable the PCs firewall to ping between PCs.

Can PC-A ping PC-B? __________

Can PC-A ping PC-C? __________

Can PC-A ping S1? __________

Can PC-B ping PC-C? __________

Can PC-B ping S2? __________

Can PC-C ping S2? __________

Can S1 ping S2? __________

If you answered no to any of the above questions, why were the pings unsuccessful?

____

____

Part 2: Create VLANs and Assign Switch Ports

In Part 2, you will create student, faculty, and management VLANs on both switches. You will then assign the VLANs to the appropriate interface. The **show vlan** command is used to verify your configuration settings.

Step 1: Create VLANs on the switches.

a. Create the VLANs on S1.

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# end
```

b. Create the same VLANs on S2.

c. Issue the **show vlan** command to view the list of VLANs on S1.

```
S1# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          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
10   Student                          active
20   Faculty                          active
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------



Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

What is the default VLAN? ___________

What ports are assigned to the default VLAN?

____

Step 2: Assign VLANs to the correct switch interfaces.

a. Assign VLANs to the interfaces on S1.

1) Assign PC-A to the Student VLAN.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

2) Move the switch IP address VLAN 99.

```
S1(config)# interface vlan 1
S1(config-if)# no ip address
S1(config-if)# interface vlan 99
```

```
    S1(config-if)# ip address 192.168.1.11 255.255.255.0
    S1(config-if)# end
```

b. Issue the **show vlan brief** command and verify that the VLANs are assigned to the correct interfaces.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, 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
10   Student                          active    Fa0/6
20   Faculty                          active
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

c. Issue the **show ip interface brief** command.

What is the status of VLAN 99? Why?

____

d. Use the Topology to assign VLANs to the appropriate ports on S2.

e. Remove the IP address for VLAN 1 on S2.

f. Configure an IP address for VLAN 99 on S2 according to the Addressing Table.

g. Use the **show vlan brief** command to verify that the VLANs are assigned to the correct interfaces.

```
S2# show vlan brief

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

Is PC-A able to ping PC-B? Why?

____

Is S1 able to ping S2? Why?

____

Part 3: Maintain VLAN Port Assignments and the VLAN Database

In Part 3, you will change VLAN assignments to ports and remove VLANs from the VLAN database.

Step 1: Assign a VLAN to multiple interfaces.

a. On S1, assign interfaces F0/11 – 24 to VLAN 10.

```
S1(config)# interface range f0/11-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# end
```

b. Issue the **show vlan brief** command to verify VLAN assignments.

c. Reassign F0/11 and F0/21 to VLAN 20.

d. Verify that VLAN assignments are correct.

Step 2: Remove a VLAN assignment from an interface.

a. Use the **no switchport access vlan** command to remove the VLAN 10 assignment to F0/24.

```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```

b. Verify that the VLAN change was made.

Which VLAN is F0/24 now associated with?

____

Step 3: Remove a VLAN ID from the VLAN database.

a. Add VLAN 30 to interface F0/24 without issuing the VLAN command.

```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

Note: Current switch technology no longer requires that the **vlan** command be issued to add a VLAN to the database. By assigning an unknown VLAN to a port, the VLAN adds to the VLAN database.

b. Verify that the new VLAN is displayed in the VLAN table.

```
S1# show vlan brief
```

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Gi0/1, Gi0/2
10   Student                          active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/22, Fa0/23
20   Faculty                          active    Fa0/11, Fa0/21
30   VLAN0030                         active    Fa0/24
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

What is the default name of VLAN 30?

c. Use the **no vlan 30** command to remove VLAN 30 from the VLAN database.

```
S1(config)# no vlan 30
S1(config)# end
```

d. Issue the **show vlan brief** command. F0/24 was assigned to VLAN 30.

After deleting VLAN 30, what VLAN is port F0/24 assigned to? What happens to the traffic destined to the host attached to F0/24?

```
S1# show vlan brief

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

e. Issue the **no switchport access vlan** command on interface F0/24.

f. Issue the **show vlan brief** command to determine the VLAN assignment for F0/24. To which VLAN is F0/24 assigned?

