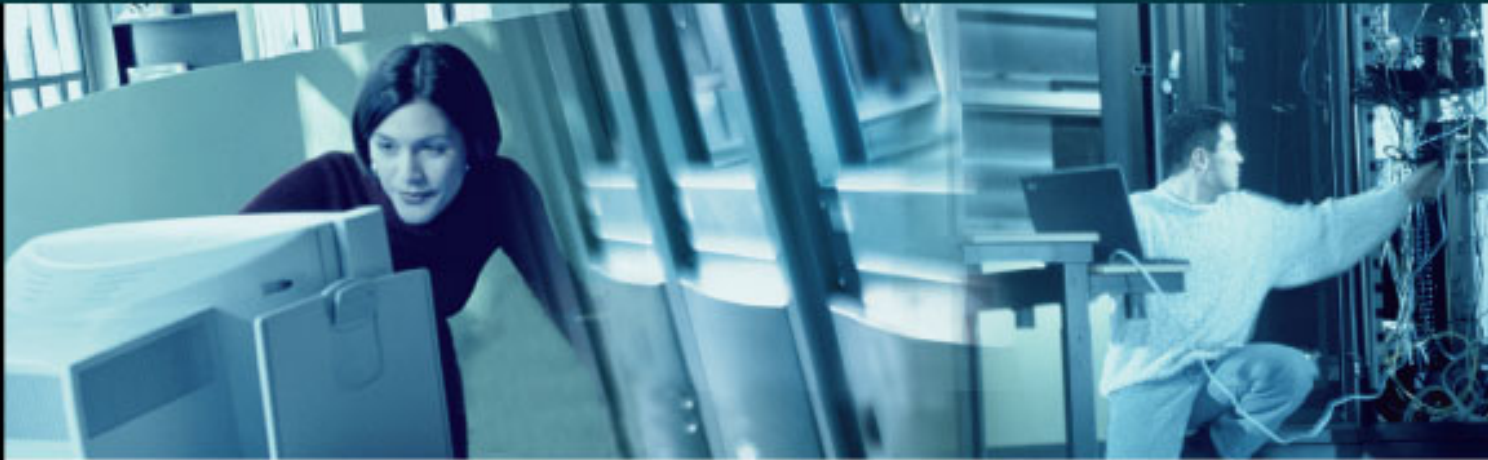




CISCO NETWORKING ACADEMY PROGRAM

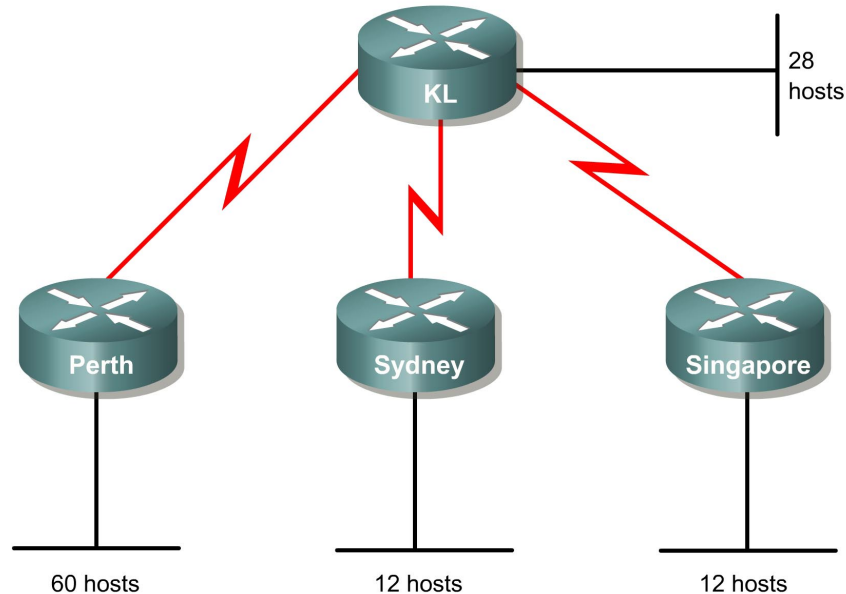


CCNA 3: Switching Basics and Intermediate Routing v3.1.1 Student Lab Manual

This document is exclusive property of Cisco Systems, Inc. Permission is granted to print and copy this document for non-commercial distribution and exclusive use by instructors in the CCNA 3: Switching Basics and Intermediate Routing course as part of an official Cisco Networking Academy



Lab 1.1.4 Calculating VLSM Subnets



Objective

Use variable-length subnet mask (VLSM) to support more efficient use of the assigned IP addresses and to reduce the amount of routing information at the top level.

Background/Preparation

A class C address of 192.168.10.0/24 has been allocated.

Perth, Sydney, and Singapore have a WAN connection to Kuala Lumpur.

- Perth requires 60 hosts.
- Kuala Lumpur requires 28 hosts.
- Sydney and Singapore each require 12 hosts.

To calculate VLSM subnets and the respective hosts allocate the largest requirements first from the address range. Requirements levels should be listed from the largest to the smallest.

In this example Perth requires 60 hosts. Use 6 bits since $2^6 - 2 = 62$ usable host addresses. Thus 2 bits will be used from the 4th octet to represent the extended-network-prefix of /26 and the remaining 6 bits will be used for host addresses.

Step 1

The first step in the subnetting process is to divide the allocated address of 192.168.10.0/24 into four equal size address blocks. Since $4 = 2^2$, 2 bits are required to identify each of the 4 subnets.

Next, take subnet #0 (192.168.10.0/26) and identify each of its hosts.

Allocated Address	Sub-networks	62 usable hosts/sub-network (subnet #0)
192.168.10.0/24	192.168.10.0/26	192.168.10.0/26 (Network Address)
	192.168.10.64/26	192.168.10.1/26
	192.168.10.128/26	192.168.10.2/26
	192.168.10.192/26	192.168.10.3/26
		thru
		192.168.10.61/26
		192.168.10.62/26
		192.168.10.63/26 (Broadcast Address)

Here is the range for the /26 mask.

Perth	Range of addresses in the last octet
192.168.10.0/26	From 0 to 63, 60 hosts required. Hosts 0 and 63 cannot be used because they are the network and broadcast addresses for their subnet.

Step 2

Allocate the next level after all the requirements are met for the higher level or levels.

Kuala Lumpur requires 28 hosts. The next available address after 192.168.10.63/26 is 192.168.10.64/26. Note from the above table that this is subnet number 1. Since 28 hosts are required, 5 bits will be needed for the host addresses, $2^5 - 2 = 30$ usable host addresses. Thus 5 bits will be required to represent the hosts and 3 bits will be used to represent the extended-network-prefix of /27. Applying VLSM on address 192.168.10.64/26 gives:

Sub-network #1	Sub-sub-networks	30 usable hosts
		192.168.10.64/27 (Network Address)
192.168.10.64/26	192.168.10.64/27	192.168.10.65/27
	192.168.10.96/27	192.168.10.66/27
		192.168.10.67/26
		thru
		192.168.10.93/27
		192.168.10.94/27
		192.168.10.95/27 (Broadcast Address)

Here is the range for the /27 mask.

Kuala Lumpur	Range of addresses in the last octet
192.168.10.64/27	From 64 to 95, 28 hosts required. Hosts 64 and 95 cannot be used because they are the network and broadcast addresses for their subnet. Thirty usable addresses are available in this range for the hosts.

Step 3

Now Sydney and Singapore require 12 hosts each. The next available address starts from 192.168.10.96/27. Note from Table 2 that this is the next subnet available. Since 12 hosts are required, 4 bits will be needed for the host addresses, $2^4 = 16$, $16 - 2 = 14$ usable addresses. Thus 4 bits are required to represent the hosts and 4 bits for the extended-network-prefix of /28. Applying VLSM on address 192.168.10.96/27 gives:

Sub-network	Sub-sub-networks	14 usable hosts
192.168.10.96/27	192.168.10.96/28	192.168.10.96/28 (Network Address)
	192.168.10.112/28	192.168.10.97/28
		192.168.10.98/28
		192.168.10.99/28
		thru
		192.168.10.109/28
		192.168.10.110/28
		192.168.10.111/28 (Broadcast Address)

Here is the range for the /28 mask.

Sydney	Range of addresses in the last octet
192.168.10.96/28	From 96 to 111, 12 hosts required. Hosts 96 and 111 cannot be used because they are network and broadcast addresses for their subnet. Fourteen useable addresses are available in this range for the hosts.

Step 4

Since Singapore also requires 12 hosts, the next set of host addresses can be derived from the next available subnet (192.168.10.112/28).

Sub-sub-networks	14 usable hosts
192.168.10.96/28	192.168.10.112/28 (Network Address)
192.168.10.112/28	192.168.10.113/28
192.168.10.128/28	192.168.10.114/28
192.168.10.224/28	192.168.10.115/28
	Thru
192.168.10.240/28	192.168.10.125/28
	192.168.10.126/28
	192.168.10.127/28 (Broadcast Address)

Here is the range for the /28 mask.

Singapore	Range of addresses in the last octet
192.168.10.112/28	From 112 to 127, 12 hosts required. Hosts 112 and 127 cannot be used because they are network and broadcast addresses for their subnet. Fourteen usable addresses are available in this range for the hosts.

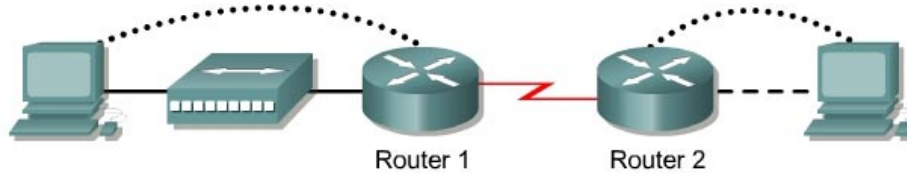
Step 5

Now allocate addresses for the WAN links. Remember that each WAN link will require two IP addresses. The next available subnet is 192.168.10.128/28. Since 2 network addresses are required for each WAN link, 2 bits will be needed for host addresses, $2^2 - 2 = 2$ usable addresses. Thus 2 bits are required to represent the links and 6 bits for the extended-network-prefix of /30. Applying VLSM on 192.168.10.128/28 gives:

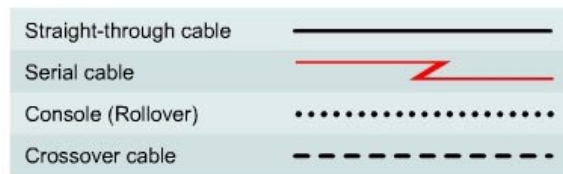
Sub-sub-networks	14 usable hosts
192.168.10.128/30	192.168.10.128/30(Network Address)
	192.168.10.129/30
	192.168.10.130/30
	192.168.10.131/30 (Broadcast Address)
192.168.10.132/30	192.168.10.132/30(Network Address)
	192.168.10.133/30
	192.168.10.134/30
	192.168.10.135/30 (Broadcast Address)
192.168.10.136/30	192.168.10.136/30 (Network Address)
	192.168.10.137/30
	192.168.10.138/30
	192.168.10.139/30 (Broadcast Address)

The available addresses for the WAN links can be taken from the available addresses in each of the /30 subnets.

Lab 1.2.3 Review of Basic Router Configuration with RIP



Router Designation	Router Name	FastEthernet 0 Address	Interface Type	Serial 0 Address	Subnet Mask for Both Interfaces	Enable Secret Password	Enable, VTY, and Console Passwords
Router 1	GAD	172.16.0.1	DCE	172.17.0.1	255.255.0.0	class	cisco
Router 2	BHM	172.18.0.1	DTE	172.17.0.2	255.255.0.0	class	cisco



Objective

- Cable and configure workstations and routers
- Setup IP addressing scheme using Class B networks
- Configure Routing Information Protocol (RIP) on routers

Background / Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 2500, and 2600 or any such combination can be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. Perform the following steps on each router unless specifically instructed otherwise.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

General Configuration Tips

- Use the question mark (?) and arrow keys to help enter commands.
- Each command mode restricts the set of available commands. If there is difficulty entering a command, check the prompt and then enter the question mark (?) for a list of available commands. The problem might be a wrong command mode or using the wrong syntax.
- To disable a feature, enter the keyword `no` before the command. For example, `no ip routing`.

- d. Save the configuration changes to NVRAM so that the changes are not lost if there is a system reload or power outage.

Router Command Modes			
Command Mode	Access Method	Router Prompt Displayed	Exit Method
User EXEC	Log in.	Router>	Use the <code>logout</code> command.
Privileged EXEC	From user EXEC mode, enter the <code>enable</code> command.	Router#	To exit to user EXEC mode, use the <code>disable</code> , <code>exit</code> , or <code>logout</code> command.
Global configuration	From the privileged EXEC mode, enter the <code>configure terminal</code> command.	Router(config)#	To exit to privileged EXEC mode, use the <code>exit</code> or <code>end</code> command, or press Ctrl-z .
Interface configuration	From the global configuration mode, enter the <code>interface type number</code> command, such as <code>interface serial 0</code> .	Router(config-if)#	To exit to global configuration mode, use the <code>exit</code> command.

Step 1 Basic router configuration

Connect a rollover cable to the console port on the router and the other end to the PC with a DB9 or DB25 adapter to a COM port. This should be completed prior to powering on of any devices.

Step 2 Start HyperTerminal program

- a. Turn on the computer and router.
- b. From the Windows taskbar, locate the HyperTerminal program:
Start > Programs > Accessories > Communications > HyperTerminal

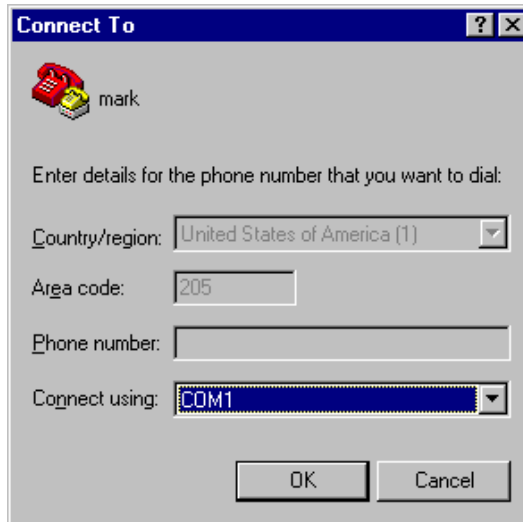
Step 3 Name the HyperTerminal Session

- a. At the “Connection Description” popup, enter a name in the connection *Name:* field and select **OK**.



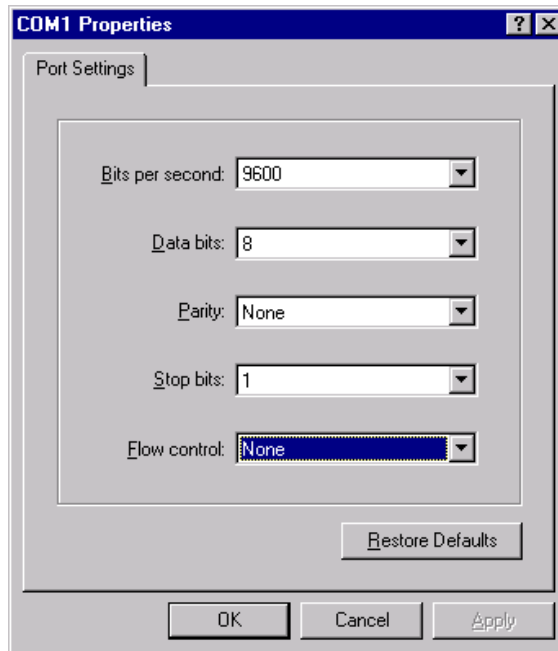
Step 4 Specify the computer connecting interface

- a. At the “Connect To” popup, use the drop down arrow in the *Connect using:* field to select **COM1** and select **OK**.

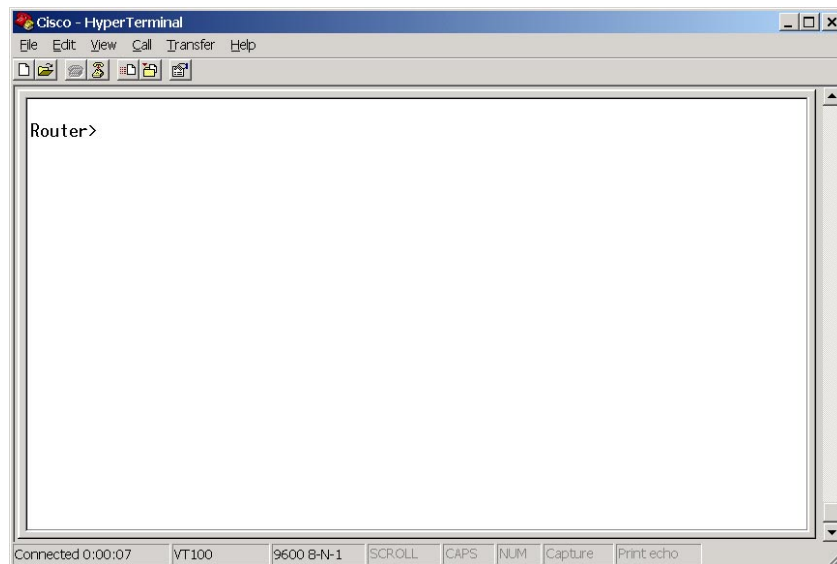


Step 5 Specify the interface connection properties

- a. At the “COM1 Properties” popup, use the drop down arrows to select:
 - Bits per second: **9600**
 - Data bits: **8**
 - Parity: **None**
 - Stop bits: **1**
 - Flow control: **None**
- b. Then select **OK**.



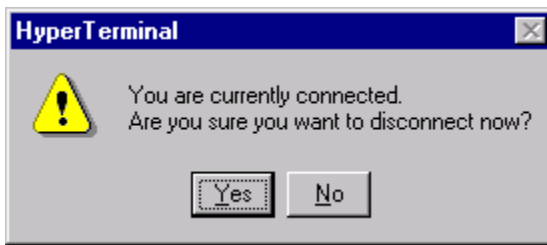
- c. When the HyperTerminal session window comes up, turn on the router or if router is already on, press the **Enter** key. There should be a response from the router.



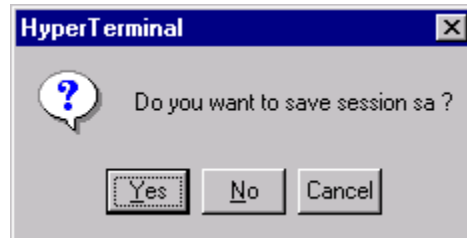
If the router responds, then the connection has been successfully completed.

Step 6 Closing the Session

- a. To end the console session from a HyperTerminal session, select:
File > Exit
- b. When the HyperTerminal disconnect warning popup appears, select **Yes**.

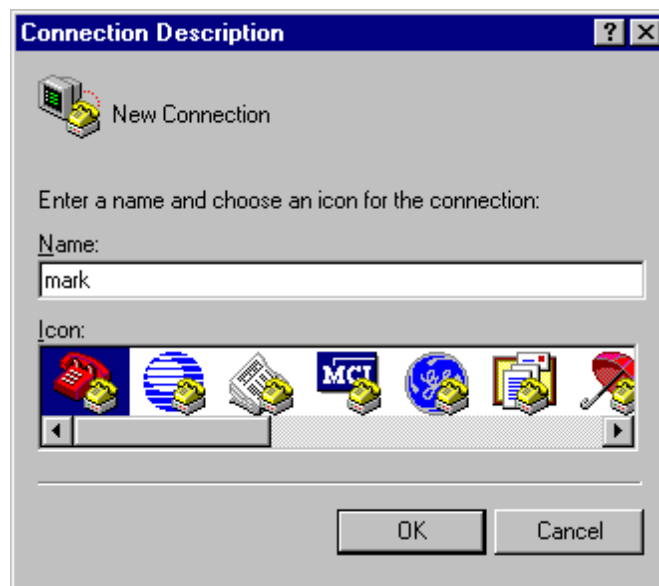


- c. The computer will then ask if the session is to be saved. Select **Yes**.



Step 7 Reopen the HyperTerminal connection, as shown in Step 2

- a. At the "Connection Description" popup, select **Cancel**.



- b. To open the saved console session from HyperTerminal, select:
File > Open
- c. The saved session will now appear and by double-clicking on the name, the connection will open without reconfiguring it each time.

Step 8 Configure the hostname and passwords on the router GAD

- a. Enter `enable` at the user mode prompt.

```
Router>enable
Router#configure terminal
Router (config)#hostname GAD
```

```
GAD(config)#enable secret class
GAD(config)#line console 0
GAD(config-line)#password cisco
GAD(config-line)#login
GAD(config-line)#line vty 0 4
GAD(config-line)#password cisco
GAD(config-line)#login
GAD(config-line)#exit
GAD(config)#
```

Step 9 Configure serial interface Serial 0 on router GAD

- a. From the global configuration mode, configure interface Serial 0 on router GAD. Refer to the interface chart.

```
GAD(config)#interface serial 0
GAD(config-if)#ip address 172.17.0.1 255.255.0.0
GAD(config-if)#clock rate 64000
GAD(config-if)#no shutdown
GAD(config-if)#exit
```

Step 10 Configure the fastethernet 0 interface on router GAD

```
GAD(config)#interface fastethernet 0
GAD(config-if)#ip address 172.16.0.1 255.255.0.0
GAD(config-if)#no shutdown
GAD(config-if)#exit
```

Step 11 Configure the IP host statements on router GAD

```
GAD(config)#ip host BHM 172.18.0.1 172.17.0.2
```

Step 12 Configure RIP routing on router GAD

```
GAD(config)#router rip
GAD(config-router)#network 172.16.0.0
GAD(config-router)#network 172.17.0.0
GAD(config-router)#exit
GAD(config)#exit
```

Step 13 Save the GAD router configuration

```
GAD#copy running-config startup-config
Destination filename [startup-config]? [Enter]
```

Step 14 Configure hostname and passwords on the router BHM

- a. Enter **enable** at the user mode prompt.

```
Router>enable
Router#configure terminal
Router(config)#hostname BHM
BHM(config)#enable secret class
BHM(config)#line console 0
BHM(config-line)#password cisco
BHM(config-line)#login
BHM(config-line)#line vty 0 4
BHM(config-line)#password cisco
BHM(config-line)#login
BHM(config-line)#exit
BHM(config)#
```

Step 15 Configure serial interface Serial 0 on router BHM

- a. From the global configuration mode, configure interface Serial 0 on router BHM. Refer to interface chart.

```
BHM(config)#interface serial 0
BHM(config-if)#ip address 172.17.0.2 255.255.0.0
BHM(config-if)#no shutdown
BHM(config-if)#exit
```

Step 16 Configure the fastethernet 0 interface on router BHM

```
BHM(config)#interface fastethernet 0
BHM(config-if)#ip address 172.18.0.1 255.255.0.0
BHM(config-if)#no shutdown
BHM(config-if)#exit
```

Step 17 Configure the IP host statements on router BHM

```
BHM(config)#ip host GAD 172.16.0.1 172.17.0.1
```

Step 18 Configure RIP routing on router BHM

```
BHM(config)#router rip
BHM(config-router)#network 172.18.0.0
BHM(config-router)#network 172.17.0.0
BHM(config-router)#exit
BHM(config)#exit
```

Step 19 Save the BHM router configuration

```
BHM#copy running-config startup-config
Destination filename [startup-config]? [Enter]
```

Step 20 Configure the hosts with the proper IP address, subnet mask, and default gateway

- a. Host connected to router GAD
 - IP Address: 172.16.0.2
 - Subnet mask: 255.255.0.0
 - Default gateway: 172.16.0.1

- b. Host connected to router BHM
 - IP Address: 172.18.0.2
 - Subnet mask: 255.255.0.0
 - Default gateway: 172.18.0.1

Step 21 Verify that the internetwork is functioning by pinging the Fast Ethernet interface of the other router

- a. From the host attached to GAD, ping the BHM router Fast Ethernet interface. Was the ping successful? _____
- b. From the host attached to BHM, ping the GAD router Fast Ethernet interface. Was the ping successful? _____
- c. If the answer is no for either question, troubleshoot the router configurations to find the error. Then do the pings again until the answer to both questions is yes. Then ping all interfaces in the network.

