Building CISCO Multilayer Switched Networks TB

Lab Guide

 Revision May 2002

Table of Contents

Enhanced Cisco Labs

LAB #1

Plug and Play - Create a Switch Block and establish IP connectivity

Objective:

In this lab, you will familiarize yourself with the classroom network, physically connect these devices and establish IP connectivity throughout the classroom network. To accomplish this goal you need to perform the following tasks:

1. Identify the switch block you will be configuring, identify all components in your switch block and identify the Core switch.
2. Physically connect the Access Switches (ASW) and Distribution Switches (DSW) in your switch block using the correct ethernet cables.
3. Connect your Switch Block to the Core Switch via fast ethernet.
4. Create an ethernet connection between your PC and your Access Switch.
5. Familiarize yourself with the IP address plan used in the network. Configure the appropriate IP addresses.
6. Make a connection between the console ports of your Distribution Switch and Access Switch and the serial port of your PC.
7. Clear any existing configurations on your Access Switch (ASW) and Distribution Switch (DSW).
8. Provide a base configuration to both your Access Switch (ASW) and the Supervisor card on Distribution Switch (DSW).
9. TFTP an IP alias table to your DSW and an IP host table to your ASW.
10. Test IP connectivity throughout the network.

Estimated Time: 60 minutes

Definitions:

Switch Block	A Switch Block (SB) is comprised of two 3500XL series switches for access switches and two more 3500XL series switches as distribution switches. An Access Switch is where users (which includes your PC) connect to the network.
Core Switch	There is 1 3500XL switch that comprises the core of the network. This Core Switch connects the Switch Blocks together.
Student Pair	A student pair is comprised of two students sharing one PC, one 3500XL Access Switch (ASW) and one 3500XL Distribution Switch (DSW).
Student Group	A Student Group is comprised of two student pairs. A Student Group (up to 4 students) is responsible for one Switch Block of equipment.

Task 1: **Identify the components in your Switch Block (SB) and physically connect the devices with the proper ethernet cables. All switches should be powered on at this time.**

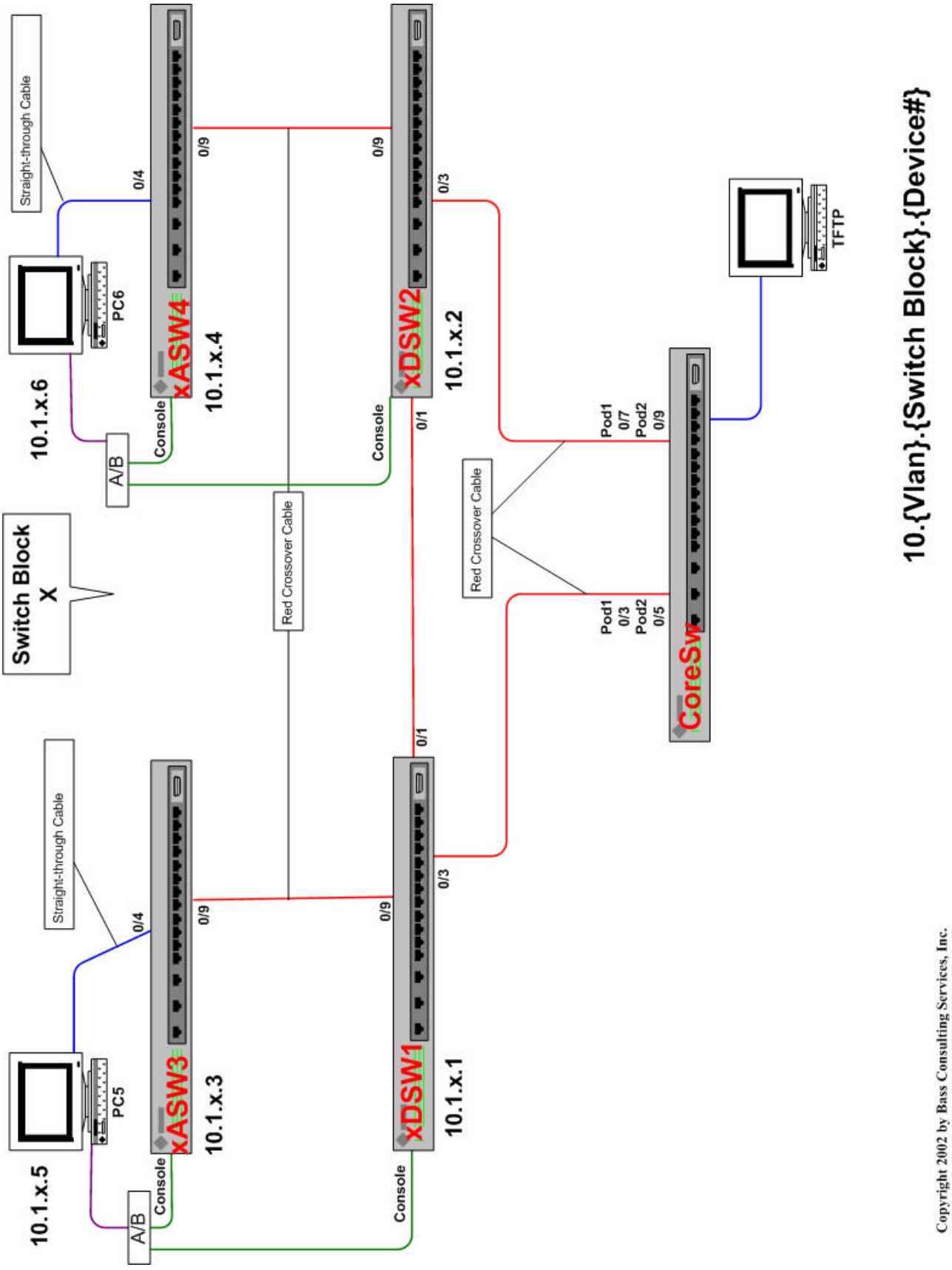
Step 1. Each student group should use the network diagram in Figure 1 to identify the components in each Switch Block and the Core Switch. Each student pair should identify the specific PC, 3500XL Access Switch (ASW) and 3500XL Distribution Switch (DSW) they have been assigned. Notice that you have either the odd switches (ASW1 and DSW3) or the even switches (ASW2 and DSW4).

Step 2: Physically connect the Access Switches (ASW) and Distribution Switches (DSW) in your switch block using the correct ethernet cables. Then connect your PC to your ASW using one straight Ethernet cable.

Finally, connect each Switch Block to the Core Switch. Please note that each DSW to either an odd or even VLAN on the core. This will be used as primary Core connection. Later, we will make a second connection to the core as a secondary path on the opposite VLAN. Use **Figure 1** as your guide.

Step 3: Plug a 9 pin to RJ45 connector into the serial (com) port of your pc. Take a roll over cable and connect from the 9 pin connector to the input port on your A/B switch. Take a straight through cable and connect from the A port of the A/B switch directly to the console port of your ASW. Take another straight through cable and connect from the B port of the A/B switch to the DSW console port.

You will be using the A/B switch to make it easy to switch between the console port of your ASW and your DSW (and later the router). Once you have made the connections, open up a HyperTerminal session on your PC.



Step 4: It is important that you take the time to visualize what you have just constructed.

If you were to send data from PC5 to PC6, or any intra-Switch Block communication for that matter, will you have to go through a Core Switch?

Yes _____ or No _____

If you were to send data from a PC in your Switch Block (SB) to a PC in another SB, or any inter-Switch Block communication for that matter, will you always have to go through the Core Switch?

Yes _____ or No _____

Task 2: Understand the network IP addressing plan and naming conventions. Then provide your PC with an IP address.

Step 5: Familiarize yourself with the IP address plan used in the network. The numbering convention is **10.{vlan#}.{Switch Block}. {Device#}**. Notice that the first character of each device name is the Switch Block number. Also notice that the third byte of each IP address is also the Switch Block number. The ASW/DSW are configured in the next lab. Please review the table below:

Student Group	Switch Block	Primary Distribution Switch Name	Primary Distribution Switch IP Address	Access Switch Name	Access Switch IP Address	PC Name	PC IP Address
1 odd	**1**	**1**DSW1	10.x.**1**.1	**1**ASW3	10.x.**1**.3	**1**PC5	10.x.**1**.5
1 even	**1**	**1**DSW2	10.x.**1**.2	**1**ASW4	10.x.**1**.4	**1**PC6	10.x.**1**.6
2 odd	**2**	**2**DSW1	10.x.**2**.1	**2**ASW3	10.x.**2**.3	**2**PC5	10.x.**2**.5
2 even	**2**	**2**DSW2	10.x.**2**.2	**2**ASW4	10.x.**2**.4	**2**PC6	10.x.**2**.6
	TFTP	**server**	10.1.7.5	Connected	to	CoreSw	

The second byte of each IP address is the VLAN#. In the first few labs, all devices will be in Vlan 1. The mask that we will use is **255.255.0.0**

If all devices are in Vlan 1 and we had a Switch Block 5, what would the odd numbered PCs IP address be?

_____

Step 6: **Configure your PC**. Turn on your PC and configure the appropriate IP address on your PC. Remember that our addressing convention is **10.{vlan#}.{Switch Block}.{Device#}.** In this lab, all devices will be in Vlan 1 and our mask is **255.255.0.0**. If in doubt, review the last chart. All devices are on the same subnet, so **a default gateway is not needed at this time**. After providing the IP address and mask, reboot your PC. Once it has booted, open up an MSDOS prompt from your desktop. Type the command "**doskey**" This will enable you to use your UpArrow to recall previous commands. Verify your work by pinging your PC's address.

Task 3: Provide a base configuration in your Access Switch and verify IP connectivity.

Step 7: First we are going to wipe out any leftover configuration file, then you will configure this switch. The 3500 is IOS based and commands are very similar to router IOS commands. Get to privileged mode

Switch>**enable**
Switch#

Erase the startup configuration file stored in NVRAM

Switch#**erase start**
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete

Step 8: Check to see if there is any vlan information left over from the prior weeks' class. If there is any leftover vlan configuration it will be in a file called "vlan.dat" in flash. Check to see if this file exists with the following command:

Switch#**show flash**

If the vlan.dat file exists, do the next command. If the vlan.dat file does not exist, skip the next command entirely and go to Step 9.

READ THE NEXT COMMAND IN ITS ENTIRETY BEFORE ENTERING THE COMMAND

Switch#**erase flash:vlan.dat**

If the vlan.dat file exists, this command is necessary to remove any vlans that were created the week before and return your ASW to factory defaults. If you do this command, be absolutely certain to include "vlan.dat" at the end. Do **NOT** enter the command "erase flash:" because this will erase everything from flash, including your entire operating system. If you then did a reload, your switch would not have its operating system.

Step 9: What command can you issue from your console to cause a router to reboot? (Hint: it is NOT reset)

_____

Switch#**reload**
System configuration has been modified. Save? [yes/no]: **no** (be certain to answer "no")
Proceed with reload? [confirm]

Watch the switch boot. Once it boots you will be at the following prompt:
Switch>**enable**
Switch#

Step 10: Now that you have wiped out any "left over" switch configuration, it's time to provide a base configuration to your ASW. Once you get back to privileged mode you will first examine the switch and then configure an IP address and other basic information on the switch. On a 3500 the default management interface is the vlan 1 interface.

Switch# **show run**

Examine the default configuration file. Identify the hostname, the list of physical interfaces and the Vlan 1 interface.

Step 11: Examine the interface you have connected your PC to:
Switch# **show int fa0/4**

What is the status of the interface? _____

What is the bandwidth of the interface? _____

What is the MAC address of the interface? _____

What is the default ethernet frame (encapsulation) type _____

Switch#**show int vlan1**
What is the status of the interface? _____

Step 12: Configure basic management information on your switch:

Provide the proper IP address. (Use the Table for IP addresses and Device names).