____

Note: Before removing a VLAN from the database, it is recommended that you reassign all the ports assigned to that VLAN.

Why should you reassign a port to another VLAN before removing the VLAN from the VLAN database?

____

____

____

Part 4: Configure an 802.1Q Trunk Between the Switches

In Part 4, you will configure interface F0/1 to use the Dynamic Trunking Protocol (DTP) to allow it to negotiate the trunk mode. After this has been accomplished and verified, you will disable DTP on interface F0/1 and manually configure it as a trunk.

Step 1: Use DTP to initiate trunking on F0/1.

The default DTP mode of a 2960 switch port is dynamic auto. This allows the interface to convert the link to a trunk if the neighboring interface is set to trunk or dynamic desirable mode.

a. Set F0/1 on S1 to negotiate trunk mode.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
*Mar  1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar  1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S1(config-if)#
*Mar  1 05:07:32.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S1(config-if)#
*Mar  1 05:08:01.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
*Mar  1 05:08:01.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

You should also receive link status messages on S2.

```
S2#
*Mar  1 05:07:29.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S2#
*Mar  1 05:07:32.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S2#
*Mar  1 05:08:01.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
*Mar  1 05:08:01.850: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

b. Issue the **show vlan brief** command on S1 and S2. Interface F0/1 is no longer assigned to VLAN 1. Trunked interfaces are not listed in the VLAN table.

```
S1# show vlan brief

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

c. Issue the **show interfaces trunk** command to view trunked interfaces. Notice that the mode on S1 is set to desirable, and the mode on S2 is set to auto.

```
S1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       desirable        802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99

S2# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       auto             802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

Note: By default, all VLANs are allowed on a trunk. The **switchport trunk** command allows you to control what VLANs have access to the trunk. For this lab, keep the default settings which allows all VLANs to traverse F0/1.

d. Verify that VLAN traffic is traveling over trunk interface F0/1.

Can S1 ping S2? ____________

Can PC-A ping PC-B? ____________

Can PC-A ping PC-C? ____________

Can PC-B ping PC-C? ____________

Can PC-A ping S1? ____________

Can PC-B ping S2? ____________

Can PC-C ping S2? ____________

If you answered no to any of the above questions, explain below.

____

____

Step 2: Manually configure trunk interface F0/1.

The **switchport mode trunk** command is used to manually configure a port as a trunk. This command should be issued on both ends of the link.

a. Change the switchport mode on interface F0/1 to force trunking. Make sure to do this on both switches.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Issue the **show interfaces trunk** command to view the trunk mode. Notice that the mode changed from **desirable** to **on**.

```
S2# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

Why might you want to manually configure an interface to trunk mode instead of using DTP?

____

____

Part 5: Delete the VLAN Database

In Part 5, you will delete the VLAN Database from the switch. It is necessary to do this when initializing a switch back to its default settings.

Step 1: Determine if the VLAN database exists.

Issue the **show flash** command to determine if a **vlan.dat** file exists in flash.

```
S1# show flash

Directory of flash:/

    2  -rwx        1285   Mar 1 1993 00:01:24 +00:00  config.text
    3  -rwx       43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
    4  -rwx           5   Mar 1 1993 00:01:24 +00:00  private-config.text
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
    6  -rwx         736   Mar 1 1993 00:19:41 +00:00  vlan.dat

32514048 bytes total (20858880 bytes free)
```

Note: If there is a **vlan.dat** file located in flash, then the VLAN database does not contain its default settings.

Step 2: Delete the VLAN database.

a. Issue the **delete vlan.dat** command to delete the vlan.dat file from flash and reset the VLAN database back to its default settings. You will be prompted twice to confirm that you want to delete the vlan.dat file. Press Enter both times.

```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
S1#
```

b. Issue the **show flash** command to verify that the vlan.dat file has been deleted.

```
S1# show flash

Directory of flash:/

    2  -rwx        1285   Mar 1 1993 00:01:24 +00:00  config.text
    3  -rwx       43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
    4  -rwx           5   Mar 1 1993 00:01:24 +00:00  private-config.text
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin

32514048 bytes total (20859904 bytes free)
```

To initialize a switch back to its default settings, what other commands are needed?