Step 22 Show the routing tables for each router

- a. From the enable privileged EXEC mode:
 - Examine the routing table entries, using the `show ip route` command on each router.
- b. What are the entries in the GAD routing table?

- c. What are the entries in the BHM routing table?

Once the previous steps are completed, logoff by typing `exit`, and turn the router off. Then remove and store the cables and adapter.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

```
Router>enable
```

If prompted for a password, enter **class**. If that does not work, ask the instructor for assistance.

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

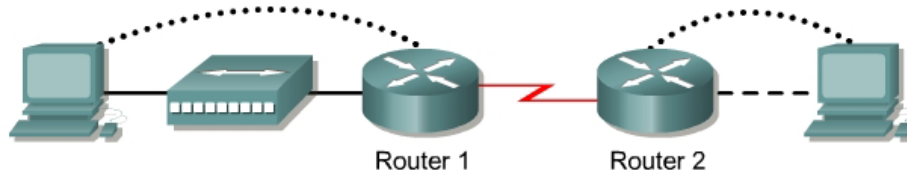
```
Press RETURN to get started!
```

Press **Enter**.

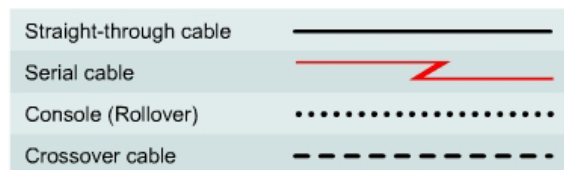
Now the router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
<p>In order to find out exactly how the router is configured, look at the interfaces. This will identify what type and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.</p>				

Lab 1.2.4 Converting RIP v1 to RIP v2



Router Designation	Router Name	FastEthernet 0 Address	Interface Type	Serial 0 Address	Subnet Mask for Both Interfaces	Enable Secret Password	Enable, VTY, and Console Passwords
Router 1	GAD	172.16.0.1	DCE	172.17.0.1	255.255.0.0	class	cisco
Router 2	BHM	172.18.0.1	DTE	172.17.0.2	255.255.0.0	class	cisco



Objective

- Configure RIP v1 on routers.
- Convert to RIP v2 on routers.

Background/Preparation

Cable a network similar to the shown in the diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 2500 and 2600 or any such combination can be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. Perform the following steps on each router unless specifically instructed otherwise.

Start a HyperTerminal session as performed in the Establishing a HyperTerminal session lab.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

Step 1 Configure the routers

On the routers, configure the hostnames as well as the console, virtual terminal, and enable passwords. Next configure the serial IP address and clock rate and the Fast Ethernet IP address interfaces. Finally configure IP host names. If there are problems performing the basic configuration, refer to the “Review of Basic Router Configuration with RIP” lab. Optional interface descriptions and message of the day banners may also be configured. Be sure to save the configurations just created.

Step 2 Configure the routing protocol on the GAD router

Go to the proper command mode and configure RIP routing on the GAD router according to the chart.

Step 3 Save the GAD router configuration

Any time that changes are correctly made to the running configuration, they should be saved to the startup configuration. Otherwise, if the router is reloaded or power cycled, the changes that are not saved in the startup configuration will be lost.

Step 4 Configure the routing protocol on the BHM router

Go to the proper command mode and configure RIP routing on the BHM router according to the chart.

Step 5 Save the BHM router configuration

Step 6 Configure the hosts with the proper IP address, subnet mask, and default gateway

Step 7 Verify that the internetwork is functioning by pinging the FastEthernet interface of the other router

- a. From the host attached to GAD, ping the other host attached to the BHM router. Was the ping successful? _____
- b. From the host attached to BHM, ping the other host attached to the GAD router. Was the ping successful? _____
- c. If the answer is no for either question, troubleshoot the router configurations to find the error. Then do the pings again until the answer to both questions is yes.

Step 8 Enable RIP version 2 routing

- a. Enable version 2 of the RIP routing protocol on both of the routers GAD and BHM.

```
GAD(config)#router rip
GAD(config-router)#version 2
GAD(config-router)#exit
GAD(config)#exit
```

```
BHM(config)#router rip
BHM(config-router)#version 2
BHM(config-router)#exit
BHM(config)#exit
```

Step 9 Ping all of the interfaces on the network from each host

- a. Were all of the interfaces still able to be pinged? _____
- b. If not, troubleshoot the network and ping again.

Once the previous steps are completed, logoff by typing `exit`, and turn the router off. Then remove and store the cables and adapter.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

```
Router>enable
```

If prompted for a password, enter **class**. If that does not work, ask the instructor for assistance.

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router(config)#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started!
```

Press **Enter**.

Now the router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

In order to find out exactly how the router is configured, look at the interfaces. This will identify what type and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.

Step 2 Configure the routing protocol on the GAD router

Go to the correct command mode and configure RIP routing on the GAD router according to the chart.

Step 3 Save the GAD router configuration

Any time that changes are correctly made to the running configuration, they should be saved to the startup configuration. Otherwise, if the router is reloaded or power cycled, the changes that are not saved in the startup configuration will be lost.

Step 4 Configure the routing protocol on the BHM router

Go to the correct command mode and configure RIP routing on the BHM router according to the chart.

Step 5 Save the BHM router configuration

Step 6 Configure the hosts with the proper IP address, subnet mask, and default gateway

Step 7 Verify that the internetwork is functioning by pinging the FastEthernet interface of the other router

- From the host attached to the GAD, ping the other host attached to the BHM router. Was the ping successful? _____
- From the host attached to the BHM, ping the other host attached to the GAD router. Was the ping successful? _____
- If the answer is no for either question, troubleshoot the router configurations to find the error. Then do the pings again until the answer to both questions is yes.

Step 8 Show the routing tables for each router

- From the enable privileged EXEC mode, examine the routing table entries using command `show ip route` command on each router.
- What are the entries in the GAD routing table?

- What are the entries in the BHM routing table?

Step 9 Enable RIP v2 routing

Enable version 2 of the RIP routing protocol on both of the routers, GAD and BHM.

```
GAD(config)#router rip
GAD(config-router)#version 2
GAD(config-router)#exit
GAD(config)#exit
```

```
BHM(config)#router rip
BHM(config-router)#version 2
BHM(config-router)#exit
BHM(config)#exit
```

Step 10 Show the routing tables

- Show the routing tables on both routers again.
 - Have they changed now that RIP v2 is now being used instead of RIP v1? _____
 - What is the difference between RIP v2 and RIP v1? _____
 - What must be done in order to see a difference between RIP v2 and RIP v1?
-

Step 11 Change the Fast Ethernet IP subnet mask on the GAD router

- Change the subnet mask on router GAD from a default Class B mask (255.255.0.0) to a default Class C mask (255.255.255.0). Use the same IP address.

```
GAD(config)#interface fastethernet 0
GAD(config-if)#ip address 172.16.0.1 255.255.255.0
GAD(config-if)#exit
```

- How does this change affect the address for the FastEthernet interface?
-

Step 12 Show the GAD routing table

- Show the GAD routing table.
- Has the output changed with the addition of a subnetted IP address? _____
- How has it changed? _____

Step 13 Show the BHM routing table

- Show the BHM routing table.
- Has the output changed with the addition of a subnetted IP address? _____

Step 14 Change the network addressing scheme

Change the addressing scheme of the network to a single Class B network with a 255.255.255.0 (default Class C) mask.

- On the BHM router:

```
BHM(config)#interface serial 0
BHM(config-if)#ip address 172.16.1.2 255.255.255.0
BHM(config-if)#exit
BHM(config)#interface fastethernet 0
BHM(config-if)#ip address 172.16.3.1 255.255.255.0
BHM(config-if)#exit
BHM(config)#exit
```

- b. On the GAD router:

```
GAD(config)#interface serial 0  
GAD(config-if)#ip address 172.16.1.1 255.255.255.0  
GAD(config-if)#exit
```

Step 15 Show the routing table

- Show the GAD routing table.
- Has the output changed with the addition of subnetted IP addresses? _____
- How has it changed? _____

Step 16 Show the routing table

- Show the BHM routing table.
- Has the output changed with the addition of a subnetted IP address? _____

Step 17 Change the host configurations

Change the host configuration to reflect the new IP addressing scheme of the network

Step 18 Ping all of the interfaces on the network from each host

- Were all of the interfaces still able to be pinged? _____
- If not, troubleshoot the network and ping again.

Step 19 Use show ip route to see different routes by type

- Enter **show ip route connected** on the GAD router.
- What networks are displayed? _____
- What interface is directly connected? _____
- Enter **show ip route rip**
- List the routes listed in the routing table? _____
- What is the administrative distance? _____
- Enter **show ip route connected** on the BHM router.
- What networks are displayed? _____
- What interface is directly connected? _____
- Enter **show ip route rip**
- List the routes listed in the routing table? _____

Step 20 Use the show IP protocol command

- Enter **show ip protocol** on the GAD router.
- When will the routes be flushed? _____
- What is the default distance listed for RIP? _____

Step 21 Remove the version 2 option

Use the `no version` command to return the router to the default RIP configuration.

Step 22 Show the routing table

- a. Show the GAD routing table.
- b. Has the output changed now that version 2 of RIP was removed? _____

Step 23 Show the routing table

- a. Show the BHM routing table.
- b. Has the output changed now that version 2 of RIP was removed? _____

Once the previous steps are completed, log off by typing `exit`, and turn the router off. Then remove and store the cables and adapter.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

```
Router>enable
```

If prompted for a password, enter **class**. If that does not work, ask the instructor for assistance.

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router(config)#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started!
```

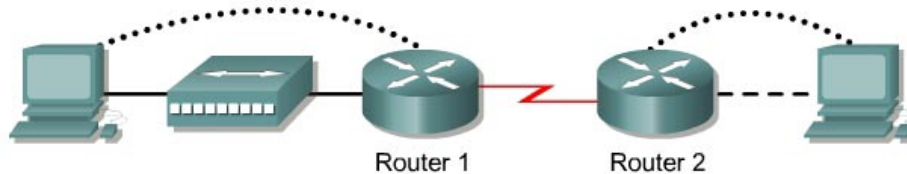
Press **Enter**.

Now the router is ready for the assigned lab to be performed.

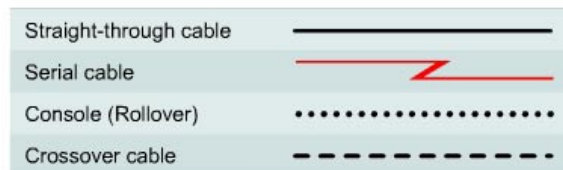
Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

In order to find out exactly how the router is configured, look at the interfaces. This will identify what type and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.

Lab 1.2.6 Troubleshooting RIP v2 using debug



Router Designation	Router Name	FastEthernet 0 Address	Interface Type	Serial 0 Address	Subnet Mask for Both Interfaces	Enable Secret Password	Enable, VTY, and Console Passwords
Router 1	GAD	172.16.0.1	DCE	172.17.1.1	255.255.0.0	class	cisco
Router 2	BHM	172.18.0.1	DTE	172.17.1.2	255.255.0.0	class	cisco



Objective

- Configure RIP v2 on both routers
- Use debug commands to verify proper RIP operation and analyze data transmitted between routers.

Background/Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 2500, and 2600 or any such combination can be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. Perform the following steps on each router unless specifically instructed otherwise.

Start a HyperTerminal session as performed in the Establishing a HyperTerminal session lab.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

Step 1 Configure the routers

On the routers, configure the hostnames as well as the console, virtual terminal, and enable passwords. Next configure the serial interface IP address and clock rate and the Fast Ethernet interface IP address. Finally configure IP host names. If there are problems performing the basic configuration, refer to the Review of Basic Configuration including RIP lab. Optional interface descriptions and message of the day banners may also be configured. Be sure to save the configurations just created.

Step 2 Configure the routing protocol on the GAD router

Go to the proper command mode and configure RIP routing on the GAD router according to the chart.

Step 3 Save the GAD router configuration

Any time that changes are correctly made to the running configuration, they should be saved to the startup configuration. Otherwise if the router is reloaded or power cycled, the changes that are not in the startup configuration will be lost.

Step 4 Configure the routing protocol on the BHM router

Go to the proper command mode and configure RIP routing on the BHM router according to the chart.

Step 5 Save the BHM router configuration

Step 6 Configure the hosts with the proper IP address, subnet mask, and default gateway

Step 7 Verify that the internetwork is functioning by pinging the FastEthernet interface of the other router

- From the host attached to the GAD, ping the other host attached to the BHM router. Was the ping successful? _____
- From the host attached to the BHM, ping the other host attached to the GAD router. Was the ping successful? _____
- If the answer is no for either question, troubleshoot the router configurations to find the error. Then do the pings again until the answer to both questions is yes.

Step 8 Show the debug IP options

- At the privileged EXEC mode type `debug ip ?`.
 - Which routing protocols can use debug commands?
-

Step 9 Show the debug IP RIP options

- At the privileged EXEC mode type `debug ip rip ?`.
- How many options are available for `debug ip rip ??` _____

Step 10 Show the RIP routing updates

- From the enable privileged EXEC mode, examine the routing table entries using command `debug ip rip` command on each router.
 - What are the three operations that take place listed in the rip debug statements?
-

- Turn off debugging by typing either `no debug ip rip` or `undebug all`.

Step 11 Enable RIP Version 2 Routing

Enable version 2 of the RIP routing protocol on the GAD router only.

Step 12 Start the debug function again on the GAD router

- a. Does a problem occur now that we have RIP v2 on the GAD router? _____
- b. What is the problem? _____

Step 13 Clear the routing table

- a. Instead of waiting for the routes to time out, type `clear ip route *`. Then type `show ip route`.
- b. What has happened to the routing table? _____
- c. Will it be updated to include RIP routes if the debug output says the update is ignored? _____

Step 14 Start the debug RIP function

- a. Start the debug RIP function on the BHM router again by typing `debug ip rip`.
- b. Does a problem occur now that RIP v2 is on the GAD router? _____
- c. What is the problem? _____

Step 15 Clear the routing table

- a. Instead of waiting for the routes to time out, type `clear ip route *`. Then type `show ip route`.
- b. What has happened to the routing table? _____
- c. Does a problem occur now that RIP v2 is on the GAD router? _____
- d. Turn off debugging by typing either `no debug ip rip` or `undebug all`.

Step 16 Enable RIP version 2 routing

Enable version 2 of the RIP routing protocol on the BHM router.

Step 17 Use the debug function to see packet traffic on a router

- a. Use the `debug` function to see packet traffic on the GAD router by typing `debug ip packet` at the privileged EXEC mode.
- b. When an RIP update is sent how many source addresses are used? _____
- c. Why are multiple source addresses used? _____
- d. What is the source address used? _____
- e. Why is this address used? _____

Step 18 Start the debug RIP database function on the BHM router

- a. Start the RIP database debugging by typing `debug ip rip database`, then clear the routing table by typing `clear ip route *`.
- b. Are the old routes in the table deleted? _____
- c. Are new routes added back into the table? _____
- d. What does the last entry in the `debug` output say? _____
- e. Turn off debugging by typing either `no debug ip rip` or `undebug all`.

Step 19 Use the debug events function to see routing updates

- a. Use the `debug` function to see routing updates by typing `debug ip rip events` in privileged EXEC mode on the BHM router.
- b. What interfaces are the routing updates sent on? _____
- c. How many routes are in the routing updates being sent? _____

Once the previous steps are completed, log off by typing `exit`, and turn the router off. Then remove and store the cables and adapter.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

```
Router>enable
```

If prompted for a password, enter **class**. If that does not work, ask the instructor for assistance.

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

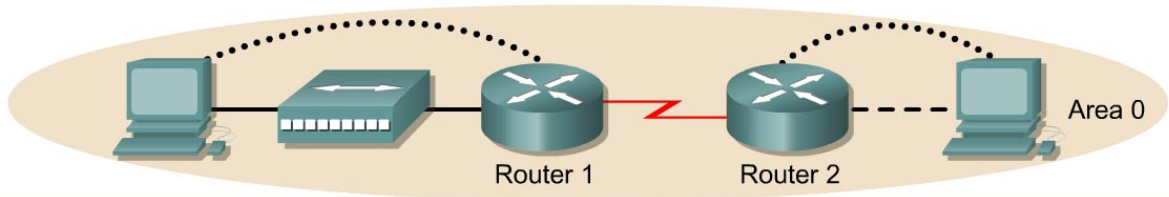
```
Press RETURN to get started!
```

Press **Enter**.

Now the router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
<p>In order to find out exactly how the router is configured, look at the interfaces. This will identify what type and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.</p>				

Lab 2.3.1 Configuring the OSPF Routing Process



Router Designation	Router Name	Enable Secret Password	Enable, VTY, and Console Passwords	Routing Protocol	Network Statements
Router 1	Berlin	class	cisco	OSPF	192.168.1.128 192.168.15.0
Router 2	Rome	class	cisco	OSPF	192.168.15.0 192.168.0.0

Router Designation	IP Host Table Entry	FastEthernet 0 Address/Subnet Mask	Interface Type Serial 0	Serial 0 Address/Subnet Mask	Interface Type Serial 1	Serial 1 Address/Subnet Mask
Router 1	Rome	192.168.1.129/26	DCE	192.168.15.1/30	NA	No address
Router 2	Berlin	192.168.0.1/24	DTE	192.168.15.2/30	NA	No address

Note: The IP Host Table Entry column contents indicate the name(s) of the other router(s) in the IP host table.

Straight-through cable		Console (Rollover)	
Serial cable		Crossover cable	

Objective

- Setup an IP addressing scheme for OSPF area 0.
- Configure and verify Open Shortest Path First (OSPF) routing.

Background/Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 2500, and 2600 or any such combination can be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. Perform the following steps on each router unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

Step 1 Configure the routers

On the routers, enter the global configuration mode and configure the hostname as shown in the chart. Then configure the console, virtual terminal and enable passwords. Next configure the interfaces according to the chart. Finally, configure the IP hostnames. Do not configure the routing protocol until specifically told to. If there are any problems configuring the router basics, refer to prior lab "Review of Basic Router Configuring with RIP".

Step 2 Save the configuration information from the privileged EXEC command mode

```
BERLIN#copy running-config startup-config
Destination filename [startup-config]? [Enter]
```

- a. Why save the running configuration to the startup configuration?

Step 3 Configure the hosts with the proper IP address, subnet mask, and default gateway

- a. Each workstation should be able to ping the attached router. Troubleshoot as necessary. Remember to assign a specific IP address and default gateway to the workstation. If running Windows 98, check by using **Start >Run > winipcfg**. If running Windows 2000, check by using the **ipconfig** command in a DOS window.
- b. At this point the workstations will not be able to communicate with each other. The following steps will demonstrate the process required to get communication working using OSPF as the routing protocol.

Step 4 View the routers configuration and interface information

- a. At the privileged EXEC mode prompt type:

```
Berlin#show running-config
```

- b. Using the **show ip interface brief** command, check the status of each interface.
- c. What is the state of the interfaces on each router?

Berlin:

FastEthernet 0: _____

Serial 0: _____

Serial 1: _____

Rome:

FastEthernet 0: _____

Serial 0: _____

- d. Ping from one of the connected serial interfaces to the other.
Was the ping successful? _____
- e. If the ping was not successful, troubleshoot the router configuration, until the ping is successful.

Step 5 Configure OSPF routing on router Berlin

- a. Configure an OSPF routing process on router Berlin. Use OSPF process number 1 and ensure all networks are in area 0.

```
Berlin(config)#router ospf 1
Berlin(config-router)#network 192.168.1.128 0.0.0.63 area 0
Berlin(config-router)#network 192.168.15.0 0.0.0.3 area 0
Berlin(config-router)#end
```

- b. Examine the routers running configurations files.
- c. Did the IOS version automatically add any lines under router OSPF 1? _____
- d. If so, what did it add?

- e. If there were no changes to the running configuration, type the following commands:

```
Berlin(config)#router ospf 1
Berlin(config-router)#log-adjacency-changes
Berlin(config-router)#end
```

- f. Show the routing table for the Berlin router.

```
Berlin#show ip route
```

- g. Are there any entries in the routing table? _____
- h. Why? _____

Step 6 Configure OSPF routing on router Rome

- a. Configure an OSPF routing process on router Rome. Use OSPF process number 1 and ensure all networks are in area 0.

```
Rome(config)#router ospf 1
Rome(config-router)#network 192.168.0.0 0.0.0.255 area 0
Rome(config-router)#network 192.168.15.0 0.0.0.3 area 0
Rome(config-router)#end
```

- b. Examine the Rome running configuration files.
- c. Did the IOS version automatically add any lines under router OSPF 1? _____
- d. If so, what did it add?

- e. If there were no changes to the running configuration, type the following commands:

```
Rome(config)#router ospf 1
Rome(config-router)#log-adjacency-changes
Rome(config-router)#end
```

- f. Show the routing table for the Rome router:

Rome#**show ip route**

- g. Are there any OSPF entries in the routing table now? _____
- h. What is the metric value of the OSPF route? _____
- i. What is the VIA address in the OSPF route? _____
- j. Are routes to all networks shown in the routing table? _____
- k. What does the O mean in the first column of the routing table? _____

Step 7 Test network connectivity

- a. Ping the Berlin host from the Rome host. Was it successful? _____
- b. If not troubleshoot as necessary.

Once the previous steps are completed, log off by typing **exit**, and turn the router off. Then remove and store the cables and adapter.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class**. If that does not work, ask the instructor for assistance.

```
Router>enable
```

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router(config)#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started!
```

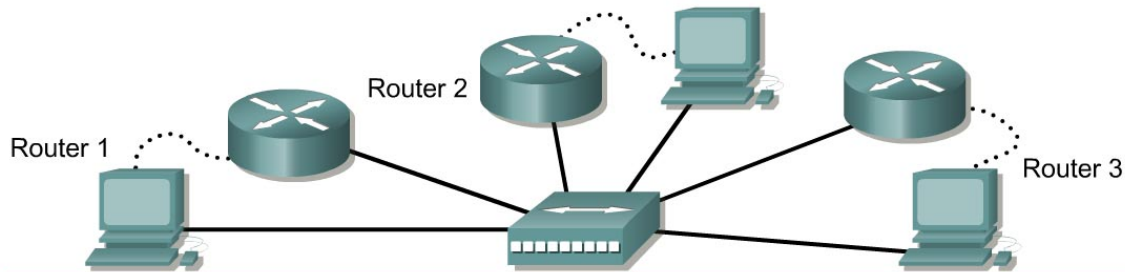
Press **Enter**.

Now the router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

In order to find out exactly how the router is configured, look at the interfaces. This will identify what type and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.

Lab 2.3.2 Configuring OSPF with Loopback Addresses



Router Designation	Router Name	Enable Secret Password	Enable, VTY, and Console Passwords	Routing Protocol	OSPF Priority	Network Statements
Router 1	London	class	cisco	OSPF	1	192.168.1.0
Router 2	Ottawa	class	cisco	OSPF	1	192.168.1.0
Router 3	Brasilia	class	cisco	OSPF	1	192.168.1.0

Router Designation	IP Host Table Entry	FastEthernet 0 Address/ Subnet Mask	Loopback Address/ Subnet Mask
Router 1	Ottawa Brasilia	192.168.1.1/24	192.168.31.11/32
Router 2	London Brasilia	192.168.1.2/24	192.168.31.22/32
Router 3	London Ottawa	192.168.1.3/24	192.168.31.33/32

Note: The IP Host Table Entry column contents indicate the name(s) of the other router(s) in the IP host table.

Straight-through cable		Console (Rollover)	
Serial cable		Crossover cable	

Objective

- Configure routers with a Class C IP addressing scheme.
- Observe the election process for designated routers (DR) and backup designated routers (BDR) on the multiaccess network.
- Configure loopback addresses for Open Shortest Path First (OSPF) stability.
- Assign each OSPF interface a priority to force the election of a specific router as DR.

Background/Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 2500, and 2600 or any such combination can be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. Perform the following steps on each router unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

Step 1 Configure the routers

On the routers, enter the global configuration mode and configure the hostname as shown in the chart. Then configure the console, virtual terminal and enable passwords. Next configure the interfaces according and the IP hostnames. If there are any problems configuring the router basics, refer to the lab "Review of Basic Router Configuring with RIP". Do not configure loopback interfaces and routing protocol yet.

Step 2 Save the configuration information for all the routers

Why save the running configuration to the startup configuration?

Step 3 Configure the hosts with the proper IP address, subnet mask and default gateway

Each workstation should be able to ping all of the attached routers. That is because they are all part of the same subnetwork. Troubleshoot as necessary. Remember to assign a specific IP address and default gateway to the workstation. If running Windows 98, check by using **Start > Run > winipcfg**. If running Windows 2000, check by using the **ipconfig** command in a DOS window.

Step 4 View the routers configuration and interface information

- At the privileged EXEC mode prompt type: **show running-config**
- Using the **show ip interface brief** command, check the status of each interface.
- What is the state of the interfaces on each router?

London:

FastEthernet 0: _____

Serial 0: _____

Serial 1: _____

Ottawa:

FastEthernet 0: _____

Serial 0: _____

Serial 1: _____

Brasilia:

FastEthernet 0: _____

Serial 0: _____

Serial 1: _____

Step 5 Verify connectivity of the routers

- Ping all of the connected FastEthernet interfaces from each other.
- Were the pings successful? _____
- If the pings were not successful, troubleshoot the router configuration, until the **ping** is successful.

Step 6 Configure OSPF routing on router London

- Configure an OSPF routing process on the router London. Use OSPF process number 1 and ensure all networks are in area 0.