Switch#**conf t**
Switch(config)#**int vlan1**

Switch(config-if)# **ip address 10.1.x.y 255.255.0.0** (use the IP address for your ASW)
Switch(config-if)#**exit**

Configure the switch name
Switch(config)#**hostname 5ASW4** (use your own ASW switch name here)

Configure a line console password
xASWy(config)#**line con 0**
xASWy(config-line)#**login**
xASWy(config-line)#**password cisco**
xASWy(config-line)#**exec-timeout 0 0** (this will keep your console session from timing out this week. This is not a command you would use where security is a concern)

Configure a line virtual terminal password
xASWy(config-line)#**line vty 0 4**
xASWy(config-line)#**login**
xASWy(config-line)#**password cisco**
Configure an enable secret password to get from user exec to privileged mode
xASWy(config-line)#**exit**
xASWy(config **)enable secret san-fran**

Provide a banner to anyone connecting to your switch
xASWy (config)#**banner motd #**

{enter your banner here}
#
Set speed and duplex for ports f0/9, f0/10, f0/11 & f0/12 and a description for f0/9**. It is critical to set speed and duplex because you will be using all four of these ports to connect to the DSWs and auto negotiate DOES NOT always work properly**.

xASWy(config)#**int f0/4**
xASWy(config-if)#**description Connection_xPC5**
xASWy(config-if)#**int f0/09**
xASWy(config-if)#**speed 100**
xASWy(config-if)#**duplex full**
xASWy(config-if)#**description Connection_xDSWy**
repeat the speed and duplex commands for ports f0/10,f0/11 and f0/12
xASWy(config-if)#**end**

Examine your running-configuration file and identify the changes you made.
xASWy# **show run**

Examine your startup-configuration file and identify the changes you made
xASWy# **show start**

Is there a difference between the configuration that is running on your switch and the configuration in NVRAM? _____
Why? _____

Save your running configuration to NVRAM
xASWy#**copy run start**

Step 13: Test connectivity to your PC by pinging it

Step 14: Examine the dynamically learned CAM (Content Addressable Memory) table
xASWy#**show mac-address-table**

Examine the arp cache on the ASW
xASWy#**show arp**

Task 4: Provide a base configuration in your Distribution Switch and verify IP connectivity.

Step 15: **Create a console connection to your Distribution Switch**. Your Distribution Switch (DSW. Turn your A/B switch to "B" and power on your DSW.

Step 16: First we are going to wipe out any leftover configuration file, then you will configure this switch. The 3500 is IOS based and commands are very similar to router IOS commands. Get to privileged mode

Switch>**enable**
Switch#

Erase the startup configuration file stored in NVRAM

Switch#**erase start**
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete

Step 17: Check to see if there is any vlan information left over from the prior weeks' class. If there is any leftover vlan configuration it will be in a file called "vlan.dat" in flash. Check to see if this file exists with the following command:

Switch#**show flash**

If the vlan.dat file exists, do the next command. If the vlan.dat file does not exist, skip the next command entirely and go to Step 18.

READ THE NEXT COMMAND IN ITS ENTIRETY BEFORE ENTERING THE COMMAND

Switch#**erase flash:vlan.dat**

If the vlan.dat file exists, this command is necessary to remove any vlans that were created the week before and return your ASW to factory defaults. If you do this command, be absolutely certain to include "vlan.dat" at the end. Do **NOT** enter the command "erase flash:" because this will erase everything from flash, including your entire operating system. If you then did a reload, your switch would not have its operating system.

Step 18: Switch#**reload**
System configuration has been modified. Save? [yes/no]: **no** (be certain to answer "no")
Proceed with reload? [confirm]

Watch the switch boot. Once it boots you will be at the following prompt:
Switch>**enable**
Switch#

Step 19: Configure basic management information on your switch:

Provide the proper IP address. (Use the Table for IP addresses and Device names).

Switch#**conf t**
Switch(config)#**int vlan1**
Switch(config-if)# **ip address 10.1.x.y 255.255.0.0** (use the IP address for your DSW)
Switch(config-if)#**exit**
Configure the switch name
Switch(config)#**hostname 5DSW1** (use your own DSW switch name here)

Configure a line console password
xDSWy(config)#**line con 0**
xDSWy(config-line)#**login**
xDSWy(config-line)#**password cisco**
xDSWy(config-line)#**exec-timeout 0 0** (this will keep your console session from timing out this week. This is not a command you would use where security is a concern)

Configure a line virtual terminal password
xDSWy(config-line)#**line vty 0 4**
xDSWy(config-line)#**login**
xDSWy(config-line)#**password cisco**

Configure an enable secret password to get from user exec to privileged mode
xDSWy(config-line)#**exit**
xDSWy(config **)enable secret san-fran**
xDSWy(config)#**end**

Provide a banner to anyone connecting to your switch
xDSWy (config)#**banner motd #**

{enter your banner here}
#
Set speed and duplex for ports f0/1through f0/5, f0/9 through f0/12**. It is critical to set speed and duplex because you will be using all of these ports to connect to different devices and auto negotiate DOES NOT always work properly**.

xDSWy#**conf t**
Enter configuration commands, one per line. End with CNTL/Z.
xDSWy(config-if)#**int f0/01**
xDSWy(config-if)#**speed 100**
xDSWy(config-if)#**duplex full**
repeat the speed and duplex commands for ports f0/2,f0/3, f0/4, f0/5, f0/9, f0/10, f0/11 and f0/12
xDSWy(config-if)#**end**
Examine your running-configuration file and identify the changes you made.
xDSWy# **show run**

Save your running configuration to NVRAM
xDSWy#**copy run start**

Step 20. Test IP connectivity.
See if you can ping the TFTP server with the following command:
xDSWy#**ping server**

Why weren't you successful? _____

Step 21: Add an IP alias
xDSWy(config)# **ip host server 10.1.7.5**
xDSWy(config)#**end**
xDSWy#**ping server**

Step 22: Retrieve a full ip alias table from the tftp server
xDSWy#**copy tftp run**
Address or name of remote host []? **server**
Source filename []? **host.txt**
Destination filename [running-config]? **<cr>**
Accessing tftp://10.1.7.5/host.txt...
xDSWy#**copy run start**

Lab #2

Create VLANs

Objective:

In this lab, you will create multiple VLANs and assign them to various switch ports. You will then explore the advantages and consequences of creating multiple VLANs in your network. To accomplish this objective you need to perform the following tasks:

1. Create multiple VLANs
2. Assign switch ports to the new VLANs
3. Explore VLAN operation
4. Test IP connectivity in your network

Estimated Time: 1:15 minutes

Task 1: **Create four new VLANs on your ASW (Access Switch) and assign them to ports**

Step1: Display the default VLANs

xASWy# **show vlan**

How many default VLANs are there? _____

Step 2: Verify connectivity with your DSW

xASWy# **show cdp neighbors**

Look at the output of this command. Which interface on your ASW is connected to your DSW? _____

Does this command provide the IP address of the DSW? _____

Try the following command:

xASWy# **show cdp neighbor detail**

Step 3: Check which VLAN the interface connected to the DSW is in.

xASWy# **show vlan brief**

Step 4: Verify IP connectivity with the DSW by pinging it

Was your ping successful? _____

Step 5: Before we create any new VLANs, you should verify the default VTP (VLAN Trunk Protocol) parameters. These will be used in the next lab.

xASWy# **show vtp status**

Is your ASW capable of running VTP version 2? _____
What is the current Configuration Revision Number? _____
How many VLANs currently exist on your ASW? _____

Step 6: Create a vtp domain

First you will have to go to the VLAN database on your 2900 ASW

xASWy# **vlan database**

Notice the change in your prompt, then type in a "**?**" to view the possible commands
xASWy(vlan)# **?**

Create vtp domain BCMSN with the following command:

xASWy(vlan)#**vtp domain BCMSN** (remember to capitalize)

Step 7: Create VLANs 2,3 and 4 and explore related commands

Which command allows you to create a vlan? _____

Display the current VLANs in the database
xASWy(vlan)# **show current**

List the vlans in the database _____

Create VLANs 2,3 and 4 and name them

xASWy(vlan)# **vlan 2 name 2nd_Floor**
VLAN 2 added:
Name: vlan2
xASWy(vlan)# **vlan 3 name 3rd_Floor**
VLAN 3 added:
Name: vlan3
xASWy(vlan)# **vlan 4 name 4th_Floor**
VLAN 4 added:
Name: vlan4

Display the current VLANs in the database

xASWy(vlan)# **show current**

Are the VLANs you just created in the database? _____
Don't panic – keep going

Display the changes you propose to make in the database

xASWy(vlan)# **show changes**

At this point what is the difference between issuing the following commands:

Abort _____
Apply _____
Exit _____

If in doubt try the following command:
xASWy(vlan)#**?**

Exit the VLAN database

xASWy(vlan)# **exit**
APPLY completed.
Exiting....

What VTP configuration revision number do you expect? _____

Execute the following command:
xASWy# **show vtp status**

What is the actual VTP configuration revision number? _____

Step 7: Using the commands previously provided, **create VLAN 5**, exit the database, and view the configuration revision number again. What number did it change to? _____

Step 8: View your new VLANs

xASWy# **show vlan**

What ports are VLANs 2,3,4 & 5 assigned to? _____

Step 9: Assign the interfaces of your ASW to the vlans specified in the following table:

VLAN Assignment	**Interface(s)**
vlan 2	f0/1, f0/2 & f0/3
vlan 3	f0/4, f0/5 & f0/6
vlan 4	F0/7, f0/8 &f0/9
vlan 5	f0/10, f0/11 & f0/12

To accomplish this you will have to do the following for each interface:
Enter global configuration mode.
xASWy#**configure terminal**

Enter interface configuration mode, and define the interface to be added to the VLAN.
xASWy(config)#**interface** *(f0/1 or f0/2, etc)*

Define the VLAN membership mode for this port as access and assign the static vlan. (The other membership modes are trunk or multi).

xASWy(config-if)#**switchport access vlan 2** repeat these steps for each interface (The vlan number will vary depending upon which interface you are configuring)

Return to privileged EXEC mode.
end

Save your configurations changes to NVRAM
copy run start

Step 10: Verify the VLAN configuration.
show vlan or **show vlan brief**
show interface *f0/?* **switchport**

Step 11: **STOP!! Check to see your Switch Block partner has reached this step. If not, wait for them to catch up before you continue.**

Task2: Explore VLAN rules and verify IP Connectivity

You and your partner need to physically move the gray cable connecting your PC to your ASW to interface f0/4, if your pc's are not already connected there.

What is the ip address of your pc? _____
What is the ip address of your ASW? _____
What is the ip address of your partner's pc? _____
What is the ip address of your partner's ASW? _____

From this point on, before you ping predict to the other members of your Switch Block whether or not the ping should be successful and discuss your reasoning.

Step 12: To be certain you understand how your VLAN configuration affects IP connectivity make the following predictions:
(Please circle your prediction BEFORE you actually ping. Do not fix any problem. The purpose of the exercise is to accurately predict what will happen).

Prediction: A ping from your PC to your own ASW will be successful. True/False

Result: successful/unsuccessful

Explain this result: _____
_____
_____
_____

(If you are having trouble making a prediction, go to Step 16, then come back)

Step 13: Prediction: A ping from your PC to your partner's PC will be successful True/False

Result: successful/unsuccessful

Explain this result: _____

Step 14: Prediction: A ping from your ASW to your partner's ASW will be successful. True/False

Result: successful/unsuccessful

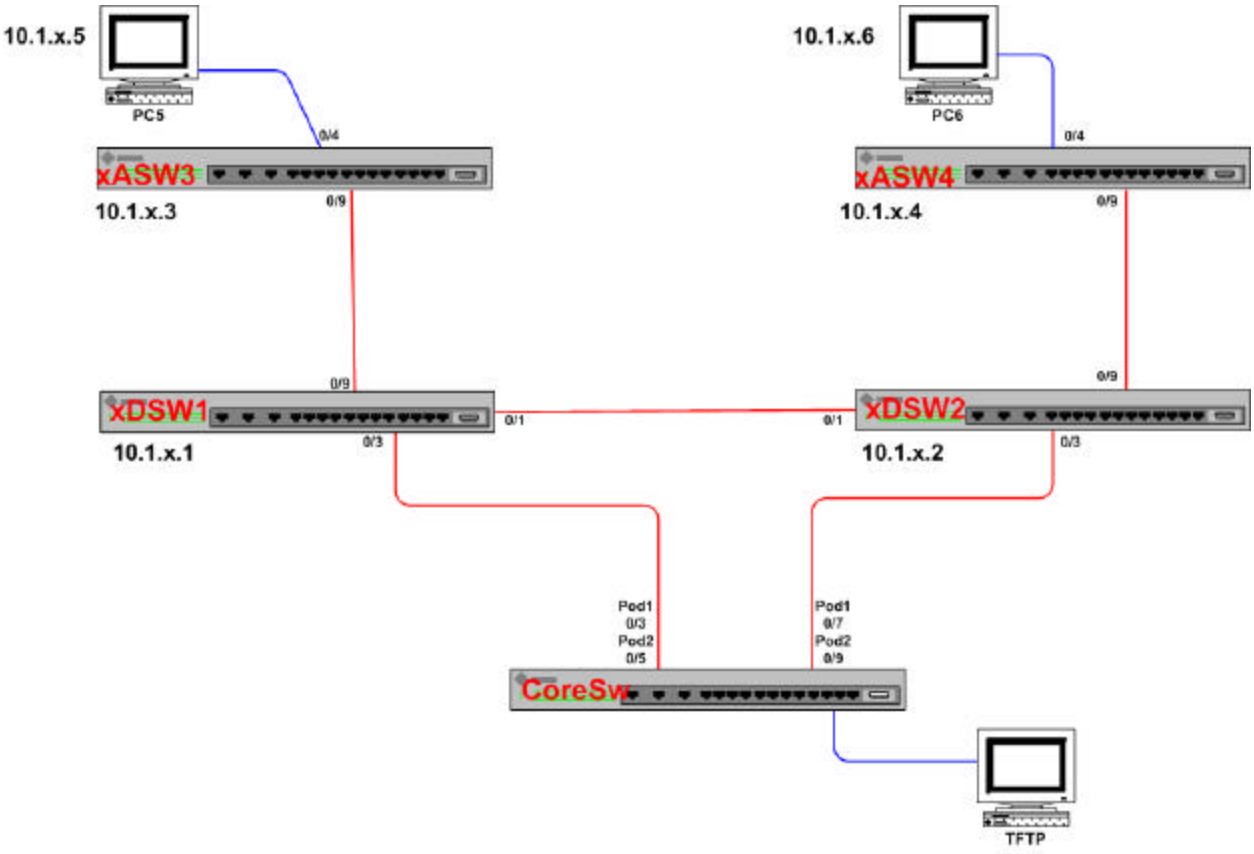
Explain this result: _____

Step 15: Prediction: A ping from your ASW to your DSW will be successful. True/False

Result: successful/unsuccessful

Explain this result: _____

Step 16: On the following diagram, label each port with the VLAN it currently belongs to. Include the ports on each DSW and the VLANs for the management interface of each switch.