____

____

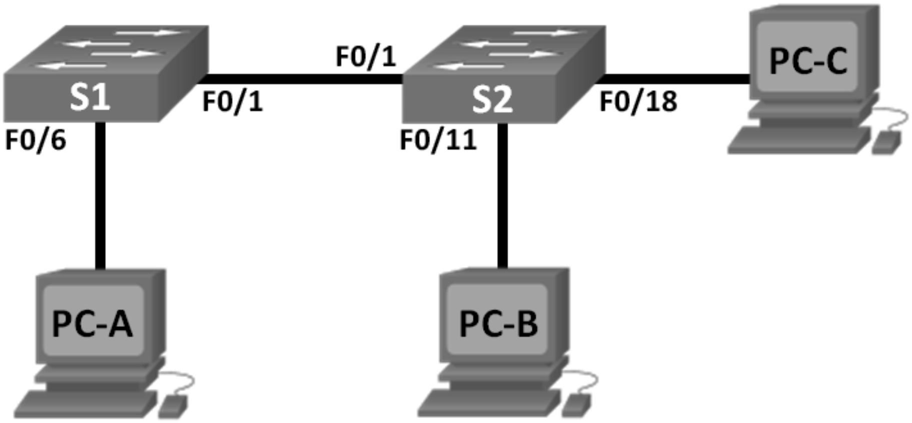
Reflection

1. What is needed to allow hosts on VLAN 10 to communicate to hosts on VLAN 20?

2. What are some primary benefits that an organization can receive through effective use of VLANs?

3.2.4.9 Lab - Troubleshooting VLAN Configurations

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
S2	VLAN 1	192.168.1.3	255.255.255.0	N/A
PC-A	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Switch Port Assignment Specifications

Ports	Assignment	Network
F0/1	802.1Q Trunk	N/A
F0/6-12	VLAN 10 – Students	192.168.10.0/24
F0/13-18	VLAN 20 – Faculty	192.168.20.0/24
F0/19-24	VLAN 30 – Guest	192.168.30.0/24

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot VLAN 10

Part 3: Troubleshoot VLAN 20

Background / Scenario

VLANs provide logical segmentation within an internetwork and improve network performance by separating large broadcast domains into smaller ones. By separating hosts into different networks, VLANs can be used to control which hosts can communicate. In this lab, a school has decided to implement VLANs in order to separate traffic from different end users. The school is using 802.1Q trunking to facilitate VLAN communication between switches.

The S1 and S2 switches have been configured with VLAN and trunking information. Several errors in the configuration have resulted in connectivity issues. You have been asked to troubleshoot and correct the configuration errors and document your work.

Note: The switches used with this lab are Cisco Catalyst 2960s 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 switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the switches with some basic settings, such as passwords and IP addresses. Preset VLAN-related configurations, which contain errors, are provided for you for the initial switch configurations. You will also configure the IP settings for the PCs in the topology.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the switches as necessary.

Step 4: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure the IP address according to the Addressing Table.

c. Assign **cisco** as the console and vty passwords and enable login for console and vty lines.

d. Assign **class** as the privileged EXEC password.

e. Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 5: Load switch configurations.

The configurations for the switches S1 and S2 are provided for you. There are errors within these configurations, and it is your job to determine the incorrect configurations and correct them.

Switch S1 Configuration:

```
hostname S1
vlan 10
 name Students
```

```
vlan 2

name Faculty
vlan 30
 name Guest
interface range f0/1-24
 switchport mode access
 shutdown



interface range f0/7-12

 switchport access vlan 10
interface range f0/13-18
 switchport access vlan 2

interface range f0/19-24
 switchport access vlan 30
end
```

Switch S2 Configuration:

```
hostname S2
vlan 10
 name Students
vlan 20
 name Faculty
vlan 30
 name Guest
interface f0/1
 switchport mode trunk
 switchport trunk allowed vlan 1,10,2,30

interface range f0/2-24
 switchport mode access
 shutdown


interface range f0/13-18
 switchport access vlan 20
interface range f0/19-24
 switchport access vlan 30
 shutdown
end
```

Step 6: Copy the running configuration to the startup configuration.