```
London(config)#router ospf 1
London(config-router)#network 192.168.1.0 0.0.0.255 area 0
London(config-router)#end
```

- Examine the London router running configuration file.
- Did the IOS version automatically add any lines under router OSPF 1? _____
- If there were no changes to the running configuration, type the following commands.

```
London(config)#router ospf 1
London(config-router)#log-adjacency-changes
London(config-router)#end
```

- Show the routing table for router:

```
London#show ip route
```

- Are there any entries in the routing table? _____
- Why? _____

Step 7 Configure OSPF routing on router Ottawa

- Configure an OSPF routing process on the router Ottawa. Use OSPF process number 1 and ensure all networks are in area 0.

```
Ottawa(config)#router ospf 1
Ottawa(config-router)#network 192.168.1.0 0.0.0.255 area 0
Ottawa(config-router)#end
```

- Examine the Ottawa running configuration file.
- Did the IOS version automatically add any lines under router OSPF 1? _____
- If there were no changes to the running configuration, type the following commands.

```
Ottawa(config)#router ospf 1
Ottawa(config-router)#log-adjacency-changes
Ottawa(config-router)#end
```

Step 8 Configure OSPF routing on router Brasilia

- Configure an OSPF routing process on the router Brasilia. Use OSPF process number 1 and ensure all networks are in area 0.

```
Brasilia(config)#router ospf 1
Brasilia(config-router)#network 192.168.1.0 0.0.0.255 area 0
Brasilia(config-router)#end
```

- b. Examine the Brasilia router running configuration file.
Did the IOS version automatically add any lines under router OSPF 1? _____
- c. What did it add? _____
- d. If there were no changes to the running configuration, type the following commands:

```
Brasilia(config)#router ospf 1
Brasilia(config-router)#log-adjacency-changes
Brasilia(config-router)#end
```

Step 9 Test network connectivity

- a. Ping the Brasilia router from the London router. Was it successful? _____
- b. If not troubleshoot as necessary.

Step 10 Show OSPF adjacencies

- a. Type the command `show ip ospf neighbor` on all routers to verify that the OSPF routing has formed adjacencies.
- b. Is there a designated router identified? _____
- c. Is there a backup designated router? _____
- d. Type the command `show ip ospf neighbor detail` for more information.
- e. What is the neighbor priority of 192.168.1.1 from router Brasilia? _____
- f. What interface is Identified as being part of Area 0? _____

Step 11 Configure the loopback interfaces

Configure the loopback interface on each router to allow for an interface that will not go down due to network change or failure. This task is performed by typing `interface loopback #` at the global configuration mode prompt, where the # represents the number of the loopback interface from 0 - 2,147,483,647.

```
London(config)#interface loopback 0
London(config-if)#ip address 192.168.31.11 255.255.255.255
London(config-router)#end
```

```
Ottawa(config)#interface loopback 0
Ottawa(config-if)#ip address 192.168.31.22 255.255.255.255
Ottawa(config-router)#end
```

```
Brasilia(config)#interface loopback 0
Brasilia(config-if)#ip address 192.168.31.33 255.255.255.255
Brasilia(config-router)#end
```

Step 12 Save the configuration information for all the routers

After saving the configurations on all of the routers, power them down and back up again.

Step 13 Show OSPF adjacencies

- Type the command `show ip ospf neighbor` on all routers to verify that the OSPF routing has formed adjacencies.
- Is there a designated router identified? _____
- Write down the router ID and link address of the DR. _____
- Is there a backup designated router? _____
- Write down the router ID and link address of the BDR. _____
- What is the third router referred to as? _____
- Write down that Routers ID and link address. _____
- Type the command `show ip ospf neighbor detail` for more information.
- What is the neighbor priority of 192.168.1.1 from router Brasilia? _____
- What interface is Identified as being part of Area 0? _____

Step 14 Verify OSPF interface configuration

- Type `show ip ospf interface fastethernet 0` on the London router.
- What is the OSPF state of the interface? _____
- What is the default priority of the interface? _____
- What is the network type of the interface? _____

Step 15 Configure London to always be the DR

To ensure that the London router always becomes the DR for this multi-access segment, the OSPF priority must be set. London is the most powerful router in the network and so best suited to become DR. To assign the London loopback a higher IP address is not advised, as the numbering system has advantages for troubleshooting. Also London is not to act as DR for all segments to which it may belong. Set the priority of the interface to 50 on the London router only.

```
London(config)#interface Fastethernet 0/0
London(config-if)#ip ospf priority 50
London(config-if)#end
```

Display the priority for Interface fastethernet 0/0.

```
London#show ip ospf interface fastethernet 0/0
```

Step 16 Watch election process

- To watch the OSPF election process restart all of the routers using the `reload` command. Be sure to save the running config before restarting the routers. As soon as the router prompt is available type:

```
Ottawa>enable
Ottawa#debug ip ospf events
```

- Which router was elected DR? _____

- c. Which router was elected BDR? _____
- d. Why? _____
- e. To turn off all debugging type `undebug all`.

Step 17 Show OSPF Adjacencies

- a. Type the command `show ip ospf neighbor` on the Ottawa router to verify that the OSPF routing has formed adjacencies.
- b. What is the priority of the DR? _____

Once the previous steps are completed log off by typing `exit` and turn the router off. Then remove and store the cables and adapter.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class**. If that does not work, ask the instructor for assistance.

```
Router>enable
```

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router(config)#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started!
```

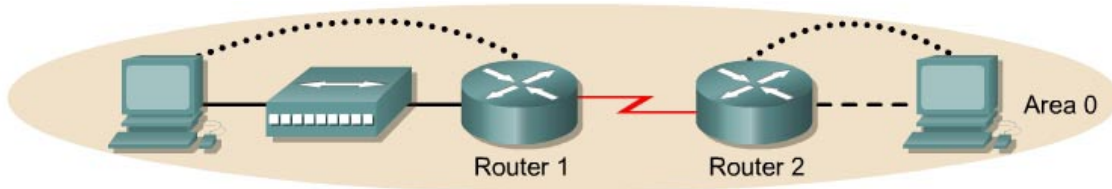
Press **Enter**.

Now the router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

In order to find out exactly how the router is configured, look at the interfaces. This will identify what type and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.

Lab 2.3.3 Modifying OSPF Cost Metric



Router Designation	Router Name	Enable Secret Password	Enable, VTY, and Console Passwords	Routing Protocol	Network Statements
Router 1	Cairo	class	cisco	OSPF	192.168.1.0
Router 2	Moscow	class	cisco	OSPF	192.168.1.0 192.168.0.0

Router Designation	IP Host Table Entry	FastEthernet 0 Address/Subnet Mask	Interface Type Serial 0	Serial 0 Address/Subnet Mask	Interface Type Serial 1	Serial 1 Address/Subnet Mask
Router 1	Moscow	192.168.1.129/26	DCE	192.168.1.1/30	NA	No address
Router 2	Cairo	192.168.0.1/24	DTE	192.168.1.2/30	NA	No address

Note: The IP Host Table Entry column contents indicate the name(s) of the other router(s) in the IP host table.

Straight-through cable		Console (Rollover)	
Serial cable		Crossover cable	

Objective

- Setup an IP addressing scheme for Open Shortest Path First (OSPF) area.
- Configure and verify OSPF routing.
- Modify OSPF cost metric on an interface.

Background/Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 2500, and 2600 or any such combination can be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. Perform the following steps on each router unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

Step 1 Configure the routers

On the routers, enter the global configuration mode and configure the hostname, console, virtual terminal, and enable passwords. Next configure the interfaces and IP hostnames according to the

chart. Do not configure the routing protocol until specifically told to. If there are any problems configuring the router basics, refer to the lab “Review of Basic Router Configuration with RIP”.

Step 2 Save the configuration information from the privileged EXEC command mode

```
Cairo#copy running-config startup-config  
Destination filename [startup-config]?[Enter]
```

```
Moscow#copy running-config startup-config  
Destination filename [startup-config]?[Enter]
```

Why save the running configuration to the startup configuration?

Step 3 Configure the hosts with the proper IP address, subnet mask and default gateway

- Each workstation should be able to ping the attached router. Troubleshoot as necessary. Remember to assign a specific IP address and default gateway to the workstation. If running Windows 9x/ME, check by using **Start > Run > winipcfg**. If running Windows NT/2000/XP, check by using the **ipconfig** command in a Command Prompt window.
- At this point the workstations will not be able to communicate with each other. The following steps will demonstrate the process required to get communication working using OSPF as the routing protocol.

Step 4 View the routers configuration and interface information

- At the privileged EXEC mode type:

```
Cairo#show running-config
```

- Using the **show ip interface brief** command, check the status of each interface.
- What is the state of the interfaces on each router?

Cairo:

FastEthernet 0: _____

Serial 0: _____

Moscow:

FastEthernet 0: _____

Serial 0: _____

- On a router, ping the serial interface of the other router.
- Was the ping successful? _____
- If the ping was not successful, troubleshoot the router configuration until the ping is successful.

Step 5 Configure OSPF routing on router Cairo

- Configure OSPF routing on each router. Use OSPF process number 1 and ensure all networks are in area 0.

```
Cairo(config)#router ospf 1  
Cairo(config-router)#network 192.168.1.128 0.0.0.63 area 0
```

```
Cairo(config-router)#network 192.168.1.0 0.0.0.3 area 0
Cairo(config-router)#end
```

- b. Examine the running configuration file.
- c. Did the IOS version automatically add any lines under router OSPF 1? _____
- d. What did it add? _____
- e. If there were no changes to the running configuration, type the following commands:

```
Cairo(config)#router ospf 1
Cairo(config-router)#log-adjacency-changes
Cairo(config-router)#end
```

- f. Show the routing table for the Cairo router.
Cairo#**show ip route**
- g. Are there any entries in the routing table? _____
- h. Why? _____

Step 6 Configure OSPF routing on router Moscow

- a. Configure OSPF routing on each router. Use OSPF process number 1 and ensure all networks are in area 0.

```
Moscow(config)#router ospf 1
Moscow(config-router)#network 192.168.0.0 0.0.0.255 area 0
Moscow(config-router)#network 192.168.1.0 0.0.0.3 area 0
Moscow(config-router)#end
```

- b. Examine the running configuration file.
- c. Did the IOS version automatically add any lines under router OSPF 1? _____
- d. If there were no changes to the running configuration, type the following commands:

```
Moscow(config)#router ospf 1
Moscow(config-router)#log-adjacency-changes
Moscow(config-router)#end
```

Step 7 Show the routing table entries

- a. Show the routing table entries for the Cairo router.

```
Cairo#show ip route
```

- b. Are there any OSPF entries in the routing table now? _____
- c. What is the metric value of the OSPF route? _____
- d. What is the VIA address in the OSPF route? _____
- e. Are routes to all networks shown in the routing table? _____
- f. What does the O mean in the first column of the routing table? _____

Step 8 Test network connectivity

- a. Ping the Cairo host from the Moscow host. Was it successful? _____
- b. If not troubleshoot as necessary.

Step 9 Look at the OSPF cost on the Cairo router interfaces

Link Bandwidth	Default OSPF Cost
56 Kbps	1785
T1	65
10-Mbps	10
16-Mbps Token-ring	6
FDDI/Fast Ethernet	1

- a. Show the properties of the Cairo router serial and FastEthernet interfaces using the `show interfaces` command.
- b. What is the default bandwidth of the interfaces?
- c. Serial Interface: _____
- d. FastEthernet Interface: _____
- e. Calculate the cost of a link divide 10^8 by the bandwidth in bps.
- f. Serial Interface: _____
- g. FastEthernet Interface: _____

Step 10 Record the OSPF cost of the serial and FastEthernet interfaces

- a. Using the `show ip ospf interface` command, record the OSPF cost of the serial and Fast Ethernet interfaces.
- b. OSPF cost of Serial Interface: _____
- c. OSPF cost of Ethernet Interface: _____
- d. Do these agree with the calculations? _____

Step 11 Manually set the cost on the serial interface

On the Serial interface of the Cairo router, set the OSPF cost to 1562 by typing `ip ospf cost 1562` at the serial interface configuration mode prompt.

Step 12. Verify cost

- a. Note that it is essential that all connected links agree about the cost for consistent calculation of the shortest path first algorithm (SPF) in an area.
- b. Verify that the interface OSPF cost was successfully modified.
- c. Reverse the effect of this command by entering in interface configuration mode the command `no ip ospf cost`.
- d. Verify that the default cost for the interface has returned.

- e. Enter the command `bandwidth 2000` at the serial 0 interface configuration mode.
- f. Record the new OSPF cost of the Serial interface. _____
- g. Can the OSPF cost of an Ethernet interface be modified in this way? _____
- h. The speed can be set on an Ethernet interface. Will this affect the OSPF cost of that interface?

- i. Verify or explain the above answer.

- j. Reset the bandwidth on the serial interface using the `no bandwidth 2000` at the serial 0 interface configuration mode.

Once completion previous steps are completed, logoff by typing `exit` and turn the router off. Then remove and store the cables and adapters.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class**. If that does not work, ask the instructor for assistance.

```
Router>enable
```

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router(config)#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

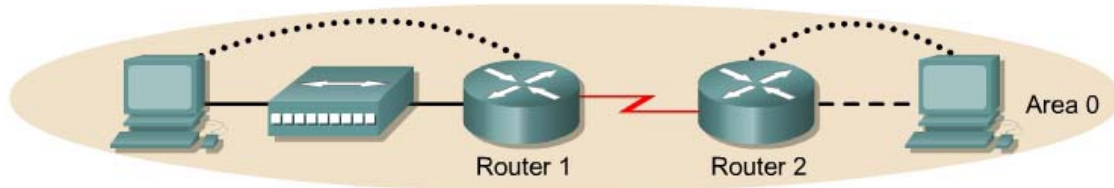
```
Press RETURN to get started!
```

Press **Enter**.

Now the router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
<p>In order to find out exactly how the router is configured, look at the interfaces. This will identify what type and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.</p>				

Lab 2.3.4 Configuring OSPF Authentication



Router Designation	Router Name	Enable Secret Password	Enable, VTY, and Console Passwords	Routing Protocol	Network Statements
Router 1	Dublin	class	cisco	OSPF	192.168.1.0
Router 2	Washington	class	cisco	OSPF	192.168.1.0 192.168.0.0

Router Designation	IP Host Table Entry	FastEthernet 0 Address/Subnet Mask	Interface Type Serial 0	Serial 0 Address/Subnet Mask	Interface Type Serial 1	Loopback 0 Address/Subnet Mask
Router 1	Washington	192.168.1.129/26	DCE	192.168.1.1/30	NA	192.168.31.11/32
Router 2	Dublin	192.168.0.1/24	DTE	192.168.1.2/30	NA	192.168.31.22/32

Note: The IP Host Table Entry column contents indicate the name(s) of the other router(s) in the IP host table.



Objective

- Setup an IP addressing scheme for Open Shortest Path First (OSPF) area.
- Configure and verify OSPF routing.
- Introduce OSPF authentication into the area.

Background/Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 2500, and 2600 or any such combination can be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. Perform the following steps on each router unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

Step 1 Configure the routers

On the routers, enter the global configuration mode and configure the hostname, console, virtual terminal and enable passwords. Next configure the interfaces and IP hostnames according to the

chart. Do not configure the routing protocol until specifically told to. If there are any problems configuring the router basics, refer to the lab "Review of Basic Router Configuration with RIP".

Step 2 Save the configuration information from the privileged EXEC command mode

```
Dublin#copy running-config startup-config  
Destination filename [startup-config]? [Enter]
```

```
Washington#copy running-config startup-config  
Destination filename [startup-config]? [Enter]
```

Why save the running configuration to the startup configuration?

Step 3 Configure the hosts with the proper IP address, subnet mask and default gateway

- Each workstation should be able to ping the attached router. Troubleshoot as necessary. Remember to assign a specific IP address and default gateway to the workstation. If running Windows 9x/ME, check by using **Start > Run > winipcfg**. If running Windows NT/2000/XP, check by using the **ipconfig** command in a Command Prompt window.
- At this point the workstations will not be able to communicate with each other. The following steps will demonstrate the process required to get communication working using OSPF as the routing protocol.

Step 4 Verify connectivity

- On a router, ping the serial interface of the other router.
- What the ping successful? _____
- If the ping was not successful, troubleshoot the routers configurations, until the ping is successful.

Step 5 Configure OSPF routing on both routers

- Configure OSPF routing on each router. Use OSPF process number 1 and ensure all networks are in area 0. Refer to the lab, "Configuring Loopback Interfaces" for review on configuring OSPF routing if necessary.
- Examine the Dublin router running configuration file. Did the IOS version automatically add any lines under router OSPF 1? _____
- Show the routing table for the Dublin router.

```
Dublin#show ip route
```

- Are there any entries in the routing table?
- Why? _____

Step 6 Test network connectivity

- Ping the Dublin host from the Washington host. Was it successful? _____
- If not troubleshoot as necessary.

Step 7 Setup up OSPF authentication

- a. OSPF authentication is being established on the routers in the network. First, introduce authentication only on the Dublin router.
- b. In the interface configuration mode on Serial 0, enter the command `ip ospf message-digest-key 1 md5 7 asecret`.

```
Dublin(config)#interface Serial 0
Dublin(config-if)#ip ospf message-digest-key 1 md5 ?
<0-7> Encryption type (0 for not yet encrypted, 7 for proprietary)
Dublin(config-if)#ip ospf message-digest-key 1 md5 7 ?
LINE The OSPF password (key)
Dublin(config-if)#ip ospf message-digest-key 1 md5 7 asecret
```

- c. What is the OSPF password being used for md5 authentication? _____
- d. What encryption type is being used? _____

Step 8 Enable OSPF authentication in this area, area 0

```
Dublin(config-if)#router ospf 1
Dublin(config-router)#area 0 authentication message-digest
```

- a. Wait for a few seconds. Does the router generate any output? _____
- b. Enter the command `show ip ospf neighbor`.
- c. Are there any OSPF neighbors? _____
- d. Examine the routing table by entering `show ip route`.
- e. Are there any OSPF routes in the Dublin router routing table?
- f. Can the Dublin host ping the Washington host? _____
- g. Enter these configuration commands, one per line. End with CNTL/Z.

```
Washington#configure terminal
Washington(config)#interface serial 0
Washington(config-if)#ip ospf message-digest-key 1 md5 7 asecret
Washington(config-if)#router ospf 1
Washington(config-router)#area 0 authentication message-digest
```

- h. Verify that there is an OSPF neighbor by entering `show ip ospf neighbor` command.
- i. Show the routing table by typing `show ip route`.
- j. Ping the Washington host from Dublin. If this was not successful troubleshoot as necessary.

Once the previous steps are completed, log off by typing `exit` and turn the router off. Then remove and store the cables and adapter.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class**. If that does not work, ask the instructor for assistance.

```
Router>enable
```

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router(config)#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started!
```

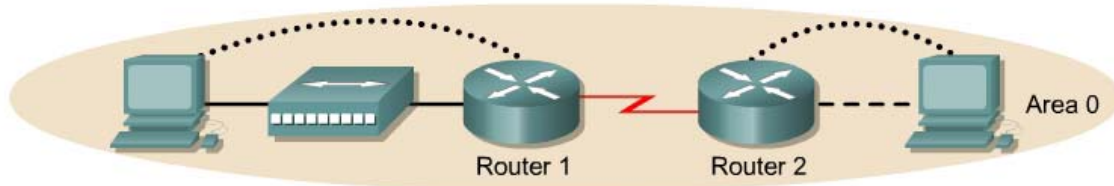
Press **Enter**.

Now the router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

In order to find out exactly how the router is configured, look at the interfaces. This will identify what type and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.

Lab 2.3.5 Configuring OSPF Timers



Router Designation	Router Name	Enable Secret Password	Enable, VTY, and Console Passwords	Routing Protocol	Network Statements
Router 1	Sydney	class	cisco	OSPF	192.168.1.0
Router 2	Rome	class	cisco	OSPF	192.168.1.0 192.168.0.0

Router Designation	IP Host Table Entry	FastEthernet 0 Address/Subnet Mask	Interface Type Serial 0	Serial 0 Address/Subnet Mask	Interface Type Serial 1	Loopback 0 Address/Subnet Mask
Router 1	Rome	192.168.1.129/26	DCE	192.168.1.1/30	NA	192.168.31.11/32
Router 2	Sydney	192.168.0.1/24	DTE	192.168.1.2/30	NA	192.168.31.22/32

Note: The IP Host Table Entry column contents indicate the name(s) of the other router(s) in the IP host table.



Objective

- Setup an IP addressing scheme for OSPF area.
- Configure and verify OSPF routing.
- Modify OSPF interface timers to adjust efficiency of network.

Background/Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 2500, and 2600 or any such combination can be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. Perform the following steps on each router unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

Step 1 Configure the routers

On the routers, enter the global configuration mode and configure the hostname, console, virtual terminal and enable passwords. Next configure the interfaces and IP hostnames according to the chart. Do not configure the routing protocol until specifically told to. If there are any problems configuring the router basics, refer to the lab "Review of Basic Router Configuration with RIP".

Step 2 Save the configuration information from the privileged EXEC command mode

```
Sydney#copy running-config startup-config
Destination filename [startup-config]? [Enter]

Rome#copy running-config startup-config
Destination filename [startup-config]? [Enter]
```

Why save the running configuration to the startup configuration?

Step 3 Configure the hosts with the proper IP address, subnet mask, and default gateway

- Each workstation should be able to ping the attached router. Troubleshoot as necessary. Remember to assign a specific IP address and default gateway to the workstation. If running Windows 9x/ME, check by using **Start > Run > winipcfg**. If running WindowsNT/2000/XP, check by using the **ipconfig** command in a DOS window.
- At this point the workstations will not be able to communicate with each other. The following steps will demonstrate the process required to get communication working using OSPF as the routing protocol.

Step 4 Verify connectivity

- On a router, ping the serial interface of the other router.
- What the ping successful? _____
- If the ping was not successful, troubleshoot the router configurations, until the ping is successful.

Step 5 Configure OSPF routing on both routers

- Configure OSPF routing on each router. Use OSPF process number 1 and ensure all networks are in area 0. Refer to the lab, "Configuring Loopback Interfaces" for review on configuring OSPF routing if necessary.
- Did the IOS version automatically add any lines under router OSPF 1? _____
- Show the routing table for the Sydney router.

```
Sydney#show ip route
```

- Are there any entries in the routing table? _____

Step 6 Test network connectivity

Ping the Sydney host from the Rome host. Was it successful? _____

If not troubleshoot as necessary.

Step 7 Observe OSPF traffic

- At the privileged EXEC mode type the command `debug ip ospf events` and observe the output.
- How frequently are Hello messages sent? _____
- Where are they coming from? _____
- Turn off debugging by typing `no debug ip ospf events` or `undebug all`.

Step 8 Show interface timer information

- Show the hello and dead interval timers on the Sydney router Ethernet and Serial interfaces by entering the command `show ip ospf interface` in privileged EXEC mode.
- Record the Hello and Dead Interval timers for these interfaces
- Hello Interval: _____
- Dead Interval: _____
- What is the purpose of the dead interval? _____

Step 9 Modify the OSPF timers

- Modify the Hello and Dead-Interval timers to smaller values to try to improve performance. On the Sydney router only enter the commands `ip ospf hello-interval 5` and `ip ospf dead-interval 20` for interface Serial 0.