Step 17: Close down the applications, which are currently open on your PC, then reconfigure your PC to have an address on VLAN 3 with a 255.255.0.0 mask.

Remember, our IP addressing convention is **10.{vlan#}.{Switch Block}. {Device#}**

Your new PC address will begin with 10.3., but the last two bytes will remain the same. After changing the address remember to restart your PC.

Step 18: Create a new VLAN 3 interface on your ASW, configure it with a valid ip address, make it the management VLAN and test ip connectivity.

```
xASWy#
xASWy# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
xASWy(config)# int vlan3
xASWy(config-subif)# ip address 10.3.x.y 255.255.0.0        (use your own ip address
                                                              10.3.{SB#}.{Device#3or4})
xASWy(config-subif)# management
xASWy(config-subif)# end
xASWy#
03:41:42: %SYS-5-CONFIG_I: Configured from console by console
xASWy# copy run start
Destination filename [startup-config]?
Building configuration...
```

Examine the vlan interfaces you have configured

xASWy#**show run**
What is the status of the vlan 1 interface? _____

Step 19: To be certain you understand how your new VLAN configuration affects IP connectivity make the following predictions:
(Please circle your prediction BEFORE you actually ping)

Prediction: A ping from your ASW to your own PC will be successful. True/False

Result: successful/unsuccessful

Explain this result: _____

_____

_____

_____

Prediction: A ping from your PC to your partner's PC will be successful.
True/False

Result: successful/unsuccessful

Explain this result: _____

_____

_____

_____

Task 3: Create a new VLAN on your DSW (Distribution Switch) and assign it to the appropriate ports

Step 20: Make a console connection to your DSW (turn A/B switch to B).

Step 21: Display the default VLANs on your DSW.

xDSWy# **show vlan**

How many default VLANs are there? _____

Why isn't your DSW aware of VLANs 2,3,4 & 5? _____

_____

Step 22: Verify connectivity with your ASW

xDSWy# **show cdp neighbor**

Which interface on your DSW is connected to your ASW? _____

Step 23: Use the following command to check which VLAN the interface connected to the ASW is in:

xDSWy# **show interface f0/9 switchport**

Step 24: Create VLAN 3 and 4 and restore IP connectivity

xDSWy# **vlan database**
xDSWy(vlan)# **vtp domain BCMSN**
xDSWy(vlan)# **vlan 3 name 3rd_Floor**
xDSWy(vlan)# **vlan 4 name 4th_Floor**
xDSWy(vlan)# **exit**

Step 25: Assign VLAN 3 to all ports between f0/5 and f0/12 (this includes the port connecting your DSW with your ASW). Assign VLAN 4 to all ports between f0/1 and f0/4.

xDSWy(config-if)# **switchport access vlan 3**
repeat for all interfaces from f0/5 to f0/12

xDSWy(config-if)# **switchport access vlan 4**
repeat for all interfaces from f0/1 to f0/4

Step 26: Go back to your ASW and assign VLAN 3 to the port connected to your DSW (it should be interface f0/09).

What is the command to put f0/9 into vlan 3 on your ASW? _____

STOP!! Check to see your Switch Block partner has reached this step. If not, wait for them to catch up before you continue.

Step 27: Make the following prediction:

Prediction: A ping from your PC to your partner's PC will be successful.
True/False

Result: successful/unsuccessful

Explain this result: _____

If you are having trouble with this prediction, go back to the previous diagram and label the VLAN each port is in on all switches between your PC and your partner's PC.

Step 28: Assign VLAN 3 to the port connecting your DSW with your partner's DSW

Step 29: Verify you VLAN port assignments

xDSWy# **show interface f0/1 switchport**

Step 30: To be certain you understand how your new VLAN configuration affects IP connectivity make the following predictions:

Prediction: A ping from your PC to your partner's PC will be successful.
True/False

Result: successful/unsuccessful

Explain this result: _____

Prediction: A ping from your DSW to your partner's DSW will be successful.
True/False

Result: successful/unsuccessful

Explain this result: _____

What VLAN is the management interface of your DSW in? _____

xDSWy# **show ip interface brief**

Step 33: Move the management interface of each DSW to VLAN 3, provide the proper ip address for sc0 in that vlan, and make the following predictions:

xDSWy(config)# **interface vlan 3**
xDSWy(config-if)# **ip address 10.3.x.y 255.255.0.0**
xDSWy(config-if)# **management**
xDSWy(config-if)# **end**

Prediction: A ping from your PC to your partner's PC will be successful.
True/False

Result: successful/unsuccessful

Explain this result: _____

Prediction: A ping from your DSW to your partner's DSW will be successful.
True/False

Result: successful/unsuccessful

Explain this result: _____

Prediction: You can ping from your DSW, ASW and PC to your partner's DSW, ASW and PC (everywhere within your Switch Block). True/False
(Be certain to try a ping from your ASW)

Result: successful/unsuccessful

Explain this result: _____

Prediction: You can ping from your PC in vlan 3 to a PC in another Switch Block that is also in vlan 3 (assuming they have done all of the steps you have done).
True/False

Result: successful/unsuccessful

Explain this result: _____

Congratulations! You are ready to move on to Trunking and VTP

Lab #3

Enable VTP (VLAN Trunk Protocol)

Objective:

In this lab, the nuances of Cisco's VTP (VLAN Trunk Protocol) protocol will be explored including the effect of different VTP modes, different domain names and different configuration revision numbers. VTP pruning will be enabled. To accomplish this objective you need to perform the following tasks:

1. Place DSW1 in each group into a VTP domain.
2. Create new VLANs on the DSWs.
3. Enable trunking on all DSW ports connecting the switches within your switch block.
4. Explore VTP operation by examining configuration revision numbers, the effects of changing VTP domains, and VTP modes.
5. Enable VTP pruning on the switches in your switch block.

Estimated Time: 1:20 minutes

It is important to coordinate your actions with all members of your switch block so that commands can be issued and their consequences examined by all switch block members. Please do not race ahead.

Task1: **Prepare to enable VTP by configuring a VTP domain on one DSW switch, create VLANs, enable VTP by trunking and examine the consequences.**

Step 1: Examine the current VLAN database on each DSW.

xDSWy#**show vlan**

Which non-default VLANs exist from the prior lab? _____
What is the current configuration revision number? _____

Step 2: Examine the default vtp mode

xDSWy#**show vtp stat**

What is the default VTP mode? _____

Step 3: **DSW1 Only:** Place **ONLY** DSW1 into a VTP domain named SwitchBlockX (yes, spell it using exactly the same capitalization. The "X" is to be replaced with your Switch Block number). Then create 6 new VLANs. Notice that you are creating vlan 5, but giving it a different name than the vlan 5 you created on your ASW.

xDSW1# **vlan database**
xDSW1(vlan)# **vtp domain SwitchBlockX**
xDSW1(vlan)#**vlan 5 name 500th_Floor**
xDSW1(vlan)# **vlan 6 name 6th_Floor**
xDSW1(vlan)# **vlan 7 name 7th_Floor**
xDSW1(vlan)# **vlan 8 name 8th_Floor**
xDSW1(vlan)# **vlan 9 name 9th_Floor**
xDSW1(vlan)# **vlan 10 name 10th_Floor**
xDSW1(vlan)# **exit**

Step 4: **DSW2 Only:** Create VLAN 6 on **ONLY** the DSW2 in each switch block, but provide a different name than it was given by DSW1 (something other than 6th_Floor). Also create new vlan 11. For now, do not change the vtp domain for DSW2.

XDSW2# **vlan database**
xDSW2(vlan)# **vlan 6 name 600th_Floor**
xDSW2(vlan)# **vlan 11 name 11th_Floor**
xDSW2(vlan)# **exit**

Step 5: Examine the current vtp and VLAN database information on each switch.

xDSWy# **show vlan**
xDSWy# **show vtp stat**

Do vlan 3 and 4 still exist on DSW1 after you changed its vtp domain? _____
What is the current configuration revision number on DSW1? _____
What is the current configuration revision number on DSW2? _____
What is the current configuration revision number on ASW3? _____
What is the current configuration revision number on ASW4? _____
What vtp domain is DSW1 and ASW3 in? _____ and _____
What vtp domain is DSW2 and ASW4 in? _____ and _____

Is either ASW aware of the new vlans that were created on either DSW? _____
Why? _____

Step 6: Enable trunking on the link between DSW1 and DSW2, then examine the port status on both DSW's

xDSWy# **config t**
xDSWy(config)# **int f 0/1**
xDSWy(config-if)# **switchport mode trunk**
xDSWy(config-if)# **end**
xDSWy#**show interface f 0/1 switchport**

Is trunking enabled on port f0/1 of both DSW's? _____ ?

Step 7: Now that trunking has been enabled, are both DSW's aware of the vlans that were created on the other switch? _____ Why? _____
_____

Task 2: Synchronize vlan databases while examining the effects of differing configuration revision numbers.

Step 8: **ASW3 Only**: On ASW3, ONLY, change its vtp domain to SwitchBlockX. The result will be that DSW1 and ASW3 are in the SwitchBlockX vtp domain and DSW2 and ASW4 are in the BCMSN domain.

xASW3#**vlan database**
xASW3(vlan)#**vtp domain SwitchBlock*{SB#}*** (*use your own SB number*)
Changing VTP domain name from BCMSN to SwitchBlock*X*
xASW3(vlan)#**exit**
APPLY completed.
Exiting....

xASW3#**show vtp status**
xASW3#**show vlan**

Now that you changed vtp domains, do you still have vlans 2-5 on ASW3? _____
Why? _____
Be certain to inform you partner of the result.

Step 9: Go to your DSW's and enable isl trunking on the connection to each ASW.

xDSWy(config-if)#**switchport mode trunk**
xDSWy(config-if)#**end**
xDSWy#**show interface f 0/9 switchport**

Step 10: Go to your ASW and enable isl trunking on the link to each DSW.

xASWy#**configure terminal**
xASWy(config)#**interface f0/9**
xASWy(config-if)#**switchport mode trunk**
xASWy(config-if)#**end**
xASWy#**copy run start**

Step 11: Both ASWs are in a separate vtp domains with their respective DSWs. What is your prediction of what vlans are in the vlan database (Remember that we created vlans 2,3,4 and 5 on each ASW in a prior lab):
XASW3: _____
XASW4: _____
Coordinate this answer with your partner

Examine the vlan database on each ASW. What has actually changed in the ASW's vlan databases now that trunking is enabled?
XASW3: _____
XASW4: _____
Coordinate this answer with your partner.

Why did these changes occur? _____
_____
_____

Step 12: Can you ping all locations in your Switch Block? **First**, place your predictions in the following table, then ping to verify your predictions.

	DSW2	**ASW4**	**PC6**
DSW1			
ASW3			
PC5			

Why did you obtain these results? _____

When you ping, do the frames travelling between each switch have a vlan 3 identifier tag or are they ordinary ethernet frames? _____

_____

What effect do the different vtp domains have on your ability to ping the various locations in your Switch Block? _____

_____

Task 3: Move all switches into a single vlan and synchronize databases

Step 13: Fill in the following vtp and vlan information about each of your switches.

	vtp domain	**config revision #**	**List of non-default vlans in domain**
DSW1 and ASW3			
DSW2 and ASW4			

Step 14: Move DSW1 back to the BCMSN domain

xDSW1(vlan)# **vtp domain BCMSN**
xDSW1(vlan)# **exit**
xDSW1# **sh vtp stat**

Move ASW3 back to the BCMSN domain

xASW3#**vlan database**
xASW3(vlan)#**vtp domain BCMSN**
Changing VTP domain name from SwitchBlock5 to BCMSN
xASW3(vlan)#**exit**
APPLY completed.
Exiting....