Part 2: Troubleshoot VLAN 10

In Part 2, you must examine VLAN 10 on S1 and S2 to determine if it is configured correctly. You will troubleshoot the scenario until connectivity is established.

Step 1: Troubleshoot VLAN 10 on S1.

a. Can PC-A ping PC-B? _______________

b. After verifying that PC-A was configured correctly, examine the S1 switch to find possible configuration errors by viewing a summary of the VLAN information. Enter the **show vlan brief** command.

c. Are there any problems with the VLAN configuration?

____

d. Examine the switch for trunk configurations using the **show interfaces trunk** and the **show interfaces f0/1 switchport** commands.

e. Are there any problems with the trunking configuration?

____

f. Examine the running configuration of the switch to find possible configuration errors.

Are there any problems with the current configuration?

____

g. Correct the errors found regarding F0/1 and VLAN 10 on S1. Record the commands used in the space below.

____

____

____

____

h. Verify the commands had the desired effects by issuing the appropriate **show** commands.

i. Can PC-A ping PC-B? _______________

Step 2: Troubleshoot VLAN 10 on S2.

a. Using the previous commands, examine the S2 switch to find possible configuration errors.

Are there any problems with the current configuration?

____

b. Correct the errors found regarding interfaces and VLAN 10 on S2. Record the commands below.

____

____

____

____

____

____

c. Can PC-A ping PC-B? _______________

Part 3: Troubleshoot VLAN 20

In Part 3, you must examine VLAN 20 on S1 and S2 to determine if it is configured correctly. To verify functionality, you will reassign PC-A into VLAN 20, and then troubleshoot the scenario until connectivity is established.

Step 1: Assign PC-A to VLAN 20.

a. On PC-A, change the IP address to 192.168.20.2/24 with a default gateway of 192.168.20.1.

b. On S1, assign the port for PC-A to VLAN 20. Write the commands needed to complete the configuration.

____

____

c. Verify that the port for PC-A has been assigned to VLAN 20.

d. Can PC-A ping PC-C? ______________

Step 2: Troubleshoot VLAN 20 on S1.

a. Using the previous commands, examine the S1 switch to find possible configuration errors.

Are there any problems with the current configuration?

____

____

a. Correct the errors found regarding VLAN 20.

b. Can PC-A ping PC-C? ______________

Step 3: Troubleshoot VLAN 20 on S2.

a. Using the previous commands, examine the S2 switch to find possible configuration errors.

Are there any problems with the current configuration?

____

b. Correct the errors found regarding VLAN 20. Record the commands used below.

____

____

____

____

____

c. Can PC-A ping PC-C? ______________

Note: It may be necessary to disable the PC firewall to ping between PCs.

Reflection

1. Why is a correctly configured trunk port critical in a multi-VLAN environment?

____

____

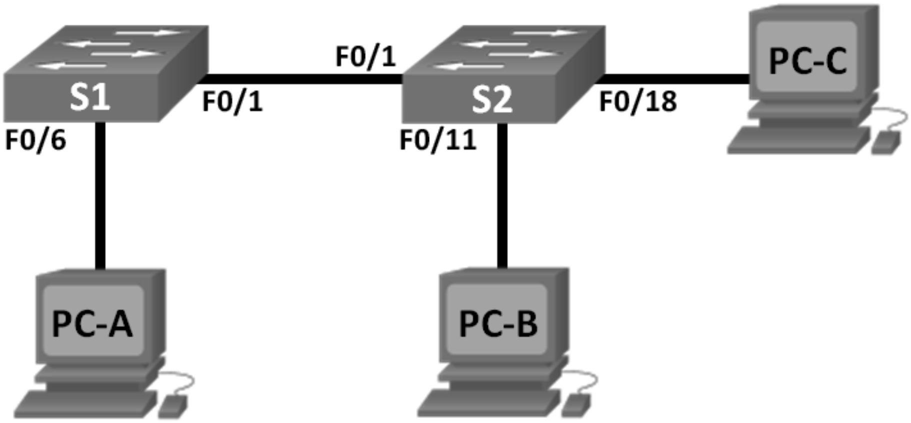
2. Why would a network administrator limit traffic for specific VLANs on a trunk port?