```
Sydney(config)#interface Serial 0
Sydney(config-if)#ip ospf hello-interval 5
Sydney(config-if)#ip ospf dead-interval 20
```

- Wait for a minute and then enter the command `show ip ospf neighbor`.
- Are there any OSPF neighbors? _____

Step 10 Examine the routing table

- Examine the Sydney router routing table by entering `show ip route`.
- Are there any OSPF routes in the table? _____
- Can the Sydney Host ping the Rome host? _____

Step 11 Look at the OSPF data transmissions.

- Enter the command `debug ip ospf events` in privileged EXEC mode.
- Is there an issue that is identified? _____
- If there is, what is the issue? _____

Step 12 Check the Rome router routing table status.

- On the Rome router check the routing table by typing `show ip route`.
- Are there any OSPF routes in the table? _____

Step 13 Set the Rome router interval timers

- a. Match the timer values on the Rome Serial link with the Sydney router.

```
Rome (config) #interface serial 0
Rome (config-if) #ip ospf hello-interval 5
Rome (config-if) #ip ospf dead-interval 20
```

- b. Verify the OSPF neighbor by entering `show ip ospf neighbor` command.
- c. Show the routing table by typing `show ip route`.
- d. Are there OSPF routes in the table? _____
- e. Ping the Rome host from Sydney. If this was not successful troubleshoot the configurations.

Step 14 Reset the routers interval timers to the default values

Use the no form of the `ip ospf hello-interval` and the `ip ospf dead-interval` to reset the OSPF timers back to their default values.

Step 15 Verify the interval timers are returned to the default values

- a. Use the `show ip ospf interface` command to verify the timers are reset to their default values.
- b. Are the values back to the default? _____
- c. If not, repeat step 13 and verify again.

Once the previous steps are completed, logoff by typing `exit` and turn the router off. Then remove and store the cables and adapter.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class**. If that does not work, ask the instructor for assistance.

```
Router>enable
```

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router(config)#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started!
```

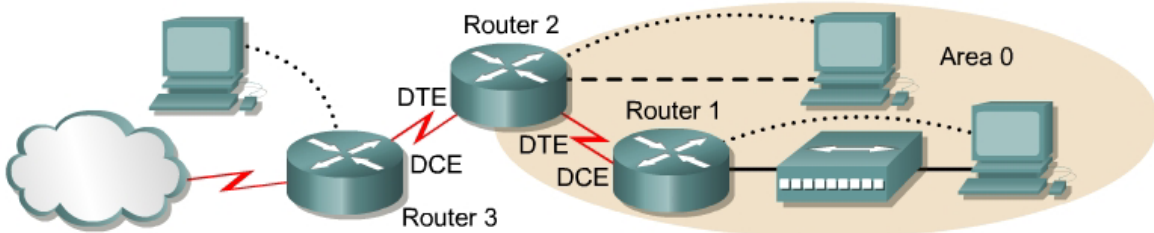
Press **Enter**.

Now the router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

In order to find out exactly how the router is configured, look at the interfaces. This will identify what type and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.

Lab 2.3.6 Propagating Default Routes in an OSPF Domain



Router Designation	Router Name	Enable Password	Secret Password	Enable, VTY, and Console Passwords	Routing Protocol	Network Statements	Loopback 0 Address/Subnet Mask
Router 1	Tokyo	class		cisco	OSPF	192.168.1.0	192.168.31.11/32
Router 2	Madrid	class		cisco	OSPF	192.168.1.0 192.168.0.0	192.168.31.22/32

Router Designation	IP Host Table Entry	FastEthernet 0 Address/Subnet Mask	Interface Type Serial 0	Serial 0 Address/Subnet Mask	Interface Type Serial 1	Serial 1 Address/Subnet Mask
Router 1	Madrid	192.168.1.129/24	DCE	192.168.1.1/30	NA	NA
Router 2	Tokyo	192.168.0.1/24	DTE	192.168.1.2/30	DTE	200.20.20.2/30

Note: The IP Host Table Entry column contents indicate the name(s) of the other router(s) in the IP host table.



Objective

- Setup an IP addressing scheme for OSPF area.
- Configure and verify Open Shortest Path First (OSPF) routing.
- Configure the OSPF network so that all hosts in OSPF area can connect to outside networks.

Background/Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 2500, and 2600 or any such combination can be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. Perform the following steps on each router unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

Step 1 Configure the ISP router

Normally the ISP router would be configured by the Internet service provider (ISP). For the purpose of this lab, after erasing the old configuration, configure the ISP router (Router 3) this way by typing:

```
Router>enable
Router#configure terminal
Router(config)#hostname ISP
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#interface serial 1
ISP(config-if)#ip address 200.20.20.1 255.255.255.252
ISP(config-if)#clock rate 64000
ISP(config-if)#no shutdown
ISP(config-if)#interface loopback 0
ISP(config-if)#ip address 138.25.6.33 255.255.255.255
ISP(config-if)#exit
ISP(config)#ip route 192.168.1.0 255.255.255.0 200.20.20.2
ISP(config)#ip route 192.168.0.0 255.255.255.0 200.20.20.2
ISP(config)#end
ISP#copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
ISP#
```

Step 2 Configure the Area 0 OSPF routers

On the routers, enter the global configuration mode and configure the hostname, console, virtual terminal and enable passwords. Next configure the interfaces and IP hostnames according to the chart. Do not configure the routing protocol until specifically told to. If there are any problems configuring the router basics, refer to the lab “Review of Basic Router Configuration with RIP”.

Step 3 Save the configuration information from the privileged EXEC command mode

```
Tokyo#copy running-config startup-config
Destination filename [startup-config]? [Enter]

Madrid#copy running-config startup-config
Destination filename [startup-config]? [Enter]
```

Why save the running configuration to the startup configuration?

Step 4 Configure the hosts with the proper IP address, subnet mask and default gateway

- Each workstation should be able to ping the attached router. Troubleshoot as necessary. Remember to assign a specific IP address and default gateway to the workstation. If running Windows 9x/ME, check by using **Start > Run > winipcfg**. If running Windows NT/2000/XP, check by using the **ipconfig** command in a DOS window.
- At this point the workstations will not be able to communicate with each other. The following steps will demonstrate the process required to get communication working using OSPF as the routing protocol.

Step 5 Verify connectivity

- a. Ping from the Madrid router to both the Tokyo and the ISP routers.
- b. Were the pings successful? _____
- c. If the ping was not successful, troubleshoot the router configurations, until the ping is successful.

Step 6 Configure OSPF routing on both area 0 routers

- a. Configure OSPF routing on each router. Use OSPF process number 1 and ensure all networks are in area 0. Refer to the lab “Configuring loopback interfaces” for review on configuring OSPF routing if necessary.
- b. Did the IOS version automatically add any lines under router OSPF 1? _____
- c. Show the routing table for the Tokyo router.

```
Tokyo#show ip route
```

- d. Are there any entries in the routing table? _____

Step 7 Test network connectivity

- a. Ping the Tokyo host from the Madrid host. Was it successful? _____
- b. If not troubleshoot as necessary.

Step 8 Observe OSPF traffic

- a. At privileged EXEC mode type the command `debug ip ospf events` and observe the output.
- b. Is there OSPF traffic? _____
- c. Turn off debugging by typing `no debug ip ospf events` or `undebug all`.

Step 9 Create a default route to the ISP

On the Madrid router only, type in a static default route through Serial 1 interface.

```
Madrid(config)#ip route 0.0.0.0 0.0.0.0 200.20.20.1
```

Step 10 Verify the default static route

- a. Verify the default static route by looking at the Madrid routing table.
- b. Is the default route in the routing table? _____

Step 11 Verify connectivity from the Madrid router

- a. Verify connectivity from the Madrid router by pinging the ISP Serial 1 interface from the Madrid router.
- b. Can the interface be pinged? _____
- c. Next, on the host attached to Madrid, open a Command Prompt and ping the serial 1 interface on the ISP router.
- d. Can the interface be pinged? _____
- e. This time, ping the loopback address of the ISP router, which represents the ISP connection to the Internet.

- f. Can the loopback interface be pinged? _____
- g. All of these pings should be successful. If they are not, troubleshoot the configurations on the host and the Madrid and ISP routers.

Step 12 Verify connectivity from the Tokyo router

- a. Verify the connection between the ISP and the Tokyo by pinging the serial 1 interface of the ISP router on the Tokyo router.
- b. Can the interface be pinged? _____
- c. If yes, why? If not, why not? _____

Step 13 Redistribute the static default route

- a. Propagate the gateway of last resort to the other routers in the OSPF domain. At the configure router prompt on the Madrid router type **default-information originate**.

```
Madrid(config-router)#default-information originate
```

- b. Is there now a default route on the Tokyo router? _____
- c. What is the address of the Gateway of last resort? _____
- d. There is an O*E2 entry in the routing table. What type of route it is? _____
- e. Can the ISP server address at 138.25.6.33 be pinged from both workstations? _____
- f. If no, troubleshoot both hosts and all three routers.

Once the previous steps are completed, log off by typing **exit** and turn the router off. Then remove and store the cables and adapter.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class**. If that does not work, ask the instructor for assistance.

```
Router>enable
```

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router(config)#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started!
```

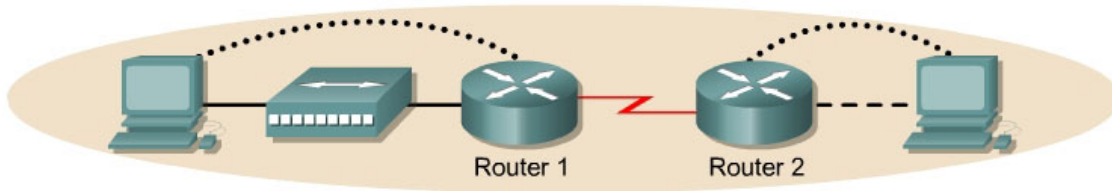
Press **Enter**.

Now the router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

In order to find out exactly how the router is configured, look at the interfaces. This will identify what type and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.

Lab 3.2.1 Configuring EIGRP Routing



Router Designation	Router Name	Enable Secret Password	Enable, VTY, and Console Passwords	Routing Protocol	Network Statements
Router 1	Paris	class	cisco	EIGRP	192.168.3.0 192.168.2.0
Router 2	Warsaw	class	cisco	EIGRP	192.168.1.0 192.168.2.0

Router Designation	IP Host Table Entry	FastEthernet 0 Address/Subnet Mask	Interface Type Serial 0	Serial 0 Address/Subnet Mask	Loopback 0 Address/Subnet Mask
Router 1	Warsaw	192.168.3.1/24	DCE	192.168.2.1/30	192.168.0.2/24
Router 2	Paris	192.168.1.1/24	DTE	192.168.2.2/30	No address

Note: The IP Host Table Entry column contents indicate the name(s) of the other router(s) in the IP host table.

Straight-through cable		Console (Rollover)	
Serial cable		Crossover cable	

Objective

- Setup an IP addressing scheme for the network.
- Configure and verify Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

Background/Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 2500, and 2600 or any such combination can be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. Perform the following steps on each router unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

Step 1 Configure the routers

On the routers, enter the global configuration mode and configure the hostname as shown in the chart. Then configure the console, virtual terminal and enable passwords. Next configure the interfaces according to the chart. Finally, configure the IP hostnames. Do not configure the routing

protocol until specifically told to. If there are any problems configuring the router basics, refer to the lab "Review of Basic Router Configuration with RIP".

Step 2 Save the configuration information from the privileged EXEC command mode

```
Paris#copy running-config startup-config
Destination filename [startup-config]? [Enter]
```

Step 3 Configure the hosts with the proper IP address, subnet mask and default gateway

- Each workstation should be able to ping the attached router. Troubleshoot as necessary. Remember to assign a specific IP address and default gateway to the workstation. If running Windows 98, check by using **Start > Run > winipcfg**. If running Windows 2000, check by using the **ipconfig** command in a DOS window.
- At this point the workstations will not be able to communicate with each other. The following steps will demonstrate the process required to get communication working using EIGRP as the routing protocol.

Step 4 View the routers configuration and interface information

- At the privileged EXEC mode prompt type:

```
Paris#show running-config
```

- Using the **show ip interface brief** command, check the status of each interface.
- What is the state of the interfaces on each router?

Paris:

FastEthernet 0: _____

Serial 0: _____

Warsaw:

FastEthernet 0: _____

Serial 0: _____

- Ping from one of the connected serial interfaces to the other.
- Was the ping successful? _____
- If the ping was not successful, troubleshoot the routers configuration, until the ping is successful.

Step 5 Configure EIGRP routing on router Paris

- Enable the EIGRP routing process on Paris, and configure the networks it will advertise. Use EIGRP autonomous system number 101.

```
Paris(config)#router eigrp 101
Paris(config-router)#network 192.168.3.0
Paris(config-router)#network 192.168.2.0
Paris(config-router)#network 192.168.0.0
Paris(config-router)#end
```

- Show the routing table for the Paris router.

```
Paris#show ip route
```

- c. Are there any entries in the routing table? _____
- d. Why? _____

Step 6 Configure EIGRP routing on router Warsaw

- a. Enable the EIGRP routing process on Warsaw, and configure the networks it will advertise. Use EIGRP autonomous system number 101.

```
Warsaw(config)#router eigrp 101  
Warsaw(config-router)#network 192.168.2.0  
Warsaw(config-router)#network 192.168.1.0  
Warsaw(config-router)#end
```

- b. Show the routing table for the Warsaw router.

```
Warsaw#show ip route
```

Step 7 Test network connectivity

Ping the Paris host from the Warsaw host. Was it successful? _____

If not troubleshoot as necessary.

Once the previous steps are completed, log off by typing **exit**, and turn the router off. Then remove and store the cables and adapter.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class**. If that does not work, ask the instructor for assistance.

```
Router>enable
```

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router(config)#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started!
```

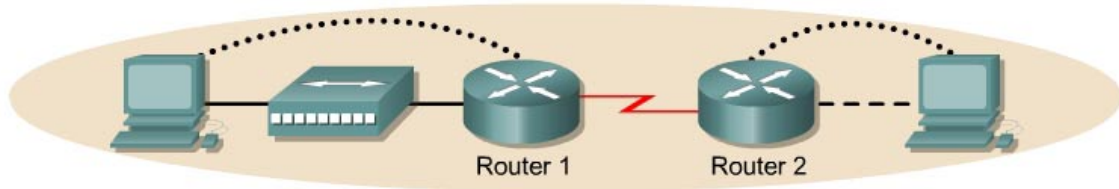
Press **Enter**.

Now the router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

In order to find out exactly how the router is configured, look at the interfaces. This will identify what type and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.

Lab 3.2.3 Verifying Basic EIGRP Configuration



Router Designation	Router Name	Enable Secret Password	Enable, VTY, and Console Passwords	Routing Protocol	Network Statements
Router 1	Paris	class	cisco	EIGRP	192.168.3.0 192.168.2.0
Router 2	Warsaw	class	cisco	EIGRP	192.168.1.0 192.168.2.0

Router Designation	IP Host Table Entry	FastEthernet 0 Address/Subnet Mask	Interface Type Serial 0	Serial 0 Address/Subnet Mask	Loopback 0 Address/Subnet Mask
Router 1	Warsaw	192.168.3.1/24	DCE	192.168.2.1/30	192.168.0.2/24
Router 2	Paris	192.168.1.1/24	DTE	192.168.2.2/30	No address

Note: The IP Host Table Entry column contents indicate the name(s) of the other router(s) in the IP host table.



Objective

- Setup an IP addressing scheme for the network.
- Configure and verify Enhanced Interior Gateway Routing Protocol (EIGRP) routing.

Background/Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the above diagram may be used. For example, router series 800, 1600, 1700, 2500, and 2600 or any such combination can be used. Please refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this lab is produced from 1721 series routers. Any other router used may produce slightly different output. Perform the following steps on each router unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

Step 1 Configure the routers

On the routers, enter the global configuration mode and configure the hostname as shown in the chart. Then configure the console, virtual terminal and enable passwords. Next configure the interfaces according to the chart. Finally, configure the IP hostnames. Do not configure the routing protocol until specifically told to. If there are any problems configuring the router basics, refer to the lab "Review of Basic Router configuration with RIP".

Step 2 Save the configuration information from the privileged EXEC command mode

```
Paris#copy running-config startup-config
Destination filename [startup-config]? [Enter]
```

Step 3 Configure the hosts with the proper IP address, subnet mask and default gateway

- Each workstation should be able to ping the attached router. Troubleshoot as necessary. Remember to assign a specific IP address and default gateway to the workstation. If running Windows 98, check by using **Start > Run > winipcfg**. If running Windows 2000, check by using the `ipconfig` command in a DOS window.
- At this point the workstations will not be able to communicate with each other. The following steps will demonstrate the process required to get communication working using EIGRP as the routing protocol.

Step 4 View the routers configuration and interface information

- At the privileged EXEC mode prompt type:

```
Paris#show running-config
```

- Using the `show ip interface brief` command, check the status of each interface.
- What is the state of the interfaces on each router?

Paris:

FastEthernet 0: _____

Serial 0: _____

Warsaw:

FastEthernet 0: _____

Serial 0: _____

- Ping from one of the connected serial interfaces to the other.
- What the ping successful? _____
- If the ping was not successful, troubleshoot the routers configuration until the ping is successful.

Step 5 Configure EIGRP routing on router Paris

- Enable the EIGRP routing process on Paris, and configure the networks it will advertise. Use EIGRP autonomous system number 101.

```
Paris(config)#router eigrp 101
Paris(config-router)#network 192.168.3.0
Paris(config-router)#network 192.168.2.0
Paris(config-router)#network 192.168.0.0
```

```
Paris(config-router)#end
```

- b. Show the routing table for the Paris router.

```
Paris#show ip route
```

- c. Are there any entries in the routing table? _____
- d. Why? _____

Step 6 Configure EIGRP routing on router Warsaw

- a. Enable the EIGRP routing process on Warsaw, and configure the networks it will advertise. Use EIGRP autonomous system number 101.

```
Warsaw(config)#router eigrp 101
Warsaw(config-router)#network 192.168.2.0
Warsaw(config-router)#network 192.168.1.0
Warsaw(config-router)#end
```

- b. Show the routing table for the Warsaw router.

```
Warsaw#show ip route
```

- c. Are there any EIGRP entries in the routing table now? _____
- d. What is the address type in the EIGRP 192.168.2.0 route? _____
- e. What does the D mean in the first column of the routing table? _____

Step 7 Show EIGRP neighbors

- a. From the Paris router show any neighbors connected using the `show ip eigrp neighbors` command at the privileged EXEC mode prompt.
- b. Are any neighbors shown? _____

Step 8 Test network connectivity

- a. Ping the Paris host from the Warsaw host. Was it successful? _____
- b. If not troubleshoot as necessary.

Step 9 View the topology table

- a. To view the topology table, issue the `show ip eigrp topology all-links` command.
- b. How many routes are in passive mode? _____
- c. To view more specific information about a topology table entry, use an IP address with this command:

```
Paris#show ip eigrp topology 192.168.1.0
```

- d. Based on the output of this command, does it tell what external protocol originated this route to 192.168.2.0?
- _____

e. Does it tell which router originated the route?

f. Finally, use `show` commands to view key EIGRP statistics. On the Paris router, issue the `show ip eigrp traffic` command.

g. How many hello packets has the Paris router received? _____

h. How many has it sent? _____

Once the previous steps are completed, log off by typing `exit`, and turn the router off. Then remove and store the cables and adapter.

Erasing and reloading the router

Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class**. If that does not work, ask the instructor for assistance.

```
Router>enable
```

At the privileged EXEC mode, enter the command **erase startup-config**.

```
Router#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue?  
[confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

Now at the privileged EXEC mode, enter the command **reload**.

```
Router(config)#reload
```

The responding line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

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

Press **Enter** to confirm.

In the first line of the response will be:

```
Reload requested by console.
```

After the router has reloaded the line prompt will be:

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

Type **n** and then press **Enter**.

The responding line prompt will be:

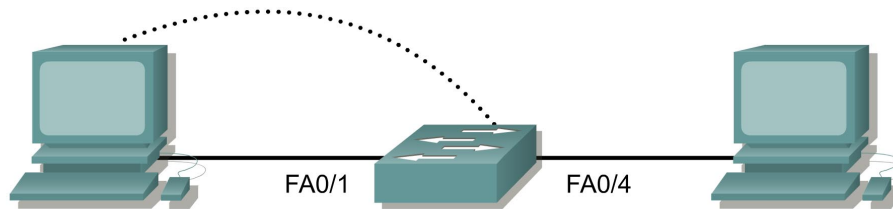
```
Press RETURN to get started!
```

Press **Enter**.

Now the router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	FastEthernet 0 (FA0)	FastEthernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	FastEthernet 0/0 (FA0/0)	FastEthernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
<p>In order to find out exactly how the router is configured, look at the interfaces. This will identify what type and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart 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 IOS command to represent the interface.</p>				

Lab 6.2.2 Basic Switch Configuration



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords
Switch 1	ALSwitch	class	cisco

Straight-through cable	
Serial cable	
Console (Rollover)	
Crossover cable	

Objective

- Configure a switch with a name and an IP address.
- Configure passwords to ensure that access to the CLI is secured.
- Configure switch port speed and duplex properties for an interface.
- Save the active configuration.
- View the switch browser interface.

Background/Preparation

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise. Instructions are also provided for the 1900 Series switch, which initially displays a User Interface Menu. Select the “Command Line” option from the menu to perform the steps for this lab.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Enter privileged mode

- Privileged mode gives access to all the switch commands. Many of the privileged commands configure operating parameters. Therefore, privileged access should be password-protected to prevent unauthorized use. The privileged 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.

```
Switch>enable
Switch#
```

1900:

```
>enable
#
```

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

Step 2 Examine the current switch configuration

- Examine the following current running configuration file:

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

- How many Ethernet or Fast Ethernet interfaces does the switch have? _____
- What is the range of values shown for the VTY lines? _____
- Examine the current contents of NVRAM as follows:

```
Switch#show startup-config
%% Non-volatile configuration memory is not present
```

- Why does the switch give this response?
-

Step 3 Assign a name to the switch

- Enter `enable` and then the configuration mode. The configuration mode allows the management of the switch. Enter `ALSwitch`, the name this switch will be referred to in the following:

```
Switch#configure terminal
```

Enter the configuration commands, one for each line. End by pressing **Ctrl-Z**.

```
Switch(config)#hostname ALSwitch
ALSwitch(config)#exit
```

- Notice the prompt changed in the configuration to reflect its new name. Type `exit` or press **Ctrl-Z** to go back into privileged mode.

Step 4 Examine the current running configuration

- Exam the current configuration that follows to verify that there is no configuration except for the hostname:

```
ALSwitch#show running-config
```

- Are there any passwords set on the lines? _____
- What does the configuration show as the hostname of this switch? _____

Step 5 Set the access passwords (1900: Skip to Step 6)

Enter config-line mode for the console. Set the password on this line as **cisco** for login. Configure the vty lines 0 to 15 with the password **cisco** as follows:

```
ALSwitch#configure terminal
```

Enter the configuration commands, one for each line. End by pressing **Ctrl-Z**.

```
ALSwitch(config)#line con 0
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login
```

```
ALSwitch(config-line)#line vty 0 15
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login
```

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

Step 6 Set the command mode passwords

- Set the **enable password** to **cisco** and the **enable secret password** to **class** as follows:

```
ALSwitch(config)#enable password cisco
ALSwitch(config)#enable secret class
```

1900:

```
ALSwitch(config)#enable password level 15 cisco
ALSwitch(config)#enable secret class
```

2950:

```
#show interface fastethernet 0/4      (Note: this can be a trunk or access port)
```

Or

```
#show interface gigabitethernet 0/1   (Note: this can be a trunk or access port)
```

- Which password takes precedence, the enable password or enable secret password? _____

Step 7 Configure the layer 3 access to the switch

- Set the IP address of the switch to 192.168.1.2 with a subnet mask of 255.255.255.0 as follows:

Note: This is done on the internal virtual interface VLAN 1.