Step 15: Examine the vtp domain and configuration revision number on DSW1. You may have to wait a few seconds for the database to update.

xDSW1# **show vtp stat**

Fill in the following vtp and vlan information about each of your switches.

	vtp domain	**Config revision #**	**List of non-default vlans in domain**
DSW1 and ASW3			
DSW2 and ASW4			

Did the configuration revision number increment on any switch? _____

Do all switches have the same configuration revision number and vlans in their databases? _____

Step 16: Examine the status of ports 1-12 on each DSW

xDSW1#**show interface**

Step 17: It is now time to observe the power and speed of vtp. When both partners are ready, have one partner create vlan 12 on their DSW.

xDSW1(vlan)# **vlan 12 name vlan_12**

As soon as the command is entered, examine the vlan database to see how long it takes the other DSW to learn of the new vlan.

xDSW1#**show vlan**

Step 18: The power to add a vlan is also the power to delete one. Have the partner that did NOT create vlan 12, type in the following command.

xDSW1(vlan)# **no vlan 4**
xDSW1(vlan)# **exit**

xDSW1#**show interface**

What is the interface status for ports 1-12? _____

Step 19: Have the partner that did NOT delete vlan 4 recreate it

xDSW1(vlan)# **vlan 4**

Examine the status of interfaces 1-12

Task 4: Enable VTP Pruning

Step 20: Ensure that all switches in the BCMSN domain are capable of vtp pruning

On each DSW, enter the following command:
xDSWy#**show vtp stat**

Are the DSWs version 2 capable? _____
Is vtp pruning enabled by default? _____

On each ASW, enter the following command:
xASWy#**show vtp status**

Are the ASWs version 2 capable? _____
Is vtp pruning enabled by default? _____

Step 21: Enable vtp pruning on a single ASW (agree between you and your partner who will enter the following commands).

xASWy#**vlan database**
xASWy(vlan)#**vtp pruning**
Pruning switched ON
xASWy(vlan)#**exit**
APPLY completed.
Exiting....
xASWy#**sh vtp status**

Step 22: Examine the vtp pruning status on each switch in the switch block.

Has pruning been enabled on each switch? _____
Does enabling pruning also enable vtp version 2? _____

Task 5: **Clean up the vlan database and re-establish connectivity in vlan 1**

Step 23: To complete this lab, after both you and you partner have reached this step, delete all vlans in the BCMSN domain. If you do this first it only needs to be done from a single switch. From a DSW:

xDSW1(vlan)# **no vlan 3**

Repeat for all other vlans that were created in this lab.

xDSW1# **show vlan**

Step 24: On each DSW, move management back to vlan 1, reassign the correct vlan 1 ip address to the switch, turn off trunking, and place all ports back into vlan 1.

xDSWy(config)# **int vlan 1**
xDSWy(config)# **management**
xDSWy(config)# **interface f0/1**
xDSWy(config-if)# **switchport mode access**
xDSWy(config-if)# **switchport access vlan 1**
(Repeat on interfaces f0/1 to f0/12)
xDSWy(config-if)# **end**
xDSWy# **copy run start**

Step 25: On each ASW, turn off trunking, change the management vlan back to vlan 1, and place all ports back into vlan 1.

xASWy(config)#**int f0/9**
xASWy(config-if)#**switchport mode access**

xASWy(config-if)#**int vlan 1**
xASWy(config-if)#**management**
xASWy(config-if)#**int f0/1**
xASWy(config-if)#**switchport access vlan 1**
(Repeat on interfaces f0/1 to f0/11)
xASWy(config-if)#**end**
xASWy#**copy run start**

Step 26: Reconfigure a vlan 1 ip address on your pc and reboot it. Verify that you have established connectivity between all switches and your pc in vlan 1 by pinging all switches in your Switch Block.

Will you be able to ping switches in other Switch Blocks? _____ Try it.
Good Work!!!

Lab #4

Configuration of STP (Spanning Tree Protocol)

Objective:

In this lab, the nuances of STP will be explored including identifying the root bridge, establishing a root & secondary root bridge, identifying the path data is taking in a bridged network with redundant links, and enabling PortFast. To accomplish this objective you need to perform the following tasks:

1. Create redundant links to meet the demand for network availability and reliability.
2. Identify the root bridge.
3. Designate a root bridge and secondary root bridge
4. Enable portfast on ports connected to endstations

Estimated Time: 30 minutes

Task 1: Add physical links to create redundancy in our network.

Step 1: Physically create redundant links using the tables below and the Figure on the next page as a guide.

Odd

The primary link for each odd ASW is the odd DSW. The secondary link for each odd ASW is a separate physical connection from f0/11 to the even DSW's f0/11. To create a redundant link to the Core, now connect from your port f0/4 to the Core.

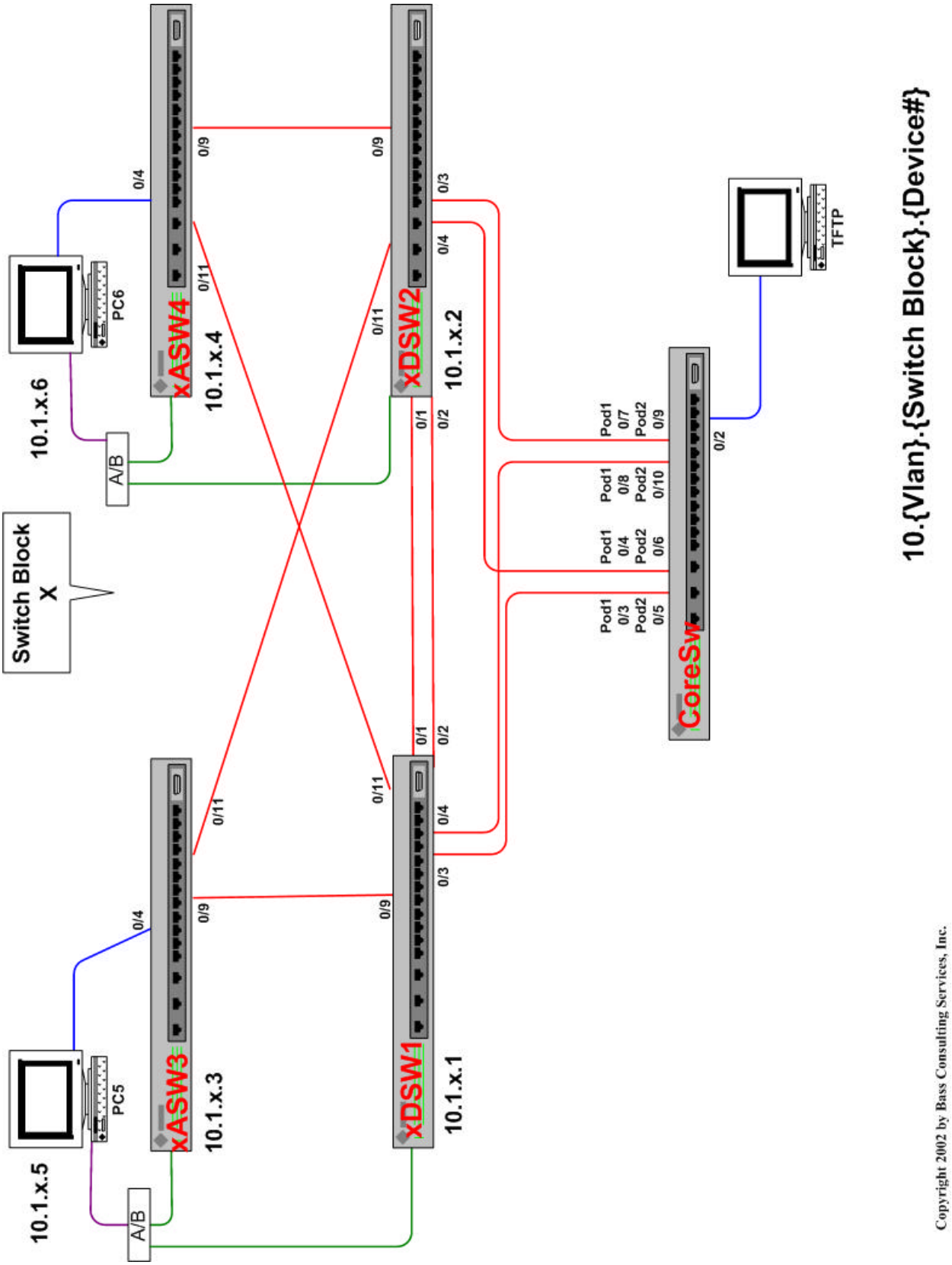
Even

The primary link for each even ASW is the even DSW. The secondary link for each even ASW is a separate physical connection from f0/11 to the odd DSW's f0/11. To create a redundant link to the Core, now connect from your port f0/4 to the Core.

Connect the DSWs within each Switch Block with a redundant link from f0/2 to f0/2.

Cabling exactly this way will be IMPORTANT in future labs.

	ASW3 port		**Core**
Primary Link	0/9	0/9 – DSW1	DSW 0/3
Secondary Link	0/11	0/11 – DSW2	DSW 0/4



Step 2: From your DSW verify that all primary and secondary ports are connected; i.e. that a physical loop has been created.

xDSWy# **show interface**
xDSWy# **show cdp neighbor**

If a neighboring switch does not appear in your cdp database, but the port shows connected, what is the most likely cause of this problem? _____

_____

_____

Step 3: To simplify our analysis and allow each Switch Block to have its own root bridge, you need to administratively disable all ports on each DSW which connect to the Core Switch.

xDSWy(config)# **int f0/3**
xDSWy(config)# **shut**
xDSWy(config)# **int f0/4**
xDSWy(config)# **shut**
xDSWy(config)# **end**

Each Switch Block is now an "island" with redundant links between all four switches.

Step 4: Identify the root bridge

xDSWx# **show spanning-tree 1** (get in the habit of placing the vlan # at the end of this command. If you do NOT specify a vlan, then the **vlan 1** spanning-tree information will be displayed.

Identify the switch that is the Designated Root.

What is the "Designated Root Priority" of the root bridge? _____

If a DSW is not the root, then an ASW became the root. To check, go to your ASW and type:

xASWy#**show spanning-tree** (if the ASW is the root it will say "**we are the root..**")

Task 2: **Designate a primary and secondary root bridge.**

Step 5: From your DSW, execute the following command:

5DSW1> (enable) **set spantree ?**

Notice that there are two commands which can be used to designate a root bridge; set spantree root <vlan> or set spantree priority

Step 6: On the **EVEN** DSW in your Switch Block, designate it to be the secondary root bridge for vlan 1 with a priority of 0x4000

xDSW2(config)# **spanningtree priority 16384**
xDSWy# **show spanning-tree 1**

Which DSW is now the root bridge? _____
What is the "Designated Root Priority" of the root bridge? _____

Step 7: On the **ODD** DSW in your Switch Block, designate it to be the root bridge for vlan 1 with a priority of 0x2000

xDSW1(config)# **spanningtree priority 8192**
xDSWy# **show spanning-tree 1**

Which DSW is now the root bridge? _____
What is the "Designated Root Priority" of the root bridge? _____

Task 3: Enable portfast on appropriate ports.

Step 8: Go to the MSDOS prompt on your pc and execute the doskey command

C:\windows**doskey** (this will allow you to use your up arrow to recall previous commands

Step 9: Initiate a continuous ping from your MSDOS prompt to your DSW

C:\windows**ping 10.1.5.1 –t** (put a "-t" at the end to make it continuous)

While you are watching the MSDOS prompt, quickly disconnect and reconnect the ethernet cable from your ethernet card. Watch your MSDOS prompt and time how long it takes for the pings to resume.

How long did it take for the pings to resume? _____

Remember that spanning tree is enabled by default and that every time there is a topology change the switch port will go through the spanning tree steps of blocking, listening, learning and then forwarding or blocking.

Step 10: Initiate a continuous ping from your MSDOS prompt to your DSW again.

C:\windows**ping 10.1.5.1 –t** (put a "-t" at the end to make it continuous. The continuous ping can be stopped with a <Ctrl>c command)

Go to your ASW and turn on debugging of spanning tree events
xASWy#**debug spanningtree events**

This time use your console connection to your ASW to observe the status of the port where your pc is connected, as you quickly disconnect and reconnect the ethernet cable from your ethernet card.