____

____

3.3.2.2 Lab – Implementing VLAN Security

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
PC-A	NIC	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	NIC	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	NIC	172.17.99.4	255.255.255.0	172.17.99.1

VLAN Assignments

VLAN	Name
10	Data
99	Management&Native
999	BlackHole

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Implement VLAN Security on the Switches

Background / Scenario

Best practice dictates configuring some basic security settings for both access and trunk ports on switches. This will help guard against VLAN attacks and possible sniffing of network traffic within the network.

In this lab, you will configure the network devices in the topology with some basic settings, verify connectivity and then apply more stringent security measures on the switches. You will examine how Cisco switches behave by using various **show** commands. You will then apply security measures.

Note: The switches used with this lab are Cisco Catalyst 2960s 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 switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will configure basic settings on the switches and PCs. Refer to the Addressing Table for device names and address information.

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

Step 2: Initialize and reload the switches.

Step 3: Configure IP addresses on PC-A, PC-B, and PC-C.

Refer to the Addressing Table for PC address information.

Step 4: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure the device names as shown in the topology.

c. Assign **class** as the privileged EXEC mode password.

d. Assign **cisco** as the console and VTY password and enable login for console and vty lines.

e. Configure synchronous logging for console and vty lines.

Step 5: Configure VLANs on each switch.

a. Create and name VLANs according to the VLAN Assignments table.

b. Configure the IP address listed in the Addressing Table for VLAN 99 on both switches.

c. Configure F0/6 on S1 as an access port and assign it to VLAN 99.

d. Configure F0/11 on S2 as an access port and assign it to VLAN 10.

e. Configure F0/18 on S2 as an access port and assign it to VLAN 99.

f. Issue **show vlan brief** command to verify VLAN and port assignments.

To which VLAN would an unassigned port, such as F0/8 on S2, belong?

____

Step 6: Configure basic switch security.

a. Configure a MOTD banner to warn users that unauthorized access is prohibited.

b. Encrypt all passwords.

c. Shut down all unused physical ports.

d. Disable the basic web service running.

```
S1(config)# no ip http server
S2(config)# no ip http server
```

e. Copy the running configuration to startup configuration.

Step 6: Verify connectivity between devices and VLAN information.

a. From a command prompt on PC-A, ping the management address of S1. Were the pings successful? Why?

____

____

b. From S1, ping the management address of S2. Were the pings successful? Why?

____

____

c. From a command prompt on PC-B, ping the management addresses on S1 and S2 and the IP address of PC-A and PC-C. Were your pings successful? Why?

____

____

d. From a command prompt on PC-C, ping the management addresses on S1 and S2. Were you successful? Why?

____

____

Note: It may be necessary to disable the PC firewall to ping between PCs.

Part 2: Implement VLAN Security on the Switches

Step 1: Configure trunk ports on S1 and S2.

a. Configure port F0/1 on S1 as a trunk port.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Configure port F0/1 on S2 as a trunk port.

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

c. Verify trunking on S1 and S2. Issue the **show interface trunk** command on both switches.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

Step 2: Change the native VLAN for the trunk ports on S1 and S2.

Changing the native VLAN for trunk ports from VLAN 1 to another VLAN is a good practice for security.

a. What is the current native VLAN for the S1 and S2 F0/1 interfaces?

____

b. Configure the native VLAN on the S1 F0/1 trunk interface to Management&Native VLAN 99.

```
S1# config t
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 99
```

c. Wait a few seconds. You should start receiving error messages on the console session of S1. What does the %CDP-4-NATIVE_VLAN_MISMATCH: message mean?

____

d. Configure the native VLAN on the S2 F0/1 trunk interface to VLAN 99.