```
ALSwitch(config)#interface VLAN 1
ALSwitch(config-if)#ip address 192.168.1.2 255.255.255.0
ALSwitch(config-if)#exit
```

```
1900:
ALSwitch(config)#ip address 192.168.1.2 255.255.255.0
ALSwitch(config)#exit
```

- b. Set the default gateway for the switch and the default management VLAN to 192.168.1.1 as follows:

```
ALSwitch(config)#ip default-gateway 192.168.1.1
ALSwitch(config)#exit
```

```
1900:
ALSwitch(config)#ip default-gateway 192.168.1.1
ALSwitch(config)#exit
```

Step 8 Verify the management LANs settings (1900: Skip to Step 10)

- a. Verify the interface settings on VLAN 1 as follows:

```
ALSwitch#show interface VLAN 1
```

- b. What is the bandwidth on this interface? _____
- c. What are the VLAN states: VLAN1 is _____, Line protocol is _____
- d. Enable the virtual interface using the **no shutdown** command

```
ALSwitch(config)#interface VLAN 1
ALSwitch(config-if)#no shutdown
ALSwitch(config-if)#exit
```

- e. What is the queuing strategy? _____

Step 9 Save the configuration

- a. The basic configuration of the switch has just been completed. Back up the running configuration file to NVRAM as follows:

Note: This will ensure that the changes made will not be lost if the system is rebooted or loses power.

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

1900:

- b. The configuration is automatically saved to NVRAM within approximately one minute of entering a command. To save the configuration to a TFTP server, enter the following:

```
ALSwitch#copy nvram tftp://tftp server ip add/destination_filename
```

- c. Configuration upload is successfully completed.

Step 10 Examine the startup configuration file (1900: Skip to Step 11)

- a. To see the configuration that is stored in NVRAM, type `show startup-config` from the privileged EXEC (enable mode).

```
ALSwitch#show startup-config
```

- b. What is displayed? _____
- c. Are all the changes that were entered recorded in the file? _____

Step 11 Exit the switch

Logoff the switch by typing `exit` as follows:

```
ALSwitch#exit
```

Once these steps are completed, logoff by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the privileged EXEC mode by typing `enable`.

If prompted for a password, enter `class` (if that does not work, ask the instructor).

```
Switch>enable
```

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the `show vlan` command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the `reload` command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the `reload` command.

5. Software restart (using the `reload` command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

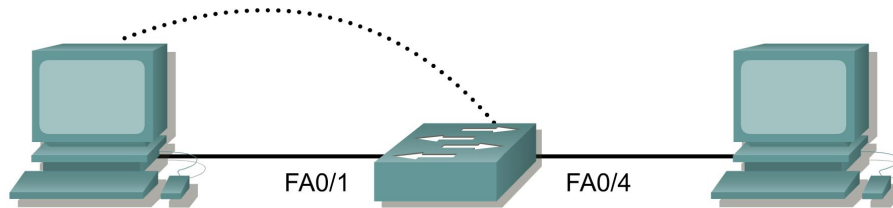
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

Lab 6.2.3 Managing the MAC Address Table



Switch Designation	Switch Name	Enable Secret Password	Enable,VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	ALSwitch	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0

Straight-through cable	
Serial cable	
Console (Rollover)	
Crossover cable	

Objective

- Create a basic switch configuration.
- Manage the switch MAC table.

Background/Preparation

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise. Instructions are also provided for the 1900 Series switch, which initially displays a User Interface Menu. Select the “Command Line” option from the menu to perform the steps for this lab.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the hostname, access and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

Configure the hosts to use the same IP subnet for the address, mask, and default gateway as on the switch.

Step 3 Verify connectivity

- To verify that hosts and switch are correctly configured, ping the switch IP address from the hosts.
- Were the pings successful? _____
- If the answer is no, troubleshoot the hosts and switch configurations.

Step 4 Record the MAC addresses of the host

- Determine and record the layer 2 addresses of the PC network interface cards.
If running Windows 98, check by using **Start > Run > winipcfg**, then click on **More info**.
If running Windows 2000, check by using **Start > Run > cmd > ipconfig /all**.
- PC1: _____
- PC2: _____

Step 5 Determine the MAC addresses that the switch has learned

- To determine the MAC addresses the switch has learned, use the `show mac-address-table` command as follows at the privileged EXEC mode prompt:

```
ALSwitch#show mac-address-table
```

- How many dynamic addresses are there? _____
- How many total MAC addresses are there? _____
- How many addresses have been user defined? _____
- Do the MAC addresses match the host MAC addresses? _____

Step 6 Determine the show MAC table options

- To determine the options the `show mac-address-table` command has use the `?` option as follows:

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

- How many options are available for the `show mac-address-table` command? _____
- Show only the MAC addresses from the table that were learned dynamically.
- How many are there? _____

Step 7 Clear the MAC address table

To remove the existing MAC addresses use the `clear mac-address-table` command from the privileged EXEC mode prompt as follows:

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

Step 8 Verify the results

- a. Verify that the `mac-address-table` was cleared as follows:

```
ALSwitch#show mac-address-table
```

- b. How many total MAC addresses are there now? _____
- c. How many dynamic addresses are there? _____

Step 9 Determine the clear MAC table options

- a. To determine the options available use the command `clear mac-address-table ?` at the privileged EXEC mode prompt as follows:

```
ALSwitch#clear mac-address-table ?
```

- b. How many options are there? _____
- c. In what circumstances would these options be used? _____

Step 10 Examine the MAC table again

- a. Look at the MAC address table again using the `show mac-address-table` command at the privileged EXEC mode prompt as follows:

```
ALSwitch#show mac-address-table
```

- b. How many dynamic addresses are there? _____
- c. Why did this change from the last display? _____
- d. The table has not changed yet. Ping the switch IP address from the hosts two times each and repeat Step 10.

Step 11 Exit the switch

- a. Type `exit`, as follows to leave the switch welcome screen.

```
Switch#exit
```

- b. Once the steps are completed, logoff by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class** (if that does not work, ask the instructor).

```
Switch>enable
```

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the **show vlan** command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the **reload** command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the **reload** command.

5. Software restart (using the **reload** command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the privileged EXEC mode enter the command **reload**.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type **n** and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter **y** and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

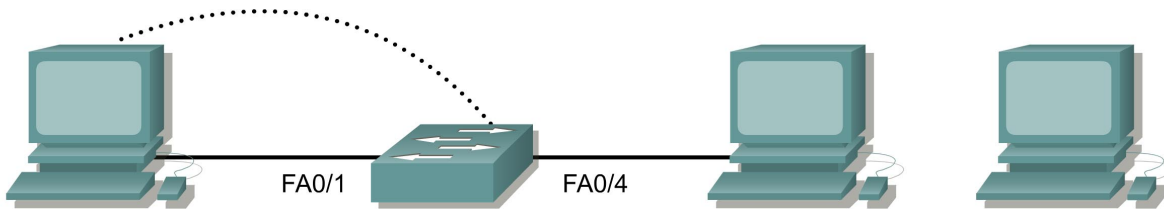
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter **y** and press **Enter**.

Lab 6.2.5 Configuring Port Security



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	ALSwitch	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0

Straight-through cable	
Serial cable	
Console (Rollover)	
Crossover cable	

Objective

- Create and verify a basic switch configuration.
- Configure port security on individual FastEthernet ports.

Background/Preparation

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are intended to be executed on each switch unless specifically instructed otherwise. Instructions are also provided for the 1900 Series switch, which initially displays a User Interface Menu. Select the “Command Line” option from the menu to perform the steps for this lab.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the hostname, access and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

- Configure the hosts to use the same IP subnet for the address, mask, and default gateway as on the switch.
- There is a third host needed for this lab. It needs to be configured with the address 192.168.1.7. The subnet mask is 255.255.255.0 and the default gateway is 192.168.1.1.

Note: Do not connect this PC to the switch yet.

Step 3 Verify connectivity

- To verify that hosts and switch are correctly configured, ping the switch IP address from the hosts.
- Were the pings successful? _____
- If the answer is no, troubleshoot the hosts and switch configurations.

Step 4 Record the host MAC addresses

- Determine and record the layer 2 addresses of the PC network interface cards.
If running Windows 98, check by using **Start > Run > winipcfg**. Click on **More info**.
If running Windows 2000, check by using **Start > Run > cmd > ipconfig /all**.
- PC1 _____
- PC2 _____

Step 5 Determine what MAC addresses that the switch has learned

- Determine what MAC addresses the switch has learned by using the `show mac-address-table` command as follows, at the privileged exec mode prompt:

```
ALSwitch#show mac-address-table
```

- How many dynamic addresses are there? _____
- How many total MAC addresses are there? _____
- Do the MAC addresses match the host MAC addresses? _____

Step 6 Determine the show MAC table options

- Enter the following to determine the options the `mac-address-table` command has use the ? option:

```
ALSwitch(config)#mac-address-table ?
```

Step 7 Setup a static MAC address

Setup a static MAC address on FastEthernet interface 0/4 as follows:

Note: Use the address that was recorded for PC4 in Step 4. The MAC address 00e0.2917.1884 is used in the example statement only.

```
ALSwitch(config)#mac-address-table static 00e0.2917.1884 interface  
fastethernet 0/4 vlan 1
```


2900:

```
ALSwitch(config)#mac-address-table static 00e0.2917.1884 fastethernet
0/4 vlan 1
```

1900:

```
ALSwitch(config)#mac-address-table permanent 00e0.2917.1884 ethernet
0/4
```

Step 8 Verify the results

- a. Enter the following to verify the MAC address table entries:

```
ALSwitch#show mac-address-table
```

- b. How many total MAC addresses are there now? _____

Step 9 List port security options

- a. Determine the options for setting port security on interface FastEthernet 0/4.

2950:

```
ALSwitch(config-if)#switchport port-security ?
aging          Port-security aging commands
mac-address    Secure mac address
maximum       Max secure addr
violation      Security Violation Mode
<cr>
```

1900:

```
ALSwitch(config)#interface ethernet 0/4
ALSwitch(config-if)#port secure ?
max-mac-count Maximum number of addresses allowed on the port
<cr>
```

- b. To allow the switchport FastEthernet 0/4 to accept only one device enter **port security** as follows:

```
ALSwitch(config-if)#switchport mode access
ALSwitch(config-if)#switchport port-security
ALSwitch(config-if)#switchport port-security mac-address sticky
```

1900:

```
ALSwitch(config-if)#port secure
```

Step 10 Verify the results

- a. Enter the following to verify the mac-address table entries:

```
ALSwitch#show mac-address-table
```

- b. How are the address types listed for the two MAC addresses? _____

- c. Show port security settings.

```
ALSwitch#show port-security
```

1900:

```
ALSwitch#show mac-address-table security
```

Step 11 Show the running configuration file

- a. Are there statements that directly reflect the security implementation in the listing of the running configuration? _____
- b. What do those statements mean? _____

Step 12 Limit the number of hosts per port

- a. On interface FastEthernet 0/4 set the port security maximum MAC count to 1 as follows:

2950:

```
ALSwitch(config-if)#switchport port-security maximum 1
```

1900:

```
ALSwitch(config)#interface Ethernet 0/4
ALSwitch(config-if)#port secure max-mac-count 1
```

- b. Disconnect the PC attached to FastEthernet 0/4. Connect to the port on the PC that has been given the IP address 192.168.1.7. This PC has not yet been attached to the switch. It may be necessary to ping the switch address 192.168.1.2 to generate some traffic.
- c. Record any observations. _____

Step 13 Configure the port to shut down if there is a security violation

- a. It has been decided that in the event of a security violation the interface should be shut down. Enter the following to make the port security action to shutdown:

2900XL:

```
ALSwitch(config-if)#switchport port-security violation shutdown
```

1900:

```
ALSwitch(config-if)#port security action shutdown
```

The default action upon address violation is "suspend"

- b. What other action options are available with port security? _____
- c. If necessary, ping the switch address 192.168.1.2 from the PC 192.168.1.7. This PC is now connected to interface FastEthernet 0/4. This ensures that there is traffic from the PC to the switch.
- d. Record any observations. _____

Step 14 Show port 0/4 configuration information

- a. To see the configuration information for just FastEthernet port 0/4, type `show interface fastethernet 0/4`, as follows, at the Privileged EXEC mode prompt:

```
ALSwitch#show interface fastethernet 0/4
```

- b. What is the state of this interface?

FastEthernet0/4 is _____, line protocol is _____

Step 15 Reactivate the port

- a. If a security violation occurs and the port is shut down, use the `no shutdown` command to reactivate it.
- b. Try reactivating this port a few times by switching between the original port 0/4 host and the new one. Plug in the original host, type the `no shutdown` command on the interface and ping using the DOS window. The `ping` will have to be repeated multiple times or use the `ping 192.168.1.2 -n 200` command. This will set the number of ping packets to 200 instead of 4. Then switch hosts and try again.

Step 16 Exit the switch

Type `exit` to leave the switch welcome screen:

```
Switch#exit
```

Once the steps are completed, logoff by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the privileged EXEC mode by typing `enable`.

If prompted for a password, enter `class` (if that does not work, ask the instructor).

```
Switch>enable
```

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the `show vlan` command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the `reload` command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the `reload` command.

5. Software restart (using the `reload` command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

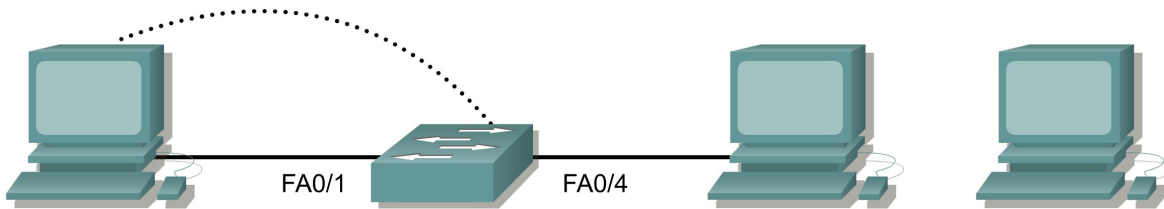
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

Lab 6.2.6 Add, Move, and Change MAC Addresses



Switch Designation	Switch Name	Enable Secret Password	Enable,VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	ALSwitch	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0

Straight-through cable	
Serial cable	
Console (Rollover)	
Crossover cable	

Objective

- Create and verify a basic switch configuration.
- Move a PC from one switch port to another and add a new PC to the switch.

Background/Preparation

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise. Instructions are also provided for the 1900 Series switch, which initially displays a User Interface Menu. Select the “Command Line” option from the menu to perform the steps for this lab.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the hostname, access and command mode passwords, as well as the management VLAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

Configure the hosts to use the same IP subnet for the address, mask, and default gateway as on the switch.

There is a third host needed for this lab. It needs to be configured with the address 192.168.1.7. The subnet mask is 255.255.255.0 and the default gateway is 192.168.1.1. Do not connect this PC to the switch yet.

Step 3 Verify connectivity

- To verify that the hosts and switch are correctly configured, ping the switch IP address from the hosts.
- Were the pings successful? _____
- If the answer is no, troubleshoot the hosts and switch configurations.

Step 4 Record the MAC addresses on the hosts

- To determine and record the layer 2 addresses of the PC network interface cards enter the following.

If running Windows 98, check by using **Start > Run > winipcfg**. Click on **More info**.

If running Windows 2000, check by using **Start > Run > cmd > ipconfig /all**.

- PC1: _____
- PC4: _____

Step 5 Determine what MAC addresses the switch has learned

- Determine what MAC addresses the switch has learned by using the `show mac-address-table` command at the privileged exec mode prompt:

```
ALSwitch#show mac-address-table
```

- How many dynamic addresses are there? _____
- How many total MAC addresses are there? _____
- Do the MAC addresses match the host MAC addresses? _____

Step 6 Determine the MAC table options

To determine the options that the `mac-address-table` command has using enter the ? option as follows:

```
ALSwitch(config)#mac-address-table ?
```

Step 7 Set up a static MAC address

To setup a static MAC address on Fast Ethernet interface 0/4 enter the following:

Note: Use the address that was recorded for PC4 in Step 4. The MAC address 00e0.2917.1884 is used in the example statement only.

```
ALSwitch(config)#mac-address-table static 00e0.2917.1884 interface  
fastethernet 0/4 vlan 1
```

1900:

```
ALSwitch(config)#mac-address-table permanent 00e0.2917.1884 ethernet 0/4
```

Step 8 Verify the results

- a. Enter the following to verify the MAC address table entries:

```
ALSwitch#show mac-address-table
```

- b. How many static addresses are there? _____

Step 9 List port security options

- a. To determine the options for setting port security on interface Fast Ethernet 0/4. Type `port security ?` from the interface configuration prompt for Fast Ethernet port 0/4.

```
ALSwitch(config)#interface fastethernet 0/4
ALSwitch(config-if)#switchport port-security ?
  aging          Port-security aging commands
  mac-address    Secure mac address
  maximum        Max secure addr
  violation      Security Violation Mode
  <cr>
```

1900:

```
ALSwitch(config)#interface ethernet 0/4
ALSwitch(config-if)#port secure ?
  max-mac-count Maximum number of addresses allowed on the port
  <cr>
```

- b. Allow the switchport on Fast Ethernet 0/4 to accept only one device by typing `port-security` as follows:

```
ALSwitch(config-if)#switchport mode access
ALSwitch(config-if)#switchport port-security
ALSwitch(config-if)#switchport port-security mac-address sticky
```

1900:

```
ALSwitch(config-if)#port secure
```

Step 10 Verify the results

- a. Enter the following to verify the `mac-address-table` entries:

```
ALSwitch#show mac-address-table
```

- b. How are the address types listed for the two MAC addresses? _____

Step 11 Show the running configuration file

- a. In the listing of the running configuration are there statements that directly reflect the security implementation? _____
 - b. What do those statements mean? _____
-

Step 12 Limit the number of hosts on each port

- a. Enter the following on interface Fast Ethernet 0/4 to set the port security maximum MAC count to 1:

```
ALSwitch(config)#interface fastethernet 0/4
ALSwitch(config-if)#switchport port-security maximum 1
```

1900:

```
ALSwitch(config)#interface ethernet 0/4
ALSwitch(config-if)#port secure max-mac-count 1
```

- b. Disconnect the PC that is attached to Fast Ethernet 0/4. Connect to the port that the PC has been given the IP address 192.168.1.7. This PC has not yet been attached to the switch. To generate some traffic ping the switch address 192.168.1.2 with the -n 50 option. For example `ping 192.168.1.2 -n 50`, where 50 is the number of pings sent.

Step 13 Move host

- a. Take the PC that had previously been connected to Fast Ethernet 0/4 and reconnect it to Fast Ethernet 0/8. The PC has been moved to a new location. This could be to another VLAN but in this instance all switch ports are in VLAN 1 and network 192.168.1.0.
- b. From this PC on Fast Ethernet 0/8, `ping 192.168.1.2 -n 50`
- c. Was the ping successful? _____
- d. Why or why not? _____
- e. Enter the following to show the `mac-address-table`.

```
ALSwitch#show mac-address-table
```

- f. Record observations about the show output. _____
-

Step 14 Clear MAC table

- a. Enter the following to clear the `mac-address-table`:

Note: This will unlock the MAC addresses from security and allow a new address to be registered.

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

- b. From the PC on the Fast Ethernet 0/8, `ping 192.168.1.2 -n 50`.

- c. Was the ping successful? _____
- d. If not troubleshoot as necessary.

Step 15 Change security settings

- a. Enter the following to show the `mac-address-table`:

```
ALSwitch#show mac-address-table
```

- b. Notice that Fast Ethernet 0/4 is secure. However, that security should be applied to the machine on port 0/8, as this is the machine that was moved from port 0/4. Remove port security from interface Fast Ethernet 0/4 as follows:

```
ALSwitch(config)#interface fastethernet 0/4
ALSwitch(config-if)#no switchport port-security
ALSwitch(config-if)#no switchport port-security mac-address sticky
ALSwitch(config-if)#no switchport port-security mac-address sticky
0008.744d.8ee2
ALSwitch(config-if)#shutdown
ALSwitch(config-if)#no shutdown
```

1900:

```
ALSwitch(config)#interface ethernet 0/4
ALSwitch(config-if)#no port secure
```

- c. Apply port security with a max-mac-count of 1 to interface Fast Ethernet 0/8 as follows:

```
ALSwitch(config)#interface fastethernet 0/8
ALSwitch(config-if)#switchport mode access
ALSwitch(config-if)#switchport port-security
ALSwitch(config-if)#switchport port-security mac-address sticky
ALSwitch(config-if)#switchport port-security maximum 1
```

1900:

```
ALSwitch(config)#interface ethernet 0/8
ALSwitch(config-if)#port secure max-mac-count 1
```

- d. Enter the following to clear the `mac-address-table`.
Note: Clearing individual entries could have also been done.

```
ALSwitch#clear mac-address-table
```

Step 16 Verify the results

- a. Verify that the `mac-address-table` has been cleared.

```
ALSwitch#show mac-address-table
```

- b. Can all PCs still successfully ping each other? _____
- c. If not troubleshoot the switch and PCs.

Step 17 Exit the switch

Type **exit** to leave the switch welcome screen as follows:

```
Switch#exit
```

Once the steps are complete, logoff by typing **exit**, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class** (if that does not work, ask the instructor).