Step 11: Enable portfast on ports f0/4 of your ASW

xASWy#**conf t**
xASWy(config)#**int f0/4**
xASWy(config-if)#**spanning-tree portfast**

Step 12: Initiate a continuous ping from your MSDOS prompt to your DSW

C:\windows**ping 10.1.5.1 –t** (put a "-t" at the end to make it continuous)

While you are watching the MSDOS prompt, quickly disconnect and reconnect the ethernet cable from your ethernet card. Watch your MSDOS prompt and time how long it takes for the pings to resume.
How long did it take for the pings to resume? _____

What spanning tree debug messages were displayed on you ASW console? _____
_____
_____

Turn off all debugging on your ASW

xASWy#**no debug all**

Look at the configuration file of your ASW under int f0/4. Does portfast show up in the configuration? _____
xASWy#**sh run**

Step 13: Initiate a continuous ping from your MSDOS prompt to your DSW

C:\windows**ping 10.1.5.1 –t**

Which path are these pings taking to get from your ASW to your DSW? _____
_____

The following command will assist you

xASWy**show spanning-tree int f0/9**
xASWy**show spanning-tree int f0/11**

The data from either you or your partner will not be taking the most direct route. This is because if your primary assigned DSW is NOT the root bridge then your data path will not be optimal. Your ASW will be blocking out the port toward your DSW because you never block out the designated port (the port used to get to the root). We can manipulate spanning tree port costs or spanning tree port vlan priorities to overcome this problem when we have more than one vlan.

Simulate a failure in the network by going to the **port on your ASW which is forwarding and shut it down**. See how long it takes for your pings to resume.

xASWy**conf t**
xASWyconfig)#**int f0/9** (or int f0/11)
xASWyconfig-if)#**shutdown**

Once the pings have resumed, re-enable the port.
xASWy(config-if)#**no shutdown**

Is there an interruption in the pings? _____
When the second link comes back up, which way is your data going? _____

_____

Good Work!

Lab #5

Configuration of Fast Etherchannel and UplinkFast

Objective:

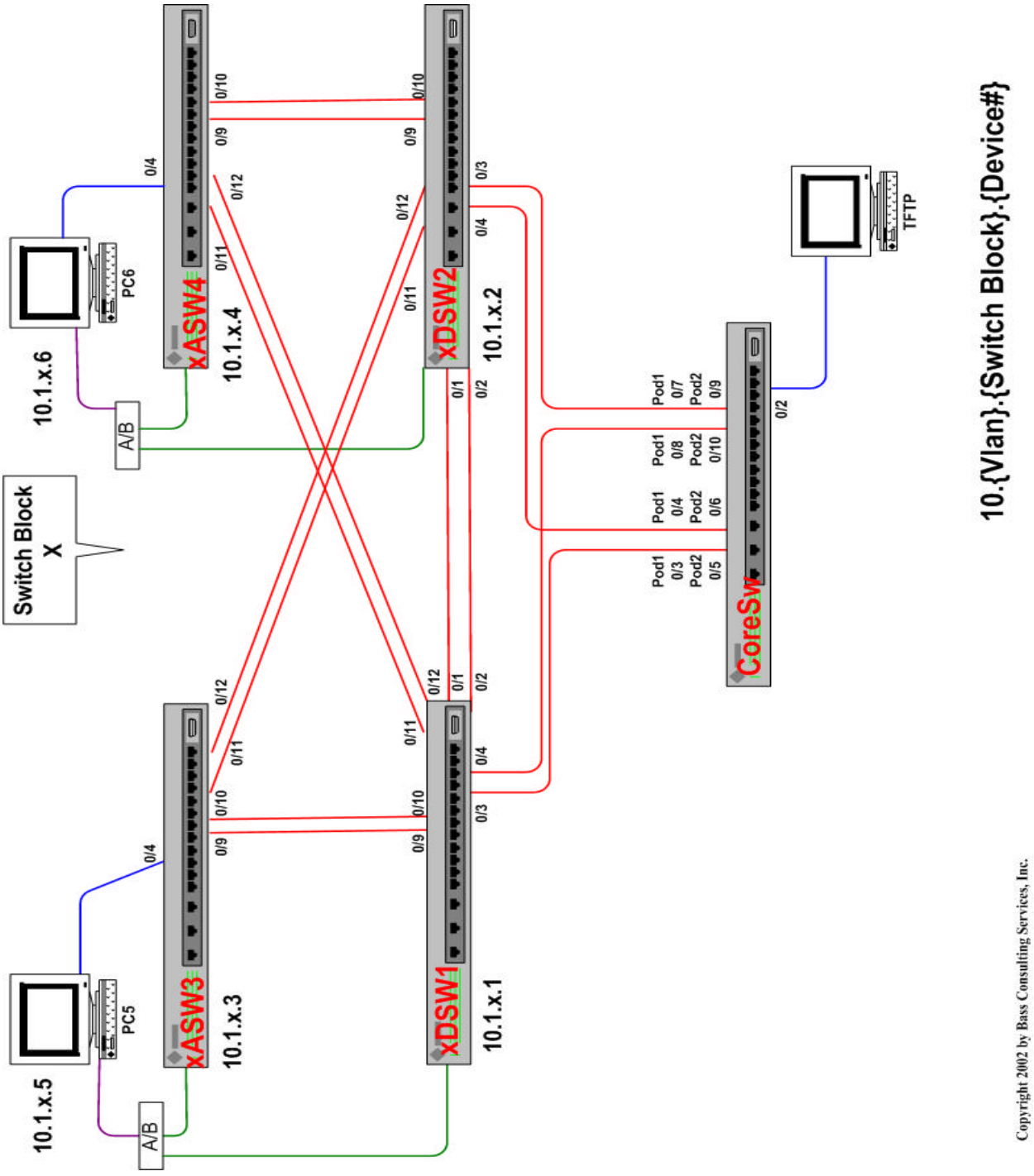
In this lab, you will continue to optimize the network. The first step is to take advantage of the available bandwidth between switches by configuring Fast Etherchannel. Uplinkfast will then be configured to limit network downtime. To accomplish this objective you need to perform the following tasks:

1. Prepare the switch for the creation of the etherchannel links.
2. Create the Fast Etherchannel links..
3. Enable trunking across the Etherchannel links
4. Configure Uplinkfast

Estimated Time: 45 minutes

Task 1: **Prepare and configure the switch for Fast Etherchannel operation.**

Step 1: Physically connect eligible ports. Eligible ports have to be capable of etherchannel operation. No 10Mb cards and only some 10/100Mb or 100Mb ethernet ports are capable of FEC (Fast Etherchannel) in the 5000 series. The 29/3500XL ports are etherchannel capable, but the eligible ports will need to be placed into a port group. This will be done in subsequent Steps.



Step 2: Identify the ports that are going to be channeled:

xASW3 - f0/9-10 to DSW1 – f0/9-10
xASW3 - f0/11-12 to DSW2 – f0/11-12
xASW4 - f0/9-10 to DSW2 – f0/9-10
xASW4 - f0/11-12 to DSW1 – f0/11-12
xDSW1 – 0/1-2 to DSW2 – 0/1-2.

What will spanning tree do now that we have redundant links? _____

_____

Step 3: Verify all ports that are going to be part of each channel have the same:
Speed and Duplex Native vlan (the vlan a port is in before trunking is enabled. It is also the vlan the port will belong to if trunking is turned off). If your management vlan is vlan one, then it would be wise to keep the native vlan on all trunk ports vlan 1. Trunking mode
Because we placed all ports in vlan 1 in a prior lab and you already manually set speed and duplex on all ports, the only thing we will modify is channeling and trunking (in later steps). For each port that is going to be part of a channel, if the duplex is not already set full, speed to 100 and the port in vlan 1, please make these changes now for ports f0/9, f0/10, f0/11 and f0/12 on your ASW and on your DSW - otherwise channeling WILL FAIL!

Step 4: Make DSW1 the root of vlan 1
DSW1 only xDSW1(config)# **spanningtree priority 1** (on DSW1 only)

Step 5: On each ASW verify the spanning tree state of interfaces f0/09-12 and record it in the table, then mark the spanning tree port state on the switchblock diagram at the beginning of Task 1 next to each port. **Also ask your partner for their spanning tree information and mark it on the diagram.**

xASWy#**show spanning-tree vlan 1 int f0/?**

	Connection to primary DSW		**Connection to secondary DSW**	
port	int f0/9	int f0/10	int f0/11	int f0/12
STP state				

On each DSW verify the spanning tree state of interfaces f0/1, f0/2, f0/9, f0/10, f0/11 and f0/12 and record it in the table then mark the spanning tree port state on the switchblock diagram at the beginning of Task 1 next to each port. **Ask your partner for their spanning tree information and mark it on the diagram, too.**

xDSWy# **show spanning-tree 1** or
xDSWy# **show spanning-tree int f0/1** (repeat for each interface)

	Partner DSW		**Primary ASW**		**Secondary ASW**	
port	F0/1	F0/2	F0/09	F0/10	F0/11	F0/12
STP state						

Step 6: Prepare your ASW for the two etherchannel links by creating two port groups and placing f0/9 and f0/10 in one port group and f0/11 and f0/12 in another port group.

xASWy#**conf t**
xASWy(config)#**int f0/9**
xASWy(config-if)#**port group 1**
xASWy(config-if)#**int f0/10**
xASWy(config-if)#**port group 1**
xASWy(config-if)#**int f0/11**
xASWy(config-if)#**port group 2**
xASWy(config-if)#**int f0/12**
xASWy(config-if)#**port group 2**
Remember to do a copy run start after this configuration

Step 7: Create the etherchannel links from your DSW. Do this slowly and watch the console messages.

xDSWy#**conf t**
xDSWy(config)#**int f0/9**
xDSWy(config-if)#**port group 1**
xDSWy(config-if)#**int f0/10**
xDSWy(config-if)#**port group 1**
xDSWy(config-if)#**int f0/11**
xDSWy(config-if)#**port group 2**
xDSWy(config-if)#**int f0/12**
xDSWy(config-if)#**port group 2**

Step 8: On each DSW verify the spanning tree state of ports f0/1, f0/2, f0/9, f0/10, f0/11 and f0/12

xDSWy# **show spanning-tree 1**

Notice that the not all ports in each channel group are listed. If you see all ports, something is configured wrong and the channel is not being created.

Step 9: Wait until the STP state of each channel is forwarding or blocking. On each DSW verify the spanning tree state of interfaces f0/1, f0/2, f0/9 (or f0/10) and f0/12 (ror f0/11) record it in the table.

xDSWy# **show spanning-tree 1** or
xDSWy# **show spaning-tree int f0/1** (repeat for each interface)

	Partner DSW		**Primary ASW**		**Secondary ASW**	
port	F0/1	F0/2	F0/9	F0/10	F0/11	F0/12
STP state						

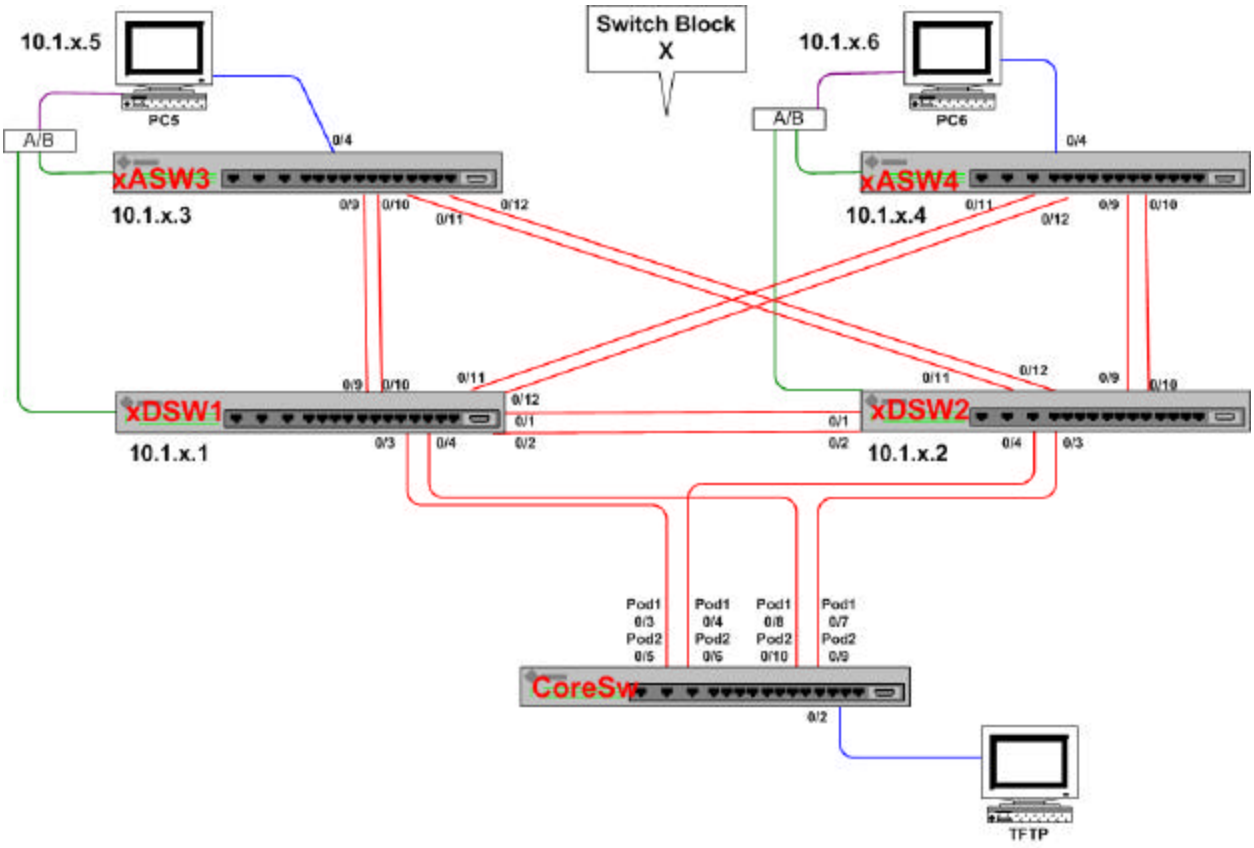
Record these results on the network diagram on the next page and include your partner's results. Compare this to the network diagram you drew in Step 5.