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
```

e. Verify that the native VLAN is now 99 on both switches. S1 output is shown below.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
```

```
Fa0/1       1,10,99,999

Port         Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,999
```

Step 3: Verify that traffic can successfully cross the trunk link.

a. From a command prompt on PC-A, ping the management address of S1. Were the pings successful? Why?

b. From the console session on S1, ping the management address of S2. Were the pings successful? Why?

c. From a command prompt on PC-B, ping the management addresses on S1 and S2 and the IP address of PC-A and PC-C. Were your pings successful? Why?

d. From a command prompt on PC-C, ping the management addresses on S1 and S2 and the IP address of PC-A. Were you successful? Why?

Step 4: Prevent the use of DTP on S1 and S2.

Cisco uses a proprietary protocol known as the Dynamic Trunking Protocol (DTP) on its switches. Some ports automatically negotiate to trunking. A good practice is to turn off negotiation. You can see this default behavior by issuing the following command:

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

a. Turn off negotiation on S1.

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
```

b. Turn off negotiation on S2.

```
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

c. Verify that negotiation is off by issuing the **show interface f0/1 switchport** command on S1 and S2.

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
<Output Omitted>
```

Step 5: Secure access ports on S1 and S2.

Even though you shut down unused ports on the switches, if a device is connected to one of those ports and the interface is enabled, trunking could occur. In addition, all ports by default are in VLAN 1. A good practice is to put all unused ports in a “black hole” VLAN. In this step, you will disable trunking on all unused ports. You will also assign unused ports to VLAN 999. For the purposes of this lab, only ports 2 through 5 will be configured on both switches.

a. Issue the **show interface f0/2 switchport** command on S1. Notice the administrative mode and state for trunking negotiation.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

b. Disable trunking on S1 access ports.

```
S1(config)# interface range f0/2 - 5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
```

c. Disable trunking on S2 access ports.

d. Verify that port F0/2 is set to access on S1.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<Output Omitted>
```

e. Verify that VLAN port assignments on both switches are correct. S1 is shown below as an example.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- ------------------------------ --------- ------------------------------
1    default                          active    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
10   Data                             active
99   Management&Native                active    Fa0/6
999  BlackHole                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                       act/unsup
1003 token-ring-default                 act/unsup
1004 fddinet-default                    act/unsup
1005 trnet-default                      act/unsup
Restrict VLANs allowed on trunk ports.
```

By default, all VLANs are allowed to be carried on trunk ports. For security reasons, it is a good practice to only allow specific desired VLANs to cross trunk links on your network.

f. Restrict the trunk port F0/1 on S1 to only allow VLANs 10 and 99.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,99
```

g. Restrict the trunk port F0/1 on S2 to only allow VLANs 10 and 99.

h. Verify the allowed VLANs. Issue a **show interface trunk** command in privileged EXEC mode on both S1 and S2.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,99
```

What is the result?

Reflection

What, if any, are the security problems with the default configuration of a Cisco switch?

____

____

____

____

3.4.1.1 Class Activity – VLAN Plan

Objective

Implement VLANs to segment a small- to medium-sized network.

Scenario

You are designing a VLAN switched network for your small- to medium- sized business.

Your business owns space on two floors of a high-rise building. The following elements need VLAN consideration and access for planning purposes:

- Management
- Finance
- Sales
- Human Resources
- Network administrator
- General visitors to your business location

You have two Cisco 3560-24PS switches.

Use a word processing software program to design your VLAN-switched network scheme.

Section 1 of your design should include the regular names of your departments, suggested VLAN names and numbers, and which switch ports would be assigned to each VLAN.

Section 2 of your design should list how security would be planned for this switched network.

Once your VLAN plan is finished, complete the reflection questions from this activity.

Save your work. Be able to explain and discuss your VLAN design with another group or with the class.

Required Resources

Word processing program

Reflection

1. What criteria did you use for assigning ports to the VLANs?

   ____

2. How could these users access your network if the switches were not physically available to general users via direct connection?

   ____

3. Could you reduce the number of switch ports assigned for general users if you used another device to connect them to the VLAN network switch? What would be affected?

   ____