```
Switch>enable
```

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat  
Delete filename [vlan.dat]? [Enter]  
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the `show vlan` command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the `reload` command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the `reload` command.

5. Software restart (using the `reload` command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?

Enter **y** and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

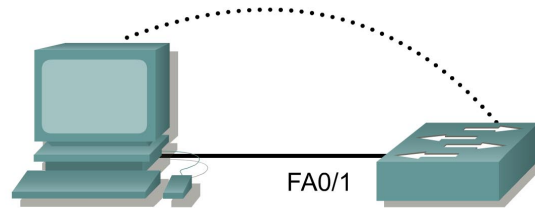
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

Reset system with factory defaults, [Y]es or [N]o?

Enter **y** and press **Enter**.

Lab 6.2.7b Managing Switch Startup Configuration Files



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	ALSwitch	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0

Straight-through cable	
Serial cable	
Console (Rollover)	
Crossover cable	

Objective

- Create and verify a basic switch configuration.
- Backup the switch startup configuration file to a TFTP server and then restore it.

Background/Preparation

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise. Instructions are also provided for the 1900 Series switch, which initially displays a User Interface Menu. Select the “Command Line” option from the menu to perform the steps for this lab.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the hostname, access, and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the host attached to the switch

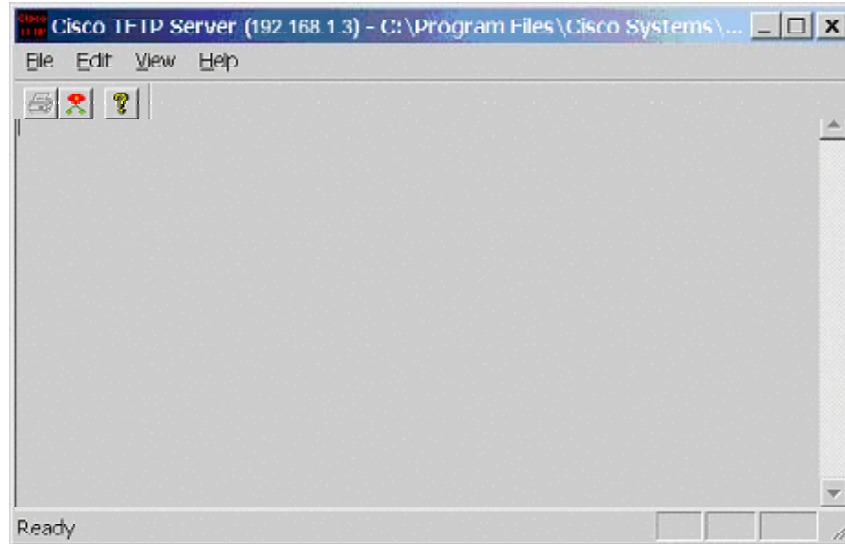
Configure the host to use the same subnet for the address, mask, and default gateway as on the switch. This host will act as the TFTP server in this lab. Be sure to take note of the IP address assigned.

Step 3 Verify connectivity

- To verify that the host and switch are correctly configured, ping the switch IP address from the host.
- Was the ping successful? _____
- If the answer is no, troubleshoot the host and switch configurations.

Step 4 Starting and configuring the Cisco TFTP server

- The TFTP server that is shown may not be like the one that is used in this classroom. Please check with the instructor for the operating instructions of the TFTP server used in place of the Cisco TFTP server.



- Once the TFTP server is running and shows the correct address configuration on the workstation, copy the IOS file to the switch.

Step 5 Copying the startup configuration file to TFTP server

- Verify that the TFTP server is running and that it can be pinged from the switch.
- What is the IP address of the TFTP server? _____
- From the console session, enter `show flash`.

2900:

```
dir flash:
```

1900:

```
(command not available)
```

- What is the name and length of the startup configuration image stored in flash?

-
- From the console session in the Privileged EXEC mode, enter the `copy running-config startup-config` command, to make sure that the running configuration file is saved to the

startup configuration file. Then type the `copy startup-config tftp` command. At the prompt enter the IP address of the TFTP server as follows:

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

```
ALSwitch#copy start tftp
Address or name of remote host []? 192.168.1.3
Destination filename [alswitch-confg]?[enter]
!!
744 bytes copied in 1.60 secs (744 bytes/sec)
ALSwitch#
```

1900:

```
ALSwitch#copy nvram tftp://192.168.1.3/alswitch-config
Configuration upload is successfully completed
```

Step 6 Verify the transfer to the TFTP server

- Verify the transfer to the TFTP server by checking the log file. Click on **View > Log File**. The output should look similar to the following:

```
Mon Sep 16 14:10:08 2002: Receiving 'switch.config' file from
192.168.1.2 in binary mode
Mon Sep 16 14:11:14 2002: Successful.
```

- Verify the 'switch.config' file size in the TFTP server directory. To locate it click on **View > Options**. This will show the TFTP server root directory. The output should be similar to the following, unless the default directories were changed:

```
C:\Program Files\Cisco Systems\Cisco TFTP Server
```

- Locate this directory using the File Manager and look at the detail listing of the file. The file length in the `show start` command should be the same file size as the file stored on the TFTP server. If the file sizes are not identical in size, check with the instructor.

Step 7 Restore the startup configuration file from the TFTP server

- To restore the startup configuration file, first the switch must be erased. Then reconfigure the switch with just the VLAN 1 IP address of 192.168.1.2 255.255.255.0. Finally type the command `copy tftp startup-config` at the Privileged EXEC mode prompt as shown in the following:

```
Switch#copy tftp startup-config
Address or name of remote host []? 192.168.1.10
Source filename []? alswitch-confg
Destination filename [startup-config]? Accessing
tftp://192.168.1.10/alswitch-confg...
Loading alswitch-confg .from 192.168.1.10 (via Vlan1): !
[OK - 1622 bytes]
[OK]
1622 bytes copied in 22.796 secs (71 bytes/sec)
Switch#
```


Note: It is important that this process is not interrupted.

Was the operation successful? _____

1900:

```
ALSwitch#copy tftp://192.168.1.3/alswitch-config nvram
TFTP successfully downloaded configuration file
```

Step 8 Test the restored startup configuration image (Not supported on the 1900)

Verify that the switch image is correct. To do this, cycle the switch power and observe the switch prompt. If it has returned to the name that was assigned to it in the original configuration, the restoration is complete. Type the command `show startup-config` to see the restored configuration.

Once these steps are completed, logoff by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the privileged EXEC mode by typing `enable`.
If prompted for a password, enter `class` (if that does not work, ask the instructor).

```
Switch>enable
```

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the `show vlan` command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the `reload` command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the `reload` command.

5. Software restart (using the `reload` command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

```
This command resets the switch with VTP parameters set to factory defaults.
```

```
All other parameters will be unchanged.
```

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter **y** and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

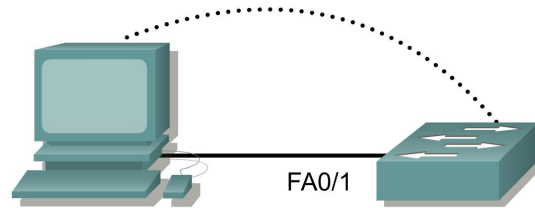
```
#delete nvram
```

```
This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.
```

```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter **y** and press **Enter**.

Lab 6.2.9 Firmware Upgrade of a Catalyst 2950 Series Switch



Switch Designation	Switch Name	Enable Password	Secret Password	Enable,VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	ALSwitch	class		cisco	192.168.1.2	192.168.1.1	255.255.255.0

Straight-through cable	
Serial cable	
Console (Rollover)	
Crossover cable	

Objective

- Create and verify a basic switch configuration.
- Upgrade the IOS and HTML files from a file supplied by the instructor.

Background/Preparation

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise.

Start a HyperTerminal session.

Notes: This lab requires that a combination of an IOS image and the HTML file called **c2950-c3h2s-mz.120-5.3.WC.1.tar** be placed in the default TFTP server directory (folder) by the instructor or student. This file should be downloaded by the instructor from the Cisco Connection on-line software center. It has been determined that this file is the latest update for the Catalyst 2950. This has the same file name stem as the current image. However, for the purpose of the lab, assume that this is an update. The IOS update release contains new HTML files to support changes to the web interface.

This lab requires that there is a saved copy of the current configuration file as backup.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the hostname, access, and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the host attached to the switch

Configure the host to use the same IP subnet for the address, mask, and default gateway as on the switch.

Step 3 Verify connectivity

- To verify that the host and switch are correctly configured, ping the switch IP address from the host.
- Was the ping successful? _____
- If the answer is no, troubleshoot the host and switch configurations.

Step 4 Display the name of the running image file

- Display the name of the running image file using the `show boot` command from the Privileged EXEC mode prompt as follows:

```
ALSwitch#show boot
BOOT path-list:
Config file:  flash:config.text
Enable Break: no
Manual Boot:  no
HELPER path-list:
NVRAM/Config file
buffer size:  32768
ALSwitch#
```

- If there is no software image defined in the boot path, enter `dir flash:` or `show flash` to display the contents as follows:

```
ALSwitch#dir flash:
Directory of flash:/

 2 -rwx 1674921 Mar 01 1993 01:28:10 c2950-c3h2s-mz.120-5.3.WC.1.bin
 3 -rwx 269 Jan 01 1970 00:00:57 env_vars
 4 drwx 10240 Mar 01 1993 00:21:13 html
165-rwx 965 Mar 01 1993 00:22:23 config.text

7741440 bytes total (4778496 bytes free)
```

Step 5 Prepare for the new image

- If the switch has enough free memory as shown in the last command, rename the existing IOS file to the same name with the `.old` extension as follows:

Note: If there is not enough memory, make sure there is a copy of the IOS on the TFTP server.

```
ALSwitch#rename flash:c2950-c3h2s-mz.120-5.3.WC.1.bin flash:c2950-
c3h2s-mz.120-5.3.WC.1.old
```

- b. Enter the following to verify that the renaming was successful:

```
ALSwitch#dir flash:
Directory of flash:/

 2 -rwx 1674921 Mar 01 1993 01:28:10 c2950-c3h2s-mz.120-5.3.WC.1.old
 3 -rwx 269 Jan 01 1970 00:00:57 env_vars
 4 drwx 10240 Mar 01 1993 00:21:13 html
167 -rwx 965 Mar 01 1993 00:22:23 config.text

7741440 bytes total (4778496 bytes free)
ALSwitch#
```

- c. As a precaution, enter the following to disable access to the switch HTML pages:

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

- d. Remove existing html files.

```
ALSwitch#delete flash:html/*
```

Step 6 Extract the new IOS image and HTML files into flash memory

- a. Enter the following to extract the new IOS image and HTML files into flash memory:

```
ALSwitch#archive tar /x tftp://192.168.1.3/c2950-c3h2s-mz.120-5.3.WC.1.tar flash:
```

Note: Depending on the TFTP server being used only one slash (/) after the IP address of the server may be needed.

- b. Re-enable access to the switch HTML pages as follows:

```
ALSwitch(config)#ip http server
```

Step 7 Associate the new boot file

Enter the `boot` command with the name of the *new image* filename at the configuration mode prompt.

```
ALSwitch(config)#boot system flash:c2950-c3h2s-mz.120-5.4.WC.1.bin
```

Step 8 Restart the switch

- Restart the switch by using the `reload` command to see if the new IOS loaded. Use the `show version` command to see the IOS file name.
- What was the name of the IOS file the switch booted from? _____
- Was this the proper file name? _____
- If the IOS filename is now correct remove the backup file from flash memory using the command `delete flash: c2950-c3h2s-mz.120-5.3.WC.1.old` from the Privileged EXEC mode prompt to remove the backup file.

Once the steps are completed, logoff by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the privileged EXEC mode by typing `enable`.

If prompted for a password, enter `class` (if that does not work, ask the instructor).

```
Switch>enable
```

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the `show vlan` command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the `reload` command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the `reload` command.

5. Software restart (using the `reload` command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

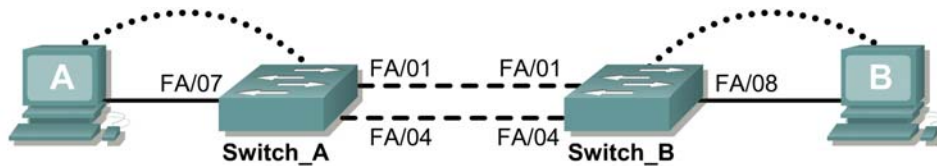
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

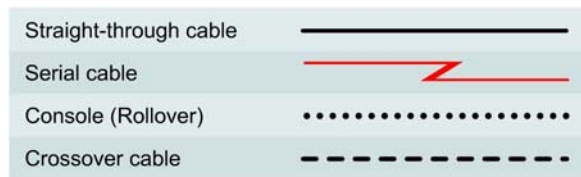
```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

Lab 7.2.4 Selecting the Root Bridge



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	Switch_A	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0
Switch 2	Switch_B	class	cisco	192.168.1.3	192.168.1.1	255.255.255.0



Objective

- Create a basic switch configuration and verify it.
- Determine which switch is selected as the root switch with the factory default settings.
- Force the other switch to be selected as the root switch.

Background/Preparation

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switches

Configure the hostname, access and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switches

Configure the host to use the same subnet for the address, mask, and default gateway as on the switch.

Step 3 Verify connectivity

- a. To verify that the hosts and switches are correctly configured, ping the switches from the hosts.
- b. Were the pings successful? _____
- c. If the answer is no, troubleshoot the hosts and switches configurations.

Step 4 Display the show interface VLAN options

- a. Type `show interface vlan 1`.
- b. List some of the options available: _____

Step 5 Display VLAN interface information

- a. On Switch_A, type the command `show interface VLAN 1` at the Privileged EXEC mode prompt as follows:

```
Switch_A#show interface vlan 1
```

- b. What is the MAC address of the switch? _____
- c. On Switch_B type the command `show interface VLAN 1` at the Privileged EXEC mode prompt as follows:

```
Switch_B#show interface vlan 1
```

- d. What is the MAC address of the switch? _____
- e. Which switch should be the root of the spanning-tree for VLAN 1? _____

Step 6 Display the spanning-tree table on each switch

- a. At the Privileged EXEC mode prompt, type the following on Switch_A:
Type `show spanning-tree brief` if running version 12.0 of the IOS. If running version 12.1 of the IOS, type `show spanning-tree`.

```
Switch_A#show spanning-tree brief
```

- b. On Switch_B type `show spanning-tree brief` at the Privileged EXEC mode prompt as follows:

```
Switch_B#show spanning-tree brief
```

Examine the output and answer the following questions.

- c. Which switch is the root switch? _____
- d. What is the priority of the root switch? _____
- e. What is the bridge id of the root switch? _____
- f. Which ports are forwarding on the root switch? _____
- g. Which ports are blocking on the root switch? _____
- h. What is the priority of the non-root switch? _____
- i. What is the bridge id of the non-root switch? _____

- j. Which ports are forwarding on the non-root switch? _____
- k. Which ports are blocking on the non-root switch? _____
- l. What is the status of the link light on the blocking port? _____

Step 7 Reassign the root bridge

- a. It has been determined that the switch selected as the root bridge, by using default values, is not the best choice. It is necessary to force the “other” switch to become the root switch.
- b. In the example output given the root switch by default is Switch_A. Switch_B is preferred as the root switch. Go to the console and enter configuration mode if necessary.
- c. Determine the parameters that can be configured for the Spanning-Tree Protocol by issuing the following:

```
Switch_B(config)#spanning-tree ?
```

- d. List the options. _____

- e. Set the priority of the switch that is not root to 4096.
If version 12.0 is used, enter the following:

```
Switch_B(config)#spanning-tree priority 1
Switch_B(config)#exit
```

If version 12.1 is used, enter the following:

```
Switch_B(config)#spanning-tree vlan 1 priority 4096
Switch_B(config)#exit
```

Step 8 Display the switch spanning-tree table

- a. At the Privileged EXEC mode prompt, type the following on Switch_A:
Note: Type `show spanning-tree brief` if running version 12.0 of the IOS. If running version 12.1 of the IOS, type `show spanning-tree`.

```
Switch_A#show spanning-tree brief
```

- b. On Switch_B type `show spanning-tree brief` at the Privileged EXEC mode prompt as follows:

```
Switch_B#show spanning-tree brief
```

Examine the output and answer the following questions.

- c. Which switch is the root switch? _____
- d. What is the priority of the root switch? _____
- e. Which ports are forwarding on the root switch? _____
- f. Which ports are blocking on the root switch? _____

- g. What is the priority of the non-root switch? _____
- h. Which ports are forwarding on the non-root switch? _____
- i. Which ports are blocking on the non-root switch? _____
- j. What is the status of the link light on the blocking port? _____

Step 9 Verify the running configuration file on the root switch

- a. On the switch that was changed to be the root bridge, type `show running-config` at the Privileged EXEC mode prompt.
- b. Is there an entry in the running configuration file that specifies the spanning-tree priority of this router? _____
- c. What does that entry say? _____

Note: The output is different depending on if the IOS used is version 12.0 or version 12.1.

Once the steps are complete, log off by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class** (if that does not work, ask the instructor).

```
Switch>enable
```

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat  
Delete filename [vlan.dat]?[Enter]  
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the **show vlan** command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the **reload** command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the **reload** command.

5. Software restart (using the **reload** command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the privileged EXEC mode enter the command `reload`.

```
Switch#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

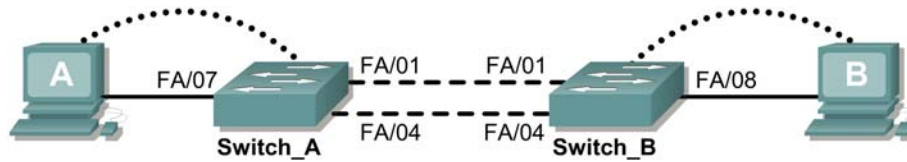
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

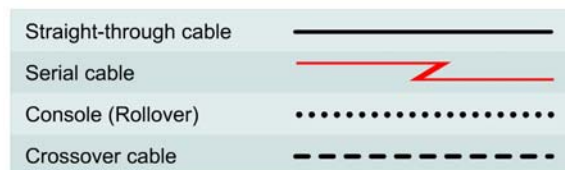
```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

Lab 7.2.6 Spanning-Tree Recalculation



Switch Designation	Switch Name	Enabel Secret Password	Enable, VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	Switch_A	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0
Switch 2	Switch_B	class	cisco	192.168.1.3	192.168.1.1	255.255.255.0



Objective

- Create a basic switch configuration and verify it.
- Observe the behavior of spanning-tree algorithm in presence of switched network topology changes.

Background/Preparation

Cable a network similar to one of the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switches

Configure the hostname, access and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switches

Configure the host to use the same IP subnet for the address, mask, and default gateway as on the switch.

Step 3 Verify connectivity

- a. To verify that the hosts and switches are correctly configured, ping the switches from the hosts.
- b. Were the pings successful? _____
- c. If the answer is no, troubleshoot the hosts and switches configurations.

Step 4 Look at the show interface information

- a. On both switches, type the command `show interface VLAN 1` at the Privileged EXEC prompt as follows:

```
Switch_A#show interface vlan 1
```

- b. What is the MAC address of the switch? _____

```
Switch_B#show interface vlan 1
```

- c. What is the MAC address of the switch? _____
- d. Which switch should be the root of the spanning-tree for VLAN 1? _____

Step 5 Look at the spanning-tree table on each switch

- a. At the Privileged EXEC mode prompt, type the following on Switch_A:
Note: Type `show spanning-tree brief` if running version 12.0 of the IOS. If running version 12.1 of the IOS, type just `show spanning-tree`. Different versions of IOS have different options for this command.

```
Switch_A#show spanning-tree brief
```

- b. On Switch_B type `show spanning-tree brief` at the Privileged EXEC mode prompt as follows:

```
Switch_B#show spanning-tree brief
```

- c. Examine the command output and answer the following questions.
- d. Which switch is the root switch? _____

- e. Record the states of the first 12 interfaces and ports of each switch.

Switch A	Port #	Switch B
	1	
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
	10	
	11	
	12	

Step 6 Remove a cable on the switch

- Remove the cable from the forwarding port on the non-root switch. For this example this is interface FastEthernet 0/1 on Switch_B.
 - Wait for at least two minutes.
 - What has happened to the switch port LEDs?
-

Step 7 Look at the spanning-tree table on each switch

- Type the following on Switch_A at the Privileged EXEC mode prompt.
Note: Type `show spanning-tree brief` if running version 12.0 of the IOS. If running version 12.1 of the IOS, type just `show spanning-tree`. Different versions of IOS have different options for this command.

```
Switch_A#show spanning-tree brief
```

- On Switch_B type `show spanning-tree brief` at the Privileged EXEC mode prompt as follows:

```
Switch_B#show spanning-tree brief
```

- What changes have taken place in the command output?

On Switch_A? _____

On Switch_B? _____

Step 8 Replace the cable in the switch

- Replace the cable in the port that it was removed from. For this example this is interface FastEthernet 0/1 on Switch_B.
- Wait for at least two minutes.
- What has happened to the switch port LEDs? _____

Step 9 Look at the spanning-tree table on each switch

- a. At the Privileged EXEC mode prompt, type the following on Switch_A:

Note: Type `show spanning-tree brief` if running version 12.0 of the IOS. If running version 12.1 of the IOS, type just `show spanning-tree`. Different versions of IOS have different options for this command.

```
Switch_A#show spanning-tree brief
```

- b. On Switch_B type `show spanning-tree brief` at the Privileged EXEC mode prompt as follows:

```
Switch_B#show spanning-tree brief
```

- c. What changes have taken place in the command output?

On Switch_A? _____

On Switch_B? _____

Once the steps are completed, log off by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class** (if that does not work, ask the instructor).

```
Switch>enable
```

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat  
Delete filename [vlan.dat]?[Enter]  
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the **show vlan** command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the **reload** command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the **reload** command.

5. Software restart (using the **reload** command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

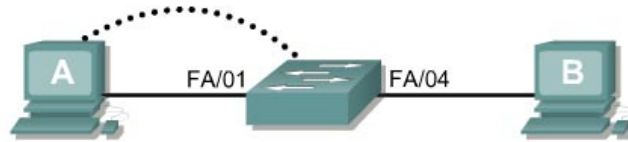
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

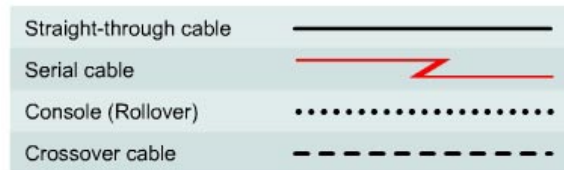
```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

Lab 8.2.3 Configuring Static VLANs



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	Switch_A	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0



Objective

- Create a basic switch configuration and verify it.
- Determine the switch firmware version.
- Create two VLANs, name them and assign member ports to them.

Background/Preparation

When managing a switch, the Management Domain is always VLAN 1. The Network Administrator's workstation must have access to a port in the VLAN 1 Management Domain. All ports are assigned to VLAN 1 by default.

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise. Instructions are also provided for the 1900 Series switch, which initially displays a User Interface Menu. Select the "Command Line" option from the menu to perform the steps for this lab.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the hostname, access and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

Configure the host to use the same subnet for the address, mask, and default gateway as on the switch.

Step 3 Verify connectivity

- a. To verify that the host and switch are correctly configured, ping the switch from the host.
- b. Was the ping successful? _____
- c. If the answer is no, troubleshoot the host and switch configurations.

Step 4 Show the IOS version

- a. It is very important to know the version of the operating system. Differences between versions may change how commands are entered. Type the `show version` command at the User EXEC or Privileged EXEC mode prompt as follows:

```
Switch_A#show version
```

- b. What version of the switch IOS is displayed? _____
- c. Does this switch have standard edition or Enterprise edition software? _____
- d. What is the Firmware or IOS Version running on this switch? _____

Step 5 Display the VLAN interface information

- a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

```
1900:
```

```
Switch_A#show vlan-membership
```

- b. Which ports belong to the default VLAN? _____
- c. How many VLANs are set up by default on the switch? _____
- d. What does the VLAN 1003 represent? _____
- e. How many ports are in the 1003 VLAN? _____

Step 6 Create and name two VLANs

Enter the following commands to create and name two VLANs:

```
Switch_A#vlan database
Switch_A(vlan)#vlan 2 name VLAN2
Switch_A(vlan)#vlan 3 name VLAN3
Switch_A(vlan)#exit

1900:
Switch_A#config terminal
Switch_A(config)#vlan 2 name VLAN2
Switch_A(config)#vlan 3 name VLAN3
```

Step 7 Display the VLAN interface information

- a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

- b. Are there new VLANs in the listing? _____

```
1900:
```

```
Switch_A#show vlan-membership
```

- c. Do they have any ports assigned to them yet? _____

Step 8 Assign ports to VLAN 2

Assigning ports to VLANs must be done from the interface mode. Enter the following commands to add port 2 to VLAN 2:

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/2
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 2
Switch_A(config-if)#end
```

```
1900:
```

```
Switch_A#config terminal
Switch_A(config)#interface Ethernet 0/2
Switch_A(config-if)#vlan static 2
Switch_A(config)#end
```

Step 9 Display the VLAN interface information

- a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

```
1900:
```

```
Switch_A#show vlan-membership
```

- b. Is port 2 assigned to VLAN 2? _____

- c. Is the port still listed in the default VLAN? _____

Step 10 Assign a port to VLAN 3

Assigning ports to VLANs must be done from the interface mode. Enter the following commands to add port 3 to VLAN3

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/3
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 3
Switch_A(config-if)#end
```

1900:

```
Switch_A#config terminal
Switch_A(config)#interface Ethernet 0/3
Switch_A(config)#vlan static 3
Switch_A(config)#end
```

Step 11 Look at the VLAN interface information

- a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

1900:

```
Switch_A#show vlan-membership
```

- b. Is port 3 assigned to VLAN 3? _____
- c. Is the port still listed in the default VLAN? _____

Step 12 Look at only VLAN2 information

- a. Instead of displaying all of the VLANs type the `show vlan id 2` command at the Privileged EXEC mode prompt as follows:

```
Switch_A#show vlan id 2
```

1900:

```
Switch_A#show vlan 2
```

- b. Does this command supply any more information than the show VLAN command? _____

Step 13 Look at only VLAN2 information with a different command (1900: Omit this step)

- a. Instead of displaying all of the VLANs type the `show vlan name VLAN2` command at the Privileged EXEC mode prompt.

```
Switch_A#show vlan name VLAN2
```


b. Does this command supply any more information than the show VLAN command? _____

Once the steps are completed, log off by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the privileged EXEC mode by typing `enable`.

If prompted for a password, enter `class` (if that does not work, ask the instructor).

```
Switch>enable
```

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the `show vlan` command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the `reload` command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the `reload` command.