Why does at least one DSW show forwarding on all ports? _____

_____

Step 10: On the next page, label the root bridge and indicate whether each interface in use is either forwarding or blocking on each switch

Label the root bridge and indicate whether each interface in use is either forwarding or blocking.



Step 13: Go to your ASW and enable isl trunking on the link to each DSW.

xASWy#**configure terminal**
xASWy(config)#**interface f0/9**
xASWy(config-if)#**switchport mode trunk**
xASWy(config-if)#**int f0/10**
xASWy(config-if)#**switchport mode trunk**
xASWy(config-if)#**int f0/11**
xASWy(config-if)#**switchport mode trunk**
xASWy(config-if)#**int f0/12**
xASWy(config-if)#**switchport mode trunk**
xASWy(config-if)#**end**
xASWy#**copy run start**

Step 14: Go to your DSW and enable isl trunking on the link to each DSW.

xDSWy#**configure terminal**
xDSWy(config)#**interface f0/9**
xDSWy(config-if)#**switchport mode trunk**
xDSWy(config-if)#**int f0/10**
xDSWy(config-if)#**switchport mode trunk**
xDSWy(config-if)#**int f0/11**
xDSWy(config-if)#**switchport mode trunk**
xDSWy(config-if)#**int f0/12**
xDSWy(config-if)#**switchport mode trunk**
xDSWy(config-if)#**end**
xDSWy#**copy run start**

Task 2: Enable Uplinkfast on each ASW

Step 15: Start a continuous ping from your pc to your DSW

Step 16: Go to your ASW and verify which etherchannel trunk is being used to forward your pings to the DSW. Which etherchannel trunk is forwarding in vlan1? _____

Step 17: Enable uplinkfast on your ASW (you should only do this on access switches)

xASWy#conf t
xASWy(config)#**spanning-tree uplinkfast**
xASWy(config)#**end**
xASWy#**copy run start**

Step 18: While continuously pinging from your pc to the DSW, go to your ASW and disable the etherchannel ports which the pings are departing on. Remember that at least one port on the switch that uplinkfast is configured on must be blocking, therefore, your ASW can not be the root bridge. Neither ASW should be the root because in a prior

lab you configured one DSWs to be the primary root bridge and the other DSW to be the secondary root bridge in vlan 1.

Verify the port which is forwarding (so you can shut it down):

xASWy# **show spanning tree** also find the line that states that "Fast uplink switchover is enabled") Compare the results of the last command results with:
xASWy#**show spanning-tree vlan 1 int f0/? (f0/9,f0/10,f0/11 and f0/12)**

Why don't you see all of the ports with the first command? _____

Now disable the forwarding ports:

If the forwarding path is via f0/9 & f0/10, then:

xASWy(config-if)#**int f0/9**
xASWy(config-if)#**shut**
xASWy(config-if)#**int f0/10**
xASWy(config-if)#**shut**

If the forwading path is via f0/11 & f0/12, then:

xASWy(config-if)#**int f0/11**
xASWy(config-if)#**shut**
xASWy(config-if)#**int f0/12**
xASWy(config-if)#**shut**

How long does it take for you pings to successfully resume? _____

xASWy(config-if)#**int f0/9 or f0/11**
xASWy(config-if)#**no shut**
xASWy(config-if)#**int f0/10 or f0/12**
xASWy(config-if)#**no shut**
xASWy(config-if)#**end**

Good Work!!!!

Lab #6

Inter-VLAN Routing

Objective:

In this lab, you will configure a 2600series router to route between VLANs. To accomplish this objective, you need to perform the following tasks:

1. Within each Switch Block, the management vlan will remain vlan 1, and all switches will be reconfigured to have a new ip address, mask and gateway assigned to this vlan.

2. Each pc within a Switch Block will be placed in a different vlan. Therefore, each pc will be configured with a new ip address, mask and gateway assigned to their respective vlan.

3. All switches within a Switch Block will be assigned to a vtp domain unique to that Switch Block.

4. Two new vlans will be created, one for each student workstation.

5. Two additional vlans will be created to be used to route into the Core.

6. The new vlans will then be assigned to ports.

7. The router will then be configured with ip addresses and other information necessary to route between the different vlans.

Estimated Time: 1 hour

Task 1: **Understand the network design and assigned ip addresses and configure your switches and pc with the appropriate address.**

Step 1: There will be three vlans used for communication within each Switch Block. Vlan 1 will be used as the management vlan for the switches, the odd numbered pc (PC5) in each Switch Block will be assigned to vlan 21 and the even numbered pc (PC6) will be assigned to vlan 22.

Vlans 51 and 52 will be used to send data from each switch block into the Core. The instructor will place the lower ports on the Core into vlan 51 and the higher ports on Core into vlan 52.

Because of the way you cabled, if you are an **odd** DSW, your f0/3 port will be assigned to vlan 51 and your f0/4 will be assigned to vlan 52.
If you are an **even** DSW, your f0/3 port will be assigned to vlan 52 and your f0/4 will be assigned to vlan 51. If the core switch is not placed into these vlans, cdp v2 will indicate that there is a native vlan mismatch, but the lab would still work.

We will now be using a 24 bit mask for all ip addresses (255.255.255.0). The subnets associated with your vlans will be 10.*{vlan #}.{switch block#}*.0. Notice that while each Switch Block will have a vlan 1, 21 and 22, there will be a separate subnet associated with each. This is because these vlans will be separated by a router and are independent of one another.

The only exception will be vlans 51 and 52 which will be used to connect the Switch Blocks. The ip subnet for these vlans will use a "**7**" in the third byte making the subnets for these vlans 10.51.7.0 and 10.52.7.0. Each of your routers will get a separate host ip address assigned to it in both vlans 51 and 52.

Review the following table very carefully. Remember that there are two routers in each switch block. If a router is connected to the odd DSW it will be known as the odd router and the even router will be on DSW2. The addressing convention for router's vlan interfaces is:

10.*{vlan#}.{switch block}*. **7** for the **odd** router and
10.*{vlan#}.{switch block}*. **8** for the **even** router.
(Vlans 51 and 52 which we use to get into the core will be addressed differently, however.)

Each ROUTER in the Switch Block will have a separate vlan interface for vlans 1, 51 and 52 and a separate ip address and MAC address has been assigned for each one. In this lab, one ROUTER will also get an address on vlan 21 and the other (even) ROUTER will get an address on vlan 22. The same MAC address has been assigned to the ROUTER interface for vlans 1,21 and 22 in each switch block because these mac addresses will be unique on their respective segments.

For every address in the table on the next page and the vlan 52 table which follows, take your pen and overwrite "{SB#}" and each "x" with your real Switchblock number. You will then have all of the correct addresses to configure your ASW's vlan1 interface, your DSW's sc0 interface with address in vlan 1, your pc's address (in either vlan 21 or 22) & and your ROUTER's vlan 1,51,52, interfaces. Each ROUTER will also have either a vlan 21 or 22 address that will have to be configured. There is also a chart for you to complete on the page after next.

Please read the instructions on the last page prior to reviewing this chart.

Vlan #	**Device**	**IP Address/mask** for the sc0's of DSWs, the ASW's management interfaces and pc's	Only look at this column if you are an **ODD** DSW. The router's IP Address & assigned MAC for the **odd DSW**	Only look at this column if you are an **EVEN** DSW. The router's IP Address & assigned MAC for the **even DSW**
1	xDSW1	10.1.{SB#}.1 /24 (address for odd DSW's sc0)	**This will be the odd router's address in vlan 1:** 10.1.*{SB#}*.7 /24 5000.0017.0001	**This will be the even router's address in vlan 1:** 10.1.*{SB#}*.8 / 24 5000.0018.0001
1	xDSW2	10.1.{SB#}.2 /24 (address for the even DSW's sc0)		
1	xASW3	10.1.{SB#}.3 /24		
1	xASW4	10.1.{SB#}.4 /24		
21	xPC5	10.21.{SB#}.5 /24 address for odd pc's	**This will be the odd router's address in vlan21:** 10.21.{SB#}.7 /24 5000.0017.0021	
22	xPC6	10.22.{SB#}.6 /24 address for even pc's		**This will be the even router's address in vlan22:** 10.22.*{SB#}*8 / 24 5000.0018.0022
51			**This will be the odd router's address in vlan 51:** (10.51.7.(add 10 to *{SB#}*) /24 to get your router's **int vlan 51** address) see below for exact address for **int vlan 51**: 10.51.7.11 – {SB#}1 5000.0051.0011 10.51.7.12 – {SB#}2 5000.0051.0012 10.51.7.13 – {SB#}3 5000.0051.0013 10.51.7.14 – {SB#}4 5000.0051.0014 10.51.7.15 – {SB#}5 5000.0051.0015 10.51.7.16 – {SB#}6 5000.0051.0016	**This will be the even router's address in vlan 51:** (10.51.7.(add 20 to *{SB#}*) /24 to get your router's **int vlan 51** address) see below for exact address for **int vlan 51**: 10.51.7.21 – {SB#}1 5000.0051.0021 10.51.7.22 – {SB#}2 5000.0051.0022 10.51.7.23 – {SB#}3 5000.0051.0023 10.51.7.24 – {SB#}4 5000.0051.0024 10.51.7.25 – {SB#}5 5000.0051.0025 10.51.7.26 – {SB#}6 5000.0051.0026

52			Only look at this column if you are an **ODD** DSW **This will be the odd router's address in vlan 52:** (10.52.7.(add 10 to *{SB#}*) /24 to get your router's **int vlan 52** address) see below for exact address for **int vlan 52**: 10.52.7.(add 10 to *{SB#}*) /24 to get router address 10.52.7.11 – {SB#}1 5000.0052.0011 10.52.7.12 – {SB#}2 5000.0052.0012 10.52.7.13 – {SB#}3 5000.0052.0013 10.52.7.14 – {SB#}4 5000.0052.0014 10.52.7.15 – {SB#}5 5000.0052.0015 10.52.7.16 – {SB#}6 5000.0052.0016	Only look at this column if you are an **EVEN** DSW **This will be the even router's address in vlan 52:** (10.52.7.(add 10 to *{SB#}*) /24 to get your router's **int vlan 52** address) see below for exact address for **int vlan 52**: 10.52.7.(add 20 to *{SB#}*) /24 to get router address 10.52.7.21 – {SB#}1 5000.0052.0021 10.52.7.22 – {SB#}2 5000.0052.0022 10.52.7.23 – {SB#}3 5000.0052.0023 10.52.7.24 – {SB#}4 5000.0052.0024 10.52.7.25 – {SB#}5 5000.0052.0025 10.52.7.26 – {SB#}6 5000.0052.0026

Notice that all 12 router interfaces in vlan 51 get separate host addresses on the same subnet. The same is true for vlan 52. Conversely, vlans 1, 21 and 22 in are associated with separate subnets in each switchblock. Why? _____

_____

_____

_____

Use the charts on the last pages and this page to fill in the addresses you are going to configure on each of your devices. Remember that each router will be configured with four vlan interfaces (vlans 1,51,52 and either vlan 21 or 22). Each vlan interface will have an address on a different subnet:

Fill in this table if you have the **odd** devices (substitute your switch block# for "x"):