5. Software restart (using the `reload` command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

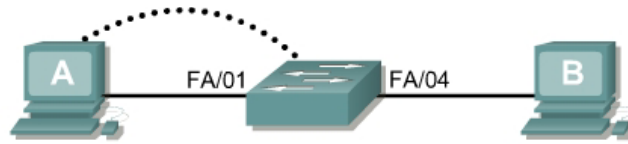
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

Lab 8.2.4 Verifying VLAN Configurations



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	Switch_A	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0

Straight-through cable	
Serial cable	
Console (Rollover)	
Crossover cable	

Objective

- Create a basic switch configuration and verify it.
- Create two VLANs.
- Name the VLANs and assign multiple member ports to them.
- Test functionality by moving a workstation from one VLAN to another.

Background/Preparation

When managing a switch, the Management Domain is always VLAN 1. The Network Administrator's workstation must have access to a port in the VLAN 1 Management Domain. All ports are assigned to VLAN 1 by default. This lab will also help demonstrate how VLANs can be used to separate traffic and reduce broadcast domains.

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise. Instructions are also provided for the 1900 Series switch, which initially displays a User Interface Menu. Select the "Command Line" option from the menu to perform the steps for this lab.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the hostname, access and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

Configure the hosts to use the same subnet for the address, mask, and default gateway as on the switch.

Step 3 Verify connectivity

- a. To verify that the hosts and switch are correctly configured, ping the switch from the hosts.
- b. Were the pings successful? _____
- c. If the answer is no, troubleshoot the host and switch configurations.

Step 4 Display the VLAN interface information

- a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

```
1900:
```

```
Switch_A#show vlan-membership
```

- b. Which ports belong to the default VLAN? _____

Step 5 Create and name two VLANs

Enter the following commands to create and name two VLANs:

```
Switch_A#vlan database
Switch_A(vlan)#vlan 2 name VLAN2
Switch_A(vlan)#vlan 3 name VLAN3
Switch_A(vlan)#exit
```

```
1900:
```

```
Switch_A#config terminal
Switch_A(config)#vlan 2 name VLAN2
Switch_A(config)#vlan 3 name VLAN3
Switch_A(config)#exit
```

Step 6 Assign ports to VLAN 2

Assigning ports to VLANs must be done from the interface mode. Enter the following commands to add ports 4, 5 and 6 to VLAN 2.

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/4
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 2
Switch_A(config-if)#interface fastethernet 0/5
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 2
Switch_A(config-if)#interface fastethernet 0/6
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 2
Switch_A(config-if)#end
```

1900:

```
Switch_A#config terminal
Switch_A(config)#interface ethernet 0/4
Switch_A(config-if)#vlan static 2
Switch_A(config-if)#interface ethernet 0/5
Switch_A(config-if)#vlan static 2
Switch_A(config-if)#interface ethernet 0/6
Switch_A(config-if)#vlan static 2
Switch_A(config-if)#end
```

Step7 Display the VLAN interface information

- a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

1900:

```
Switch_A#show vlan-membership
```

- b. Are ports 4 through 6 assigned to VLAN 2?
-

Step 8 Assign ports 7, 8, and 9 to VLAN 3

Enter the following commands to add ports 7, 8 and 9:

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/7
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 3
Switch_A(config-if)#interface fastethernet 0/8
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 3
Switch_A(config-if)#interface fastethernet 0/9
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 3
Switch_A(config-if)#end
```

1900:

```
Switch_A#config terminal
Switch_A(config)#interface ethernet 0/7
Switch_A(config-if)#vlan static 3
Switch_A(config-if)#interface ethernet 0/8
Switch_A(config-if)#vlan static 3
Switch_A(config-if)#interface ethernet 0/9
Switch_A(config-if)#vlan static 3
Switch_A(config-if)#end
```

Step 9 Display the VLAN interface information

- a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

1900:

```
Switch_A#show vlan-membership
```

- b. Are ports 7 through 9 assigned to VLAN 3?
-

Step 10 Test the VLANs

Ping from the host in port 0/4 to the host in port 0/1.

- a. Was the ping successful? _____

- b. Why? _____

Ping from the host in port 0/1 to the host in port 0/4.

- c. Was the ping successful? _____

- d. Why? _____

Ping from the host in port 0/4 to the switch IP 192.168.1.2.

- e. Was the ping successful? _____

- f. Why? _____

Ping from the host in port 0/1 to the switch IP 192.168.1.2.

- g. Was the ping successful? _____

- h. Why? _____

Step 11 Move a host

Move the host in port 0/4 to port 0/3. Wait until the port LED goes green and then go to the next step.

Step 12 Test the VLANs

Ping from the host in port 0/3 to the host in port 0/1.

- a. Was the ping successful? _____

- b. Why? _____

Ping from the host in port 0/1 to the host in port 0/3.

- c. Was the ping successful? _____

Ping from the host in port 0/3 to the switch IP 192.168.1.2.

- d. Was the ping successful? _____

Step 13 Move hosts

Move the host in port 0/3 to port 0/4 and the host in port 0/1 to port 0/5. Wait until the port LEDs go green and then go to the next step.

Step 14 Test the VLANs

Ping from the host in port 0/4 to the host in port 0/5.

- a. Was the ping successful? _____

- b. Why? _____

Ping from the host in port 0/5 to the host in port 0/4.

c. Was the ping successful? _____

Ping from the host in port 0/4 to the switch IP 192.168.1.2.

d. Was the ping successful? _____

Ping from the host in port 0/5 to the switch IP 192.168.1.2.

e. Was the ping successful? _____

f. Why? _____

Step 15 Move hosts

Move the host in port 0/4 to port 0/8. Wait until the port LED goes green and then go to the next step.

Step 16 Test the VLANs

Ping from the host in port 0/4 to the host in port 0/8.

a. Was the ping successful? _____

b. Why? _____

Ping from the host in port 0/8 to the host in port 0/4.

c. Was the ping successful? _____

Ping from the host in port 0/4 to the switch IP 192.168.1.2.

d. Was the ping successful? _____

Ping from the host in port 0/8 to the switch IP 192.168.1.2.

e. Was the ping successful? _____

Once the steps are completed, log off by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the Privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class** (if that does not work, ask the instructor).

```
Switch>enable
```

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat  
Delete filename [vlan.dat]?[Enter]  
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the **show vlan** command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the **reload** command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the **reload** command.

5. Software restart (using the **reload** command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the Privileged EXEC mode enter the command `reload`.

```
Switch(config) #reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

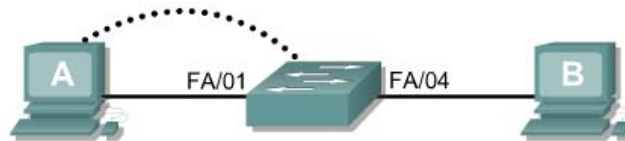
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

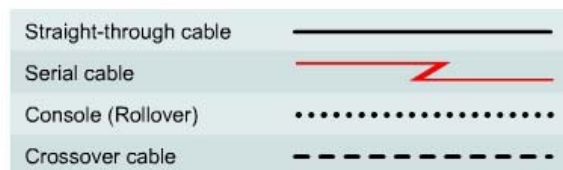
```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

Lab 8.2.6 Deleting VLAN Configurations



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	Switch_A	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0



Objective

- Create a basic switch configuration and verify it.
- Create two VLANs.
- Name the VLANs and assign multiple member ports to them.
- Remove an interface from a VLAN and Delete a VLAN
- Understand why it is not possible to delete VLAN 1.

Background/Preparation

When managing a switch, the Management Domain is always VLAN 1. The Network Administrator's workstation must have access to a port in the VLAN 1 Management Domain. All ports are assigned to VLAN 1 by default. This lab will also help demonstrate how to remove an interface from and existing VLAN and how to delete an entire VLAN.

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise. Instructions are also provided for the 1900 Series switch, which initially displays a User Interface Menu. Select the "Command Line" option from the menu to perform the steps for this lab.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the hostname, access and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

Configure the hosts to use the same subnet for the address, mask, and default gateway as on the switch.

Step 3 Verify connectivity

- a. To verify that the hosts and switch are correctly configured, ping the switch from the hosts.
- b. Were the pings successful? _____
- c. If the answer is no, troubleshoot the host and switch configurations.

Step 4 Display the VLAN interface information

- a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

```
1900:
```

```
Switch_A#show vlan-membership
```

- b. Which ports belong to the default VLAN? _____

Step 5 Create and name two VLANs

Enter the following commands to create and name two VLANs:

```
Switch_A#vlan database
Switch_A(vlan) #vlan 2 name VLAN2
Switch_A(vlan) #vlan 3 name VLAN3
Switch_A(vlan) #exit
```

```
1900:
```

```
Switch_A#configure terminal
Switch_A(config) #vlan 2 name VLAN2
Switch_A(config) #vlan 3 name VLAN3
```

Step 6 Assign ports to VLAN 2

Assigning ports to VLANs must be done from the interface mode. Enter the following commands to add ports 4, 5 and 6 to VLAN 2.

```
Switch_A#configure terminal
Switch_A(config) #interface fastethernet 0/4
Switch_A(config-if) #switchport mode access
Switch_A(config-if) #switchport access vlan 2
Switch_A(config-if) #interface fastethernet 0/5
Switch_A(config-if) #switchport mode access
Switch_A(config-if) #switchport access vlan 2
Switch_A(config-if) #interface fastethernet 0/6
Switch_A(config-if) #switchport mode access
```

```
Switch_A(config-if)#switchport access vlan 2
Switch_A(config-if)#end
```

1900:

```
Switch_A#configure terminal
Switch_A(config)#interface Ethernet 0/4
Switch_A(config-if)#vlan static 2
Switch_A(config-if)#interface Ethernet 0/5
Switch_A(config-if)#vlan static 2
Switch_A(config-if)#interface Ethernet 0/6
Switch_A(config-if)#vlan static 2
Switch_A(config)#end
```

Step 7 Display the VLAN interface information

- a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

1900:

```
Switch_A#show vlan-membership
```

- b. Are ports 4 through 6 assigned to VLAN 2? _____

Step 8 Assign Ports to VLAN 3

```
Switch_A#configure terminal
Switch_A(config-if)#interface fastethernet 0/7
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 3
Switch_A(config-if)#interface fastethernet 0/8
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 3
Switch_A(config-if)#interface fastethernet 0/9
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 3
Switch_A(config-if)#end
```

Step 9 Display the VLAN Interface Information

- a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt.

```
Switch_A#show vlan
```

- b. Are ports 7-9 assigned to VLAN 3? _____

Step 10 Test the VLANs

Ping from the host in port 0/4 to the host in port 0/1.

- a. Was the ping successful? _____

Why? _____

Ping from the host in port 0/1 to the host in port 0/4.

b. Was the ping successful? _____

Why? _____

Ping from the host in port 0/4 to the switch IP 192.168.1.2.

c. Was the ping successful? _____

d. Why? _____

Ping from the host in port 0/1 to the switch IP 192.168.1.2.

d. Was the ping successful? _____

Why? _____

Step 11 Delete a Host from a VLAN

To remove a host from a VLAN, use the **no** form of the **switchport** commands in the port interface configuration mode.

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/4
Switch_A(config-if)#no switchport access vlan 2
```

1900:

```
Switch_A#configure terminal
Switch_A(config)#interface Ethernet 0/4
Switch_A(config-if)#no vlan-membership 2
Switch_A(config-if)#end
```

Step 12 Display the VLAN Interface Information

a. On Switch_A, type the command **show vlan** at the Privileged EXEC prompt.

```
Switch_A#show vlan
```

b. Is port 0/4 removed from VLAN 2? _____

Step 13 Delete a VLAN

a. To remove an entire VLAN, enter the VLAN database mode and use the negative form of the command.

```
Switch_A#vlan database
Switch_A(vlan)#no vlan 3
Deleting VLAN 3
Switch_A(vlan)#exit
```

1900:

```
Switch_A#config terminal
Switch_A(config)#interface ethernet 0/7
Switch_A(config-if)#no vlan 3
Switch_A(config-if)#exit
```

Step 14 Display the VLAN Interface Information

- a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt.

```
Switch_A#show vlan
```

- b. Is VLAN 3 removed? _____
- c. What happened to the ports that were released from VLAN 3? _____

Step 15 Delete VLAN 1

- a. Try to delete VLAN 1, which is the default VLAN, the same way that you deleted VLAN 3.

```
Switch_A#vlan database
Switch_A(vlan)#no vlan 1
A default VLAN may not be deleted.
Switch_A(vlan)#exit
```

1900:

```
Switch_A#config t
Switch_A(config)#no vlan 1
Switch_A(config)#no vlan 1
                        ^

% Invalid input detected at '^' marker.
Switch_A(config)#exit
```

- b. The default VLAN cannot be deleted.

Once the steps are completed, logoff by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the Privileged EXEC mode by typing **enable**.

If prompted for a password, enter **class** (if that does not work, ask the instructor).

```
Switch>enable
```

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat  
Delete filename [vlan.dat]?[Enter]  
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the **show vlan** command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the **reload** command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the **reload** command.

5. Software restart (using the **reload** command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the Privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

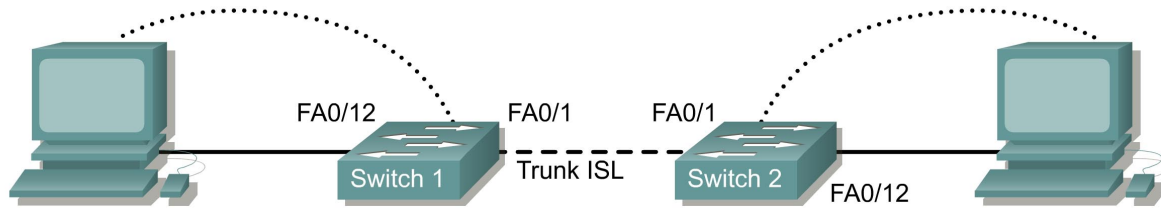
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

Lab 9.1.5a Trunking with ISL



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, VLAN 1 IP and Console Passwords	VLAN 1 IP Address	Subnet Mask	VLAN Names and Numbers	Switch Port Assignments
Switch 1	Switch_A	class	cisco	192.168.1.2	255.255.255.0	VLAN 1 Native VLAN 10 Accounting VLAN 20 Marketing VLAN 30 Engineering	fa0/2 - 0/3 fa0/4 - 0/6 fa0/7 - 0/9 fa0/10 - 0/12
Switch 2	Switch_B	class	cisco	192.168.1.3	255.255.255.0	VLAN 1 Native VLAN 10 Accounting VLAN 20 Marketing VLAN 30 Engineering	fa0/2 - 0/3 fa0/4 - 0/6 fa0/7 - 0/9 fa0/10 - 0/12

Straight-through cable Serial cable Console (Rollover) Crossover cable

Objective

- Create a basic switch configuration and verify it.
- Create multiple VLANs, name them and assign multiple member ports to them.
- Create an ISL trunk line between the two switches to allow communication between paired VLANs.
- Test the VLANs functionality by moving a workstation from one VLAN to another.

Background/Preparation

Note: The use of Catalyst 2950 switches is not appropriate for this lab as they only support 802.1q trunking.

Trunking changes the formatting of the packets. The ports need to be in agreement as to which format is being used to transmit data on the trunk or no data will be passed. If there is different trunking encapsulation on the two ends of the link they will not be able to communicate. Similar situation will occur if one of the ports is configured in trunking mode, unconditionally, and the other one is in access mode, unconditionally.

When managing a switch, the Management Domain is always VLAN 1. The Network Administrator's workstation must have access to a port in the VLAN 1 Management Domain. All ports are assigned to VLAN 1 by default. This lab will also help demonstrate how VLANs can be used to separate traffic.

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2900 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the hostname, access and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

Configure the IP address, mask, and default gateway on each host. Be sure to choose addresses that are on the same subnet as the switch.

Step 3 Verify connectivity

- a. To verify that the host and switch are correctly configured, ping the switches from the host.
- b. Were the pings successful? _____
- c. If the answer is no, troubleshoot the host and switches configurations.

Step 4 Display the VLAN interface information

On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

Note: There should be an entry for VLAN 1 and the default VLANs (1002 +). If other VLANs appear, they could be deleted as instructed in Step 2 of the Erasing and Reloading instructions at the end of this lab or refer to the Lab Exercise: Deleting VLAN Configurations.

Step 5 Create and name three VLANs

Enter the following commands to create and name three VLANs:

```
Switch_A#vlan database
Switch_A(vlan)#vlan 10 name Accounting
Switch_A(vlan)#vlan 20 name Marketing
Switch_A(vlan)#vlan 30 name Engineering
Switch_A(vlan)#exit
```

Use the `show vlan` command to verify that the VLANs have been created correctly.

Step 6 Assign ports to a VLAN 10

Assigning ports to VLANs must be done from the interface mode. Enter the following commands to add ports 0/4 to 0/6 to VLAN 10:

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/4
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#interface fastethernet 0/5
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#interface fastethernet 0/6
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#end
```

Step 7 Assign ports to VLAN 20

Enter the following commands to add ports 0/7 to 0/9 to VLAN 20:

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/7
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#interface fastethernet 0/8
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#interface fastethernet 0/9
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#end
```

Step 8 Assign ports to VLAN 30

Enter the following commands to add ports 0/10 to 0/12 to VLAN 30:

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/10
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#interface fastethernet 0/11
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#interface fastethernet 0/12
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#end
```

Step 9 Create VLANs on Switch_B

Repeat Steps 5 through 8 on Switch_B to create its VLANs.

Step 10 Display the VLAN interface information

- a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

- b. Are ports 0/10 through 0/12 assigned to VLAN 30? _____

Step 11 Test the VLANs

Ping from the host in Switch_A port 0/12 to the host in Switch_B port 0/12.

- a. Was the ping successful? _____
b. Why? _____

Ping from the host in Switch_A port 0/12 to the switch IP 192.168.1.2.

- c. Was the ping successful? _____
d. Why? _____

Step 12 Create the ISL trunk

On both switches, Switch_A and Switch_B, type the following command at the fastethernet 0/1 interface command prompt

```
Switch_A(config)#interface fastethernet 0/1  
Switch_A(config-if)#switchport mode trunk  
Switch_A(config-if)#switchport trunk encapsulation isl  
Switch_A(config-if)#end
```

```
Switch_B(config)#interface fastethernet 0/1  
Switch_B(config-if)#switchport mode trunk  
Switch_B(config-if)#switchport trunk encapsulation isl  
Switch_B(config-if)#end
```

Step 13 Verify the ISL trunk

- a. To verify that port fastethernet 0/1 has been established as a trunk port, type `show interface fastethernet 0/1 switchport` at the Privileged EXEC mode prompt.
- b. What type of trunking encapsulation is shown on the output results? _____
- c. According to the output with `show interface fastethernet 0/1 switchport` on Switch_B, is there a difference from the Administrative Trunking Encapsulation from the Operational Trunking Encapsulation?

- d. On the fragment "Trunking VLANs Enable" from the output, what does the word "ALL" mean? _____
- e. What would happen if the two ports of the trunk were using different encapsulation? _____
- f. Explain. _____

Step 14 Test the VLANS and the trunk

Ping from the host in Switch_A port 0/12 to the host in Switch_B port 0/12.

- a. Was the ping successful? _____
- b. Why? _____

Ping from the host in Switch_A port 0/12 to the switch IP 192.168.1.2.

- c. Was the ping successful? _____
- d. Why? _____

Step 15 Move host

Move the host in Switch_A from port 0/12 to port 0/8. Wait until the port LED goes green and then go to the next step.

Step 16 Test the VLANS and the trunk

Ping from the host in Switch_A port 0/8 to the host in Switch_B port 0/12.

- a. Was the ping successful? _____
- b. Why? _____

Ping from the host in Switch_A port 0/8 to the switch IP 192.168.1.2.

- c. Was the ping successful? _____
- d. Why? _____

Step 17 Move host

Move the host in Switch_B from port 0/12 to port 0/7. Wait until the port LED goes green and then go to the next step.

Step 18 Test the VLANS and the trunk

Ping from the host in Switch_A port 0/8 to the host in Switch_B port 0/7.

- a. Was the ping successful? _____
- b. Why? _____

Ping from the host in Switch_A port 0/8 to the switch IP 192.168.1.2.

- c. Was the ping successful? _____
- d. Why? _____

Step 19 Move host

Move the host in Switch_A from port 0/8 to port 0/2. Wait until the port LED goes green and then go to the next step.

Step 20 Test the VLANS and the trunk

Ping from the host in Switch_A port 0/2 to the host in Switch_B port 0/7.

- a. Was the ping successful? _____

Ping from the host in Switch_A port 0/2 to the switch IP 192.168.1.2.

- b. Was the ping successful? _____

c. Why? _____

Step 21 Move host

Move the host in Switch_B from port 0/7 to port 0/3. Wait until the port LED goes green and then go to the next step.

Step 22 Test the VLANs and the trunk

Ping from the host in Switch_A port 0/2 to the host in Switch_B port 0/3.

a. Was the ping successful? _____

b. Why? _____

Ping from the host in Switch_B port 0/3 to the switch IP 192.168.1.2.

c. Was the ping successful? _____

d. Why? _____

Ping from the host in Switch_B port 0/3 to the switch IP 192.168.1.3.

e. Was the ping successful? _____

f. Why? _____

g. What conclusions can be drawn from the testing that was just performed in regards to VLAN membership and VLANs across a trunk?

Once the steps are complete, logoff by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the Privileged EXEC mode by typing `enable`.

```
Switch>enable
```

If prompted for a password, enter `class`, if that does not work, ask the instructor.

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the `show vlan` command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the `reload` command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the `reload` command.

5. Software restart (using the `reload` command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the Privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

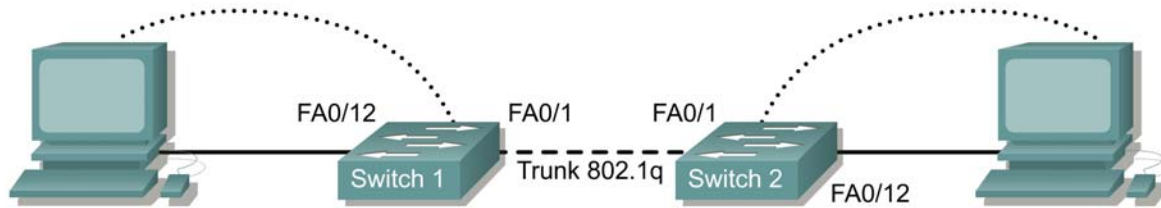
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

Lab 9.1.5b Trunking with 802.1q



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, VLAN 1 IP Address and Console Passwords	Subnet Mask	VLAN Names	Switch Port and Numbers Assignments	
Switch 1	Switch_A	class	cisco	192.168.1.2	255.255.255.0	VLAN 1 Native VLAN 10 Accounting VLAN 20 Marketing VLAN 30 Engineering	fa0/2 - 0/3 fa0/4 - 0/6 fa0/7 - 0/9 fa0/10 - 0/12
Switch 2	Switch_B	class	cisco	192.168.1.3	255.255.255.0	VLAN 1 Native VLAN 10 Accounting VLAN 20 Marketing VLAN 30 Engineering	fa0/2 - 0/3 fa0/4 - 0/6 fa0/7 - 0/9 fa0/10 - 0/12

Straight-through cable ————— Serial cable Console (Rollover) •••••••• Crossover cable - - - - -

Objective

- Create a basic switch configuration and verify it.
- Create multiple VLANs, name them, and assign multiple member ports to them.
- Create an 802.1q trunk line between the two switches to allow communication between paired VLANs.
- Test the VLANs functionality by moving a workstation from one VLAN to another.

Background/Preparation

Trunking changes the formatting of the packets. The ports need to be in agreement as to which format is being used to transmit data on the trunk or no data will be passed. If there is different trunking encapsulation on the two ends of the link they will not be able to communicate. Similar situation will occur if one of the ports is configured in trunking mode (unconditionally) and the other one is in access mode (unconditionally).

When managing a switch, the Management Domain is always VLAN 1. The Network Administrator's workstation must have access to a port in the VLAN 1 Management Domain. All ports are assigned to VLAN 1 by default. This lab will also help demonstrate how VLANs can be used to separate traffic and reduce broadcast domains.

Cable a network similar to one of the diagram. The configuration output used in this lab is produced from 2950 series switch. Any other switch used may produce different output. The following steps are intended to be executed on each switch unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the Hostname, access and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the “Basic Switch Configuration lab”. Do not configure VLANs and trunking yet.

Step 2 Configure the hosts attached to the switch

Configure the IP address, mask, and default gateway on each host. Be sure to choose addresses that are on the same subnet as the switch.

Step 3 Verify connectivity

- a. To verify that the host and switch are correctly configured, ping the switch from the hosts.
- b. Were the pings successful? _____
- c. If the answer is no, troubleshoot the host and switches configurations.

Step 4 Display the VLAN interface information

On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

Note: There should be an entry for VLAN 1 and the default VLANs (1002 +). If other VLANs appear, they could be deleted as instructed in Step 2 of the Erasing and Reloading instructions at the end of this lab or refer to the Lab Exercise: Deleting VLAN Configurations.

Step 5 Create and name three VLANs

Enter the following commands to create and name three VLANs:

```
Switch_A#vlan database
Switch_A(vlan)#vlan 10 name Accounting
Switch_A(vlan)#vlan 20 name Marketing
Switch_A(vlan)#vlan 30 name Engineering
Switch_A(vlan)#exit
```

Use the `show vlan` command to verify that the VLANs have been created correctly.

Step 6 Assign ports to a VLAN 10

Assigning ports to VLANs must be done from the interface mode. Enter the following commands to add ports 0/4 to 0/6 to VLAN 10:

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/4
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
```

```
Switch_A(config-if)#interface fastethernet 0/5
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#interface fastethernet 0/6
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#end
```

Step 7 Assign ports to VLAN 20

Enter the following commands to add ports 0/7 to 0/9 to VLAN 20:

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/7
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#interface fastethernet 0/8
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#interface fastethernet 0/9
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#end
```

Step 8 Assign ports to VLAN 30

Enter the following commands to add ports 0/10 to 0/12 to VLAN 30:

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/10
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#interface fastethernet 0/11
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#interface fastethernet 0/12
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#end
```

Step 9 Create VLANs on Switch_B

Repeat Steps 5 through 9 on Switch_B to create its VLANs

Step 10 Display the VLAN interface information

- a. On both switches, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

- b. Are ports 0/10 through 0/12 assigned to VLAN 30?
-

Step 11 Test the VLANs

Ping from the host in Switch_A port 0/12 to the host in Switch_B port 0/12.

- a. Was the ping successful? _____
- b. Why? _____

Ping from the host in Switch_A port 0/12 to the switch IP 192.168.1.2.

- c. Was the ping successful? _____
- d. Why? _____

Step 12 Create the trunk

On both switches, Switch_A and Switch_B, type the following command at the fastethernet 0/1 interface command prompt. Note that it is not necessary to specify the encapsulation on a 2950, since it only supports 802.1Q.

```
Switch_A(config)#interface fastethernet 0/1
Switch_A(config-if)#switchport mode trunk
Switch_A(config-if)#end
```

```
Switch_B(config)#interface fastethernet 0/1
Switch_B(config-if)#switchport mode trunk
Switch_B(config-if)#end
```

2900:

```
Switch_A(config)#interface fastethernet0/1
Switch_A(config-if)#switchport mode trunk
Switch_A(config-if)#switchport trunk encapsulation dot1q
Switch_A(config-if)#end
```

```
Switch_B(config)#interface fastethernet0/1
Switch_B(config-if)#switchport mode trunk
Switch_B(config-if)#switchport trunk encapsulation dot1q
Switch_B(config-if)#end
```

Step 13 Verify the trunk

- a. To verify that port Fast Ethernet 0/1 has been established as a trunk port, type **show interface fastethernet 0/1 switchport** at the Privileged EXEC mode prompt.
- b. What type of trunking encapsulation is shown on the output results?

- c. According to the output with **show interface fastethernet 0/1 switchport** on Switch_B, is there a difference from the Administrative Trunking Encapsulation from the Operational Trunking Encapsulation?

- d. On the fragment “Trunking VLANs Enable” from the output, what does the word “ALL” mean?

- e. What would happen if the two ports of the trunk were using different encapsulation? _____

- f. Explain _____

Step 14 Test the VLANs and the trunk

Ping from the host in Switch_A port 0/12 to the host in Switch_B port 0/12.

a. Was the ping successful? _____

b. Why? _____

Ping from the host in Switch_A port 0/12 to the switch IP 192.168.1.2.

c. Was the ping successful? _____

d. Why? _____

Step 15 Move host.

Move the host in Switch_A from port 0/12 to port 0/8. Wait until the port LED goes green and then go to the next step.

Step 16 Test the VLANs and the trunk

Ping from the host in Switch_A port 0/8 to the host in Switch_B port 0/12.

a. Was the ping successful? _____

b. Why? _____

Ping from the host in Switch_A port 0/8 to the switch IP 192.168.1.2.

c. Was the ping successful? _____

d. Why? _____

Step 17 Move host

Move the host in Switch_B from port 0/12 to port 0/7. Wait until the port LED goes green and then go to the next step.

Step 18 Test the VLANs and the trunk

Ping from the host in Switch_A port 0/8 to the host in Switch_B port 0/7.

a. Was the ping successful? _____

b. Why? _____

Ping from the host in Switch_A port 0/8 to the switch IP 192.168.1.2.

c. Was the ping successful? _____

d. Why? _____

Step 19 Move hosts

Move the host in Switch_A from port 0/8 to port 0/2. Wait until the port LED goes green and then go to the next step.

Step 20 Test the VLANs and the trunk

Ping from the host in Switch_A port 0/2 to the host in Switch_B port 0/7.

a. Was the ping successful? _____

Ping from the host in Switch_A port 0/2 to the switch IP 192.168.1.2.

- b. Was the ping successful? _____
- c. Why? _____

Step 21 Move host

Move the host in Switch_B from port 0/7 to port 0/3. Wait until the port LED goes green and then go to the next step.

Step 22 Test the VLANs and the trunk

Ping from the host in Switch_A port 0/2 to the host in Switch_B port 0/3.

- a. Was the ping successful? _____
- b. Why? _____

Ping from the host in Switch_B port 0/3 to the switch IP 192.168.1.2.

- c. Was the ping successful? _____
- d. Why? _____

Ping from the host in Switch_B port 0/3 to the switch IP 192.168.1.3.

- e. Was the ping successful? _____
- f. Why? _____
- g. What conclusions can be drawn from the testing that was just performed in regards to VLAN membership and VLANs across a trunk?

Once the steps are complete, logoff by typing **exit**, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the Privileged EXEC mode by typing **enable**.

```
Switch>enable
```

If prompted for a password, enter **class**, if that does not work, ask the instructor.

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the **show vlan** command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the **reload** command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the **reload** command.

5. Software restart (using the **reload** command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the Privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

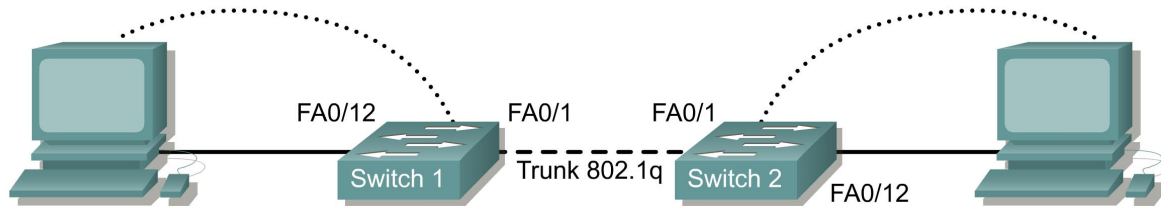
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

Lab 9.2.5 VTP Client and Server Configurations



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, VLAN 1 IP and Console Passwords	VLAN 1 IP Address	Subnet Mask	VLAN Names and Numbers	Switch Port Assignments
Switch 1	Switch_A	class	cisco	192.168.1.2	255.255.255.0	VLAN 1 Native VLAN 10 Accounting VLAN 20 Marketing VLAN 30 Engineering	fa0/2 - 0/3 fa0/4 - 0/6 fa0/7 - 0/9 fa0/10 - 0/12
Switch 2	Switch_B	class	cisco	192.168.1.3	255.255.255.0	VLAN 1 Native VLAN 10 Accounting VLAN 20 Marketing VLAN 30 Engineering	fa0/2 - 0/3 fa0/4 - 0/6 fa0/7 - 0/9 fa0/10 - 0/12

Straight-through cable ————— Serial cable Console (Rollover) •••••••• Crossover cable - - - - -

Objective

- Create a basic switch configuration and verify it.
- Create multiple VLANs, name them and assign multiple member ports to them.
- Configure the VTP protocol to establish Server and client switches.
- Create an 802.1q trunk line between the two switches to allow communication between paired VLANs.
- Then test the VLANs functionality by moving a workstation from one VLAN to another.

Background/Preparation

When managing a switch, the Management Domain is always VLAN 1. The Network Administrator's workstation must have access to a port in the VLAN 1 Management Domain. All ports are assigned to VLAN 1 by default.

Cable a network similar to the one of in diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the hostname, access, and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

Configure the IP address, mask, and default gateway on each host. Be sure to choose addresses that are on the same subnet as the switch.

Step 3 Verify connectivity

- a. To verify that the host and switch are correctly configured, ping the switch from the hosts.
- b. Were the pings successful? _____
- c. If the answer is no, troubleshoot the host and switches configurations.

Step 4 Display the VLAN interface information

On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

Note: There should be an entry for VLAN 1 and the default VLANs (1002 +). If other VLANs appear, they could be deleted as instructed in Step 2 of the Erasing and Reloading instructions at the end of this lab or refer to the Lab Exercise: Deleting VLAN Configurations.

Step 5 Configure VTP

- a. VLAN Trunking Protocol (VTP) needs to be configured on both switches. VTP is the protocol that will communicate information about which VLANs exist from one switch to another. If VTP did not provide this information, VLANs would have to be created on all switches individually.
- b. By default, the Catalyst switch series are configured as VTP servers. In the event that the server services are turned off, use the following command to turn it back on:

```
Switch_A#vlan database
Switch_A(vlan)#vtp server
Switch_A(vlan)#vtp domain group1
Switch_A(vlan)#exit
```

Step 6 Create and name three VLANs

Enter the following commands to create and name three VLANs:

```
Switch_A#vlan database
Switch_A(vlan)#vlan 10 name Accounting
Switch_A(vlan)#vlan 20 name Marketing
Switch_A(vlan)#vlan 30 name Engineering
Switch_A(vlan)#exit
```

Use the `show vlan` command to verify that the VLANs have been created correctly.

Step 7 Assign ports to VLAN 10

Assigning ports to VLANs must be done from the interface mode. Enter the following commands to add ports 0/4 to 0/6 to VLAN 10:

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/4
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#interface fastethernet 0/5
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#interface fastethernet 0/6
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#end
```

Step 8 Assign ports to VLAN 20

Enter the following commands to add ports 0/7 to 0/9 to VLAN 20:

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/7
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#interface fastethernet 0/8
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#interface fastethernet 0/9
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#end
```

Step 9 Assign ports to VLAN 30

Enter the following commands to add ports 0/10 to 0/12 to VLAN 30:

```
Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/10
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#interface fastethernet 0/11
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#interface fastethernet 0/12
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 30
Switch_A(config-if)#end
```

Step 10 Display the VLAN interface information

a. On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

- b. Are ports 0/10 through 0/12 assigned to VLAN 30?
-

Step 11 Configure VTP client

Enter the following commands to configure Switch_B to be a VTP client:

```
Switch_B#vlan database
Switch_B(vlan)#vtp client
Switch_B(vlan)#vtp domain group1
Switch_B(vlan)#exit
```

Step 12 Create the trunk

On both switches, Switch_A and Switch_B, type the following command at the fastethernet 0/1 interface command prompt. Note that it is not necessary to specify the encapsulation on a 2950, since it only supports 802.1Q.

```
Switch_A(config)#interface fastethernet 0/1
Switch_A(config-if)#switchport mode trunk
Switch_A(config-if)#end
```

```
Switch_B(config)#interface fastethernet 0/1
Switch_B(config-if)#switchport mode trunk
Switch_B(config-if)#end
```

2900:

```
Switch_A(config)#interface fastethernet0/1
Switch_A(config-if)#switchport mode trunk
Switch_A(config-if)#switchport trunk encapsulation dot1q
Switch_A(config-if)#end
```

```
Switch_B(config)#interface fastethernet0/1
Switch_B(config-if)#switchport mode trunk
Switch_B(config-if)#switchport trunk encapsulation dot1q
Switch_B(config-if)#end
```

Step 13 Verify the trunk

- To verify that port fastethernet 0/1 has been established as a trunk port, type `show interface fastethernet 0/1 switchport` at the Privileged EXEC mode prompt
- What type of trunking encapsulation is shown on the output results? _____

Step 14 Display the VLAN interface information

- On Switch_B, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_B#show vlan
```

- Do VLANs 10, 20, and 30 show without having to type them in? _____
- Why did this happen? _____

Step 15 Assign ports to a VLAN 10

Although the VLAN definitions have migrated to Switch_B using VTP, it is still necessary to assign ports to these VLANs on Switch_B. Assigning ports to VLANs must be done from the interface mode. Enter the following commands to add ports 0/4 to 0/6 to VLAN 10.

```
Switch_B#configure terminal
Switch_B(config)#interface fastethernet 0/4
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 10
Switch_B(config-if)#interface fastethernet 0/5
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 10
Switch_B(config-if)#interface fastethernet 0/6
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 10
Switch_B(config-if)#end
```

Step 16 Assign ports to VLAN 20

Enter the following commands to add ports 0/7 to 0/9 to VLAN 20:

```
Switch_B#configure terminal
Switch_B(config)#interface fastethernet 0/7
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 20
Switch_B(config-if)#interface fastethernet 0/8
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 20
Switch_B(config-if)#interface fastethernet 0/9
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 20
Switch_B(config-if)#end
```

Step 17 Assign ports to VLAN 30

Enter the following commands to add ports 0/10 to 0/12 to VLAN 30:

```
Switch_B#configure terminal
Switch_B(config)#interface fastethernet 0/10
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 30
Switch_B(config-if)#interface fastethernet 0/11
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 30
Switch_B(config-if)#interface fastethernet 0/12
Switch_B(config-if)#switchport mode access
Switch_B(config-if)#switchport access vlan 30
Switch_B(config-if)#end
```

Step 18 Display the VLAN interface information

- a. On Switch_B, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_B#show vlan
```

b. Are ports 0/10 through 0/12 assigned to VLAN 30? _____

Step 19 Test the VLANs and the trunk

Ping from the host in Switch_A port 0/12 to the host in Switch_B port 0/12.

a. Was the ping successful? _____

b. Why? _____

Ping from the host in Switch_A port 0/12 to the switch IP 192.168.1.2.

c. Was the ping successful? _____

d. Why? _____

Step 20 Move hosts

Move the host in Switch_A from port 0/12 to port 0/8. Wait until the port LED goes green and then go to the next step.

Step 21 Test the VLANs and the trunk

Ping from the host in Switch_A port 0/8 to the host in Switch_B port 0/12.

a. Was the ping successful? _____

b. Why? _____

Ping from the host in Switch_A port 0/8 to the switch IP 192.168.1.2.

c. Was the ping successful? _____

d. Why? _____

Once the steps are complete, logoff by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the Privileged EXEC mode by typing `enable`.

```
Switch>enable
```

If prompted for a password, enter `class`, if that does not work, ask the instructor.

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]? [Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the `show vlan` command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the `reload` command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the `reload` command.

5. Software restart (using the `reload` command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the Privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

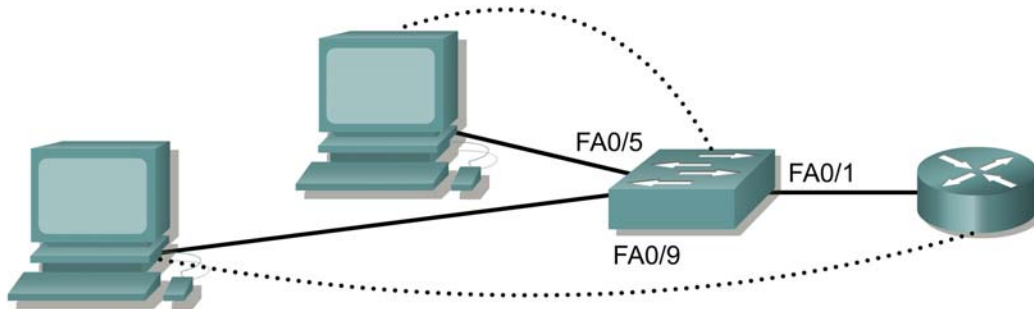
```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

Lab 9.3.6 Configuring Inter-VLAN Routing



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords	VLAN 1 IP Address	Subnet Mask	VLAN Names and Numbers	Switch Port Assignments
Switch 1	Switch_A	class	cisco	192.168.1.2	255.255.255.0	VLAN 1 Native VLAN 10 Sales VLAN 20 Support	fa0/1 - 0/4 fa0/5 - 0/8 fa0/9 - 0/12



Objective

- Create a basic switch configuration and verify it.
- Create multiple VLANs, name them and assign multiple member ports to them.
- Create a basic configuration on a router.
- Create an 802.1q trunk line between the switch and router to allow communication between VLANs.
- Test the routing functionality.

Background/Preparation

When managing a switch, the Management Domain is always VLAN 1. The Network Administrator's workstation must have access to a port in the VLAN 1 Management Domain. All ports are assigned to VLAN 1 by default. This lab will also help demonstrate how VLANs can be used to separate traffic and reduce broadcast domains.

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are to be executed on each switch unless specifically instructed otherwise. Instructions are also provided for the 2900 and 1900 Series switches. The 1900 Series switch initially displays a User Interface Menu. Select the "Command Line" option from the menu to perform the steps for this lab.

Note: The router used must have a Fast Ethernet interface in order to support trunking and inter-VLAN routing. The 2500 series router cannot be used for this lab.

Start a HyperTerminal session.

Note: Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the hostname, access, and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

Configure the hosts using the following information.

- a. For the host in port 0/5:
IP address 192.168.5.2
Subnet mask 255.255.255.0
Default gateway 192.168.5.1
- b. For the host in port 0/9:
IP address 192.168.7.2
Subnet mask 255.255.255.0
Default gateway 192.168.7.1

Step 3 Verify connectivity

Check to see if the hosts can ping the switch.

- a. Ping the switch IP address from the hosts.
- b. Were the pings successful? _____
- c. Why or why not? _____

Step 4 Create and name two VLANs

Enter the following commands to create and name two VLANs:

```
Switch_A#vlan database
Switch_A(vlan)#vlan 10 name Sales
Switch_A(vlan)#vlan 20 name Support
Switch_A(vlan)#exit

1900:

Switch_A#config terminal
Switch_A(config)#vlan 10 name Sales
Switch_A(config)#vlan 20 name Support
Switch_A(config)#exit
```

Step 5 Assign ports to VLAN 10

Assigning ports to VLANs must be done from the interface mode. Enter the following commands to add ports 0/5 to 0/8 to VLAN 10:

```

Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/5
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#interface fastethernet 0/6
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#interface fastethernet 0/7
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#interface fastethernet 0/8
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 10
Switch_A(config-if)#end

```

1900:

```

Switch_A#config terminal
Switch_A(config)#interface ethernet 0/5
Switch_A(config-if)vlan static 10
Switch_A(config-if)#interface ethernet 0/6
Switch_A(config-if)vlan static 10
Switch_A(config-if)#interface ethernet 0/7
Switch_A(config-if)vlan static 10
Switch_A(config-if)#interface ethernet 0/8
Switch_A(config-if)vlan static 10
Switch_A(config-if)#end

```

Step 6 Assign ports to VLAN 20

Enter the following commands to add ports 0/9 to 0/12 to VLAN 20:

```

Switch_A#configure terminal
Switch_A(config)#interface fastethernet 0/9
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#interface fastethernet 0/10
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#interface fastethernet 0/11
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#interface fastethernet0/12
Switch_A(config-if)#switchport mode access
Switch_A(config-if)#switchport access vlan 20
Switch_A(config-if)#end

```

1900:

```

Switch_A#config terminal
Switch_A(config)#interface ethernet 0/9
Switch_A(config-if)vlan static 20
Switch_A(config-if)#interface ethernet 0/10
Switch_A(config-if)vlan static 20
Switch_A(config-if)#interface ethernet 0/11
Switch_A(config-if)vlan static 20
Switch_A(config-if)#interface ethernet 0/12

```

```
Switch_A(config-if)vlan static 20
Switch_A(config-if)#end
```

Step 7 Display the VLAN interface information

- On Switch_A, type the command `show vlan` at the Privileged EXEC prompt as follows:

```
Switch_A#show vlan
```

- Are ports assigned correctly? _____

Step 8 Create the trunk

On Switch_A, type the following commands at the Fast Ethernet 0/1 interface command prompt. Note that Ethernet 0/1 and the other access ports on a 1900 switch only support 10 Mbps Ethernet and cannot be used as trunk ports. The trunk ports (if present) on a 24-port 1900 are typically Fast Ethernet 0/26 and 0/27.

```
Switch_A(config)#interface fastethernet0/1
Switch_A(config-if)#switchport mode trunk
Switch_A(config-if)#end
```

2900:

```
Switch_A(config)#interface fastethernet0/1
Switch_A(config-if)#switchport mode trunk
Switch_A(config-if)#switchport trunk encapsulation dot1q
Switch_A(config-if)#end
```

1900:

```
Switch_A#config terminal
Switch_A(config)#interface fastethernet0/26
Switch_A(config-if)#trunk on
```

Step 9 Configure the router

- Configure the router with the following data. Note that in order to support trunking and inter-VLAN routing, the router must have a Fast Ethernet interface.

Hostname is **Router_A**

Console, VTY, and enable passwords are **cisco**.

Enable secret password is **class**.

- Then configure the Fast Ethernet interface using the following commands:

Note: If working with a 1900 switch, replace the “dot1q” encapsulation with “isl” in the following router configuration commands.

```
Router_A(config)#interface fastethernet 0/0
Router_A(config-if)#no shutdown
Router_A(config-if)#interface fastethernet 0/0.1
Router_A(config-subif)#encapsulation dot1q 1
Router_A(config-subif)#ip address 192.168.1.1 255.255.255.0
Router_A(config-if)#interface fastethernet 0/0.2
Router_A(config-subif)#encapsulation dot1q 10
Router_A(config-subif)#ip address 192.168.5.1 255.255.255.0
Router_A(config-if)#interface fastethernet 0/0.3
Router_A(config-subif)#encapsulation dot1q 20
```

```
Router_A(config-subif)#ip address 192.168.7.1 255.255.255.0
Router_A(config-subif)#end
```

Step 10 Save the router configuration

Step 11 Display the router routing table

- Type `show ip route` at the Privileged EXEC mode prompt.
- Are there entries in the routing table? _____
- What interface are they all pointing to? _____
- Why is there not a need to run a routing protocol? _____

Step 12 Test the VLANS and the trunk

Ping from the host in Switch_A port 0/9 to the host in port 0/5.

- Was the ping successful? _____
- Why? _____

Ping from the host in Switch_A port 0/5 to the switch IP 192.168.1.2.

- Was the ping successful? _____

Step 13 Move the hosts

- Move the hosts to other VLANs and try pinging the management VLAN 1.
- Note the results of the pinging.

Once the steps are complete, logoff by typing `exit`, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the Privileged EXEC mode by typing **enable**.

```
Switch>enable
```

If prompted for a password, enter **class**, if that does not work, ask the instructor.

2. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat  
Delete filename [vlan.dat]?[Enter]  
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed.

```
%Error deleting flash:vlan.dat (No such file or directory)
```

3. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt will be:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

4. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step 2 using the **show vlan** command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the **reload** command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the **reload** command.

5. Software restart (using the **reload** command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

- a. At the Privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

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

- b. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

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

- c. Type `n` and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
```

This command resets the switch with VTP parameters set to factory defaults.

All other parameters will be unchanged.

```
Reset system with VTP parameters set to factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

```
Reset system with factory defaults, [Y]es or [N]o?
```

Enter `y` and press **Enter**.