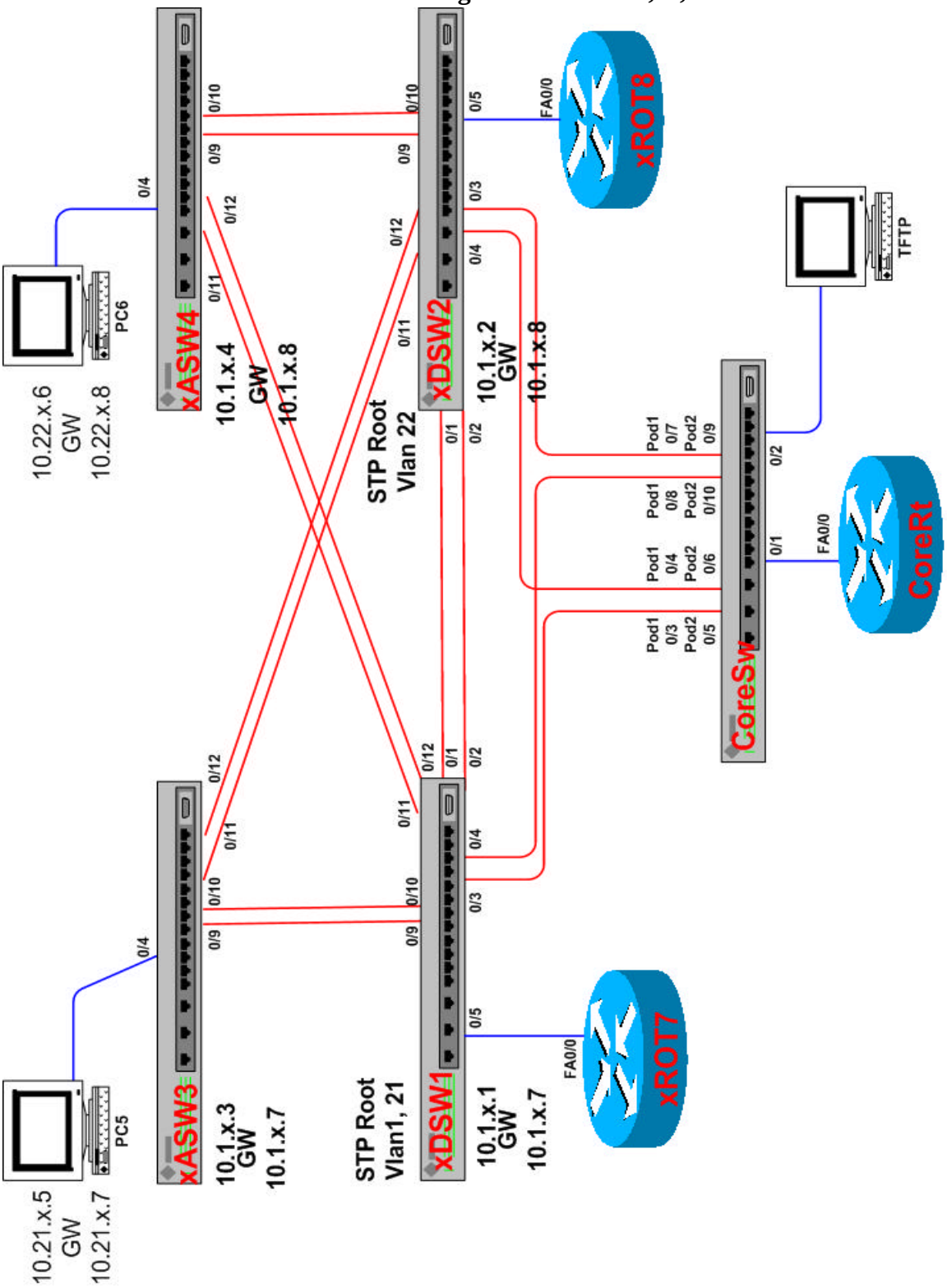
Device	Interface	Vlan Membership	IP Address	Mask	Configured Gateway or MAC Address
xPC5	f0/4 on xASW3	21	10.21.x.5	255.255.255.0	10.21.x.7 -router's address
xASW3	int vlan 1	1	10.1.x.3	255.255.255.0	10.1.x.7 -router's address
xDSW1	int sc0	1	10.1.x.1	255.255.255.0	10.1.x.7 -router's address
xROUTER7	int vlan 1	1	10.1.x.7	255.255.255.0	5000.0017.0001
xROUTER7	int vlan 21	21	10.21.x.7	255.255.255.0	5000.0017.0021
xROUTER7	int vlan 51	51	10.51.7.(SB# + 10)	255.255.255.0	5000.0051.00(SB# + 10)
xROUTER7	int vlan 52	52	10.52.7.(SB# + 10)	255.255.255.0	5000.0052.00(SB# + 10)

Fill in this table if you have the **even** devices (substitute your switch block# for "x"):

Device	Interface	Vlan Membership	IP Address	Mask	Configured Gateway or MAC Address
xPC6	f0/4 on xASW4	21	10.21.x.5	255.255.255.0	10.22.x.8 -router's address
xASW4	int vlan 1	1	10.1.x.3	255.255.255.0	10.1.x.8 -router's address
xDSW2	int sc0	1	10.1.x.1	255.255.255.0	10.1.x.8 -router's address
xROUTER8	int vlan 1	1	10.1.x.8	255.255.255.0	5000.0018.0001
xROUTER8	int vlan 21	21	10.21.x.8	255.255.255.0	5000.0018.0022
xROUTER8	int vlan 51	51	10.51.7.(SB# + 20)	255.255.255.0	5000.0051.00(SB# + 20)
xROUTER8	int vlan 52	52	10.52.7.(SB# + 20)	255.255.255.0	5000.0052.00(SB# + 20)

Visual Objective: You will be configuring your switchblock to look like this diagram.

The odd router's will be configured with vlan 1,21,51 and 52 interfaces
The even router's will be configured with vlan 1,22,51 and 52 interfaces



Step 2: Address your switches with vlan 1 addresses for management vlan 1:

On your ASW:

xASWy#**conf t**
xASW3(config)#**ip default-gateway 10.1.*{SB#}*.7 –** if you are **odd** or
xASW4(config)#**ip default-gateway 10.1.*{SB#}*.8 -** if you are **even**
xASWy(config)#**int vlan1**
xASWy(config-if)# **ip address 10.1.x.y 255.255.255.0** (use the IP address for your ASW)

On your DSW:

xDSWy#**conf t**
xDSW1(config)#**ip default-gateway 10.1.*{SB#}*.7 –** if you are **odd** or
xDSW2(config)#**ip default-gateway 10.1.*{SB#}*.8 -** if you are **even**
xDSWy(config)#**int vlan1**
xDSWy(config-if)# **ip address 10.1.x.y 255.255.255.0** (use the IP address for your DSW)

Step 3: Configure your pc with the appropriate ip address for vlan 21 if you're **odd**, or vlan 22 if you're **even**

Odd pc's ip address - 10.21.*{SB#}*.5 255.255.255.0
Odd pc's gateway – 10.21.*{SB#}*.7 This is your ROUTER's address on vlan 21

Even pc's ip address - 10.22.*{SB#}*.6 255.255.255.0
Even pc's gateway – 10.22.*{SB#}*.8 This is your ROUTER's address on vlan 22

Task 2: Vlan Configuration

Step 4: Place all switches in your switch block into a new vtp domain called Switchblock*{SB#}*- after the word Switchblock, just add your switch block number.

On your ASW:

xASWy# **vlan database**
xASWy(vlan)#**vtp domain Switchblock*{SB#}*** (remember to capitalize the "S")

On your DSW

xDSWy# **vlan database**
xDSWy(vlan)#**vtp domain Switchblock*{SB#}*** (remember to capitalize the "S")

Step 5: Because all four switches in your Switchblock are now in the same vtp domain and you are already trunking end-to-end from the prior lab, you are ready to create vlans and assign them to ports. It is only necessary for one switch to create the vlans because vtp will propagate anything that is created. Divide this job up with your partner.
On a DSW, create the vlans:

xDSWy(vlan)# **vlan 21 name vlan21**
xDSWy(vlan)# **vlan 22 name vlan22**
xDSWy(vlan)# **vlan 51 name vlan51**
xDSWy(vlan)# **vlan 52 name vlan52**

Step 6: Make DSW1 the root of vlans 1,21 and 51 and DSW2 the root of vlans 22 and 52.

xDSW1(config)# **spaningtree vlan 1 priority 8192** (repeat for 21 on DSW1only)
xDSW2(config)# **spaningtree vlan 22 priority 8192** (on DSW2 only)

Step 7: Then both DSW's need to re-enable ports f0/3 & f0/4 (they were disabled in a prior lab) and assign vlans 51 and 52 to the ports facing into the Core.

For **odd** DSW's, vlan 51 should be assigned to f0/3 (vlan 51 should be assigned to f0/4 for **even** DSW's) and vlan 52 should be assigned to f0/3 for **odd** DSW's (vlan 52 is assigned to f0/4 for even DSW's).

xDSWy(config)#**int f0/3** (for **both** odd and even DSWs)
xDSWy(config-if)#**no shut**
xDSWy(config-if)#**switchport access vlan 51** (vlan 52 for even DSW's)
xDSWy(config-if)#**int f0/4** (for **both** odd and even DSWs)
xDSWy(config-if)#**no shut**
xDSWy(config-if)#**switchport access vlan 52** (vlan 51 for even DSW's)
xDSWy(config-if)#**end**

Step 8: On your ASW, assign vlan 21, if you are odd (22 if you're even), to interface f0/4 so that the port your pc in is connected in the proper vlan.

xASWy#**configure terminal**
xASWy(config)#**interface f0/4**
xASWy(config-if)#**switchport access vlan 21** (or vlan 22 if you're an even ASW)

Task 3: Configure the router

Step 9: Open a console session to your router.

Step 10: Provide a base router configuration which will permit you to route between all vlans

Router>**en**
Router#**conf t**

Router(config)#**hostname *{SB#}*ROUTER7** (xROUTER8 in the even switches)

Router(config)#**no ip domain-lookup** (to stop the DNS lookup process on the router)

Router(config)#**enable pass san-fran**

Router(config)#**line con 0**

Router(config-line)#**logging synchronous**
Router(config-line)#**login**
Router(config-line)#**password cisco**
Repeat for the virtual terminal session (line vty 0 4)

Create a vlan 1 interface and assign it an ip address and a mac address:
xROUTER7(config-line)#**int vlan 1**

xROUTER7(config-if)#**ip address 10.1.*{SB#}*.7 255.255.255.0** (10.1.*{SB#}*.8 for even routers)
xROUTER7(config-if)#**mac-address 5000.0017.0001** (5000.00**18**.0001 for even routers)
xROUTER7(config-if)#**no shut**

xROUTER7(config-if)#**int vlan 21** (or 22 if you are the even router)

(repeat the steps listed above for each additional vlan (create the vlan interface, provide a mac address and provide an ip address for vlans 21 or 22, 51 and 52 in each ROUTER. Use the table from the beginning of the lab for the correct mac address and ip address for each interface)

Step 11: Enable a routing protocol

xROUTERy(config-if)#**exit**
xROUTERy(config)#**router ospf 1**
xROUTERy(config-router)#**network 10.1.x.0 0.0.0.255 area x**
xROUTERy(config-router)#**network 10.21.x.0 0.0.0.255 area x**
xROUTERy(config-router)#**network 10.22.x.0 0.0.0.255 area x**
xROUTERy(config-router)#**network 10.48.0.0 0.7.255.255 area 0**
xROUTERy(config-router)#**end**
xROUTERy#**copy run start**

Step 12: Double check your configuration for accuracy and test connectivity

xROUTERy#**show run**
xROUTERy#**show int**

Test your ip connectivity by pinging other locations in the room.
What path is a ping taking to get from your pc to another pc? _____

_____

Go to your ROUTER and do the following comands:

xROUTER7#**show ip route**
xROUTER7#**show ip route connect**

If we had not enabled a routing protocol would you have been able to communicate with devices in the other switch blocks? _____

_____

Great Job!!

Lab #7

Configuration of HSRP (Hot Stand-By Routing Protocol)

Objective:

In this lab, you will configure the HSRP (Hot Standby Routing Protocol) to add resiliency to your network. To accomplish this objective, you need to perform the following tasks:

1. Configure both routers in your switch block to have ip addresses on all three vlans.

2. Obtain the assigned HSRP ip address, HSRP priority and HSRP group ID.

3. Reconfigure the gateway of all ip hosts to point to the HSRP virtual address as the default gateway instead of the physical address that they are currently using.

4. Test the functionality of HSRP

Estimated Time: 45 minutes

In Lab 6 the following addresses were created (except for the bold ones):

VLAN	xROUTER7 (odd)	xROUTER8 (even)
1	10.1.SB#.7 / 24	10.1.SB#.8 / 24
21	10.21.SB#.7 / 24	**10.21.SB#.8** / 24
22	**10.22.SB#.7** / 24	10.22.SB#8 / 24

Step 1: Both routers need an address in each vlan. The two bold addresses need to be created on the appropriate router. You will do the following commands for the vlan interface you are missing, either vlan 21 or vlan 22.

xROUTER7(config)#**int vlan 22**
xROUTER7(config-if)#**ip address 10.22.*{SB#}*.7 255.255.255.0**
or
xROUTER8(config)#**int vlan 21**
xROUTER8(config-if)#**ip address 10.21.*{SB#}*.7 255.255.255.0**

Step 2: To configure HSRP, you need three pieces of information:

1. the HSRP ip address – this is the address of the "virtual router". It is the new gateway address that your pc, ASW and DSW will use in their respective vlans.

2. the HSRP priority for each router

3. the HSRP group ID

This information is supplied in the following table.

VLAN	group-id	ROUTER7 Priority	ROUTER8 Priority	HSRP ip- address
1	1	100	50	**10.1.{SB#}.10** /24
21	21	100	50	**10.21.{SB#}.10** /24
22	22	50	100	**10.22.{SB#}.10** /24

Step 3: Enter the following commands to enable HSRP on you router:

xROUTERy(config-if)# **standby** *{group-id}* **ip** *{hsrp-ip-address}*
xROUTERy(config-if)# **standby** *{group-id}* **priority** *{hsrp-priority}*

If you are the odd router do the following on the vlan 1 and vlan 21 interfaces and if you are the even router do this command on your vlan 22 interface:

xROUTERy(config-if)# **standby** *{group-id}* **preempt**

Step 4: Which router is the primary router for:

	Primary router
Vlan 1	_____
Vlan 21	_____
Vlan 22	_____

Step 4: Verify your configuration

xROUTERy# **show standby vlan** *{vlan#}*

Step 5: Replace the current gateways in your pc, DSW and ASW with the appropriate HSRP gateway ip address. Be certain to replace the gateway in all three devices with the **virtual router's ip address**. For the odd switches they need the vlan 1 virtual gateway address of 10.1.*{SB#}*.**10** and pc5 needs to have its current gateway removed and the virtual router's ip address in vlan 21, which is 10.21.{SB#}.**10**, added as its gateway. **Notice the vitual router addresses all end in 10**.

Step 6: Demonstrate HSRP fallover by having you and your partner start a continuous ping from your ms-dos prompt to your DSW's. You will now be sending data from vlan 21 to vlan 22.

Then reboot the odd router. To reboot a router **BE CERTAIN YOU HAVE SAVED THE ROUTER'S CONFIGURATION**. Do not use the **reload** command on the router, it will cause an immediate transition to the standby router, you must power cycle the router to simulate a true failure.

Did you miss any pings?_____

What happens when the odd router comes back up?_____

_____

Why? _____

_____

Once the routers are re-stabilized, repeat on the even router. Both should have had about the same results, if not, then there is something wrong.

Good Work!!

Lab #8

Configuring IP Multicast

Objective:

In this lab you will complete the following tasks: Configure the routers to forward multicast traffic using the PIM DM protocol on your assigned interfaces. Configure the routers to forward multicast traffic using the PIM SM protocol on your assigned interfaces. Verify the configuration. Enable CGMP on routers interfaces and the distribution switch. Verify operation of CGMP on both access and distribution switches.

1. Globally enable IP Multicast on your router.
2. Set up IP PIM Dense mode on your router
3. Verify using a multicast client on the PCs
4. Set up IP PIM Spares mode and verify operation
5. Set up CGMP on the switches

Estimated Time: 30 minutes

Task 1: Configuring the Primary Distribution Router to Forward Multicast Traffic Using the PIM DM Protocol

In this task, you enable multicast routing on the distribution router. You configure your specific VLAN interface with the PIM dense mode protocol and view the mroute information. There are two routers in each switch block.

Complete the following steps:

Step 1 Log in to your assigned router.

Step 2 In global configuration mode, enter the **ip multicast-routing** command.

Step 3 In privileged mode, enter the **show run** command to confirm that multicast routing is enabled. Your configuration should resemble the following output.

```
Building configuration...

Current configuration:
!
version 11.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname xROUTERy
!
enable password san-fran
!
ip multicast-routing
```

Step 4 In privileged mode, enter the **show ip mroute** command to display the multicast routing information. Your configuration should resemble the following output.

```
xROUTERy#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L -
Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit
set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD,
State/Mode

xROUTERy#
```

Step 5 In interface configuration mode, enter the **ip pim sparse-dense-mode** command to enable the PIM protocol on your VLAN51 interface.

Step 6 In privileged mode, enter the **show ip mroute** command to display the multicast routing information. Your configuration should resemble the following output.

```
xROUTERy#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L -
Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit
set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD,
State/Mode

(*, 224.2.210.17), 00:01:00/00:02:59, RP 0.0.0.0,
flags: DJ
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan51, Forward/Sparse-Dense, 00:00:50/00:00:00

(10.53.7.5/32, 224.2.210.17), 00:00:43/00:02:16,
flags: PT
  Incoming interface: Vlan51, RPF nbr 172.16.51.3
  Outgoing interface list: Null

(*, 224.2.182.213), 00:01:00/00:02:59, RP 0.0.0.0,
flags: DJ
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan51, Forward/Sparse-Dense, 00:00:51/00:00:00

(10.53.7.5/32, 224.2.182.213), 00:00:50/00:02:09,
flags: PT
  Incoming interface: Vlan51, RPF nbr 172.16.51.3
  Outgoing interface list: Null

 text deleted

(*, 224.0.1.40), 00:01:10/00:00:00, RP 0.0.0.0, flags:
DJCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan51, Forward/Sparse-Dense, 00:01:10/00:00:00
```

Step 7 Record the (*,224) addresses in the table below.

Multicast Group Address	Flags/Description

Step 8 In interface configuration mode, enter the **ip pim sparse-dense-mode** command to enable the PIM protocol on your VLAN52 interface.

Step 9 In privileged mode, enter the **show ip mroute** command to display the multicast routing information. Notice that VLAN52 has been added to the (*,g) entries. Your display should resemble the following output. This depends on other router in your block.

```
xROUTERy #show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L -
Local, P - Pruned
       R - RP-bit set, F - Register flag, T - SPT-bit
set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD,
State/Mode

(*, 224.2.210.17), 00:13:12/00:02:59, RP 0.0.0.0,
flags: DJ
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan52, Forward/Sparse-Dense, 00:00:24/00:00:00
    Vlan51, Forward/Sparse-Dense, 00:13:02/00:00:00

(10.53.7.5/32, 224.2.210.17), 00:00:39/00:02:42,
flags: PT
  Incoming interface: Vlan51, RPF nbr 10.51.7.7
  Outgoing interface list:
    Vlan52, Prune/Sparse-Dense, 00:00:25/00:02:42
```

```
(*, 224.2.182.213), 00:13:12/00:02:59, RP 0.0.0.0,
flags: DJ
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan52, Forward/Sparse-Dense, 00:00:25/00:00:00
    Vlan51, Forward/Sparse-Dense, 00:13:03/00:00:00

 text deleted
```

In interface configuration mode, enter the **ip pim sparse-dense-mode** command to enable the PIM protocol on the rest of your assigned VLAN interfaces. (VLAN 1, VLAN 21 and VLAN 22)

Step 10 In privileged mode, enter the **show run** command to display the current configuration and verify that *all* interfaces are either running PIM or are shut down.

Verifying From Your PC

Step 1 From your PC, Ping 10.53.7.5 to verify that you can reach the server

Step 2 You now need to get a copy of Freeamps, a freeware client software.
From a MS-DOS window:
FTP 10.53.7.5
Login is: TB
Password: cisco
get freeamps.exe
quit

Step 3 Now that you have Freeamps, launch it and let it load where it wants.

Step 4 Once completed, start Freeamps.

Step 5 Click on **Files**, on the URL line type:

rtp://x.x.x.x:port (where the x.x.x.x is the class D address the instructor will supply and the port is the UDP port number).

Step 6 Click on the **Open URL (NOT Open)**, then you should go back to the Freeamps window and it should start to buffer and there should be a "**RTP Stream"** statement in the window. If it has HTTP, then either you clicked Open, put HTTP rather than RTP or have the slashes in the wrong direction. If everything is work correctly, you should start hearing music. If you see that it is playing, but there is no sound, check to see if the speaker is muted.

Task 2: Configuring Multicast Traffic Using PIM SM

In this task, you configure the IP address of the rendezvous point on the distribution router. Verification of this task is made when your IPTV program is successfully launched and the **mroute** command display flags are set to sparse mode.

Step 1 From your PC, connect to your assigned router.

Step 2 In global configuration mode, enter the **ip pim rp-address** 10.51.7.7 command to designate the rendezvous point for your assigned router. The system should return the following message as soon as the **ip pim rp-address** command has successfully executed.

```
00:37:52: %AUTORP-5-MAPPING: RP for 224.0.1.39/32 is
now 10.51.7.7
00:37:52: %AUTORP-5-MAPPING: RP for 224.0.1.40/32 is
now 10.53.7.7
```

Step 3 In privileged mode, enter the **show run** command to verify your configuration. Your configuration should resemble the following output.

```
Building configuration...

Current configuration:
!
(text deleted)
ip multicast-routing
ip dvmrp route-limit 20000
mls rp ip
!!
no ip classless
ip pim rp-address 10.51.7.7
```

Step 4 In privileged mode, enter the **show ip mroute** command, locate the flags in the command output, and verify that the routers are routing packets in PIM Sparse Mode. Your display should resemble the following output. Output may vary depending on the number of multicast streams detected.

```
(*, 224.2.239.61), 00:37:29/00:02:59, RP 10.51.7.7,
flags: SJC
  Incoming interface: Vlan51, RPF nbr 10.53.7.7
  Outgoing interface list:
    Vlan12, Forward/Sparse-Dense, 00:15:09/00:01:57

(10.53.7.5/32, 224.2.239.61), 00:16:15/00:02:59,
flags: CT
  Incoming interface: Vlan51, RPF nbr 10.51.7.7
  Outgoing interface list:
    Vlan21, Forward/Sparse-Dense, 00:15:09/00:01:57
```

Step 5 In privileged EXEC mode, enter the **copy run start** command to save the configuration.

Step 6 Verify operation with Freeamps

Task 3: Enabling CGMP

Enabling CGMP on router Interfaces

Complete the following steps:

Step 1 Connect to your router.

Step 2 In interface configuration mode for your assigned VLAN, enter the **ip cgmp** command to enable processing of CGMP on the interface.

Step 3 In privileged EXEC mode, enter the **show ip igmp interface vlan num** command to display current settings. You are looking for the CGMP status. Your output should resemble the following.

xROUTERy#**sh ip igmp interface vlan 21**

```
Vlan21 is up, line protocol is up
  Internet address is 10.21.1.7/24
  IGMP is enabled on interface
  Current IGMP version is 2
  CGMP is enabled on interface
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Inbound IGMP access group is not set
  IGMP activity: 10 joins, 1 leaves
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 10.21.1.8
  IGMP querying router is 10.21.1.7 (this system)
  Multicast groups joined: 224.0.1.40
```

Step 4 Return to your PC.

Enabling CGMP on Distribution Switches

Complete the following steps:

Step 1 Connect to your distribution switch.

Step 2 In configuration mode, enter the **cgmp** command to enable CGMP on the distribution switch.

In privileged mode, enter the **show cgmp** command.

Step 3 Return to your PC.

Enabling CGMP on Your Access Switch

Complete the following steps:

Step 1 Telnet to your assigned access switch.

Step 2 In privileged EXEC mode, enter the **show cgmp** command. Your output should resemble the following. CGMP is enabled by default.

```
ASW21#sh cgmp
CGMP Status :   Enabled

CGMP Holdtime (secs) : 600
VLAN    Address              Destination
---------------------------------------
!
 text delete
```

Step 3 In global configuration mode, enter the **cgmp hold-time 300** command to lower the holdtime from 600 secs to 300 secs.

Good Work!!

Lab #9

Configuration Management and Access Control

Objective:

In this lab, configurations will be saved and restored. Password recovery will be performed. Privilege levels will also be enabled on the RSM to limit user control. Access control to your DSW and ASW will also be enabled. You will then wipe out the configurations in your ASW, router and DSW To accomplish this objective, you need to perform the following tasks:

1. Save the configurations of your router, DSW and ASW to a tftp server.

2. Establish privilege levels to limit control of your router.

3. Create and apply an access list to limit access to your ASW. Apply an ip permit statement to limit access to your DSW.

4. Delete your configuration files.

Estimated Time: 45 minutes

Task 1: Save your configuration files

Step 1: Verify connectivity to the tftp server from your ASW, DSW and router. (If the ping doesn't work ask your instructor for the correct TFTP server address)

ping 10.1.7.5

Step 2: Save the ASW configuration. Go to your ASW and send its running-config file to the tftp server. Our naming convention for configuration files is the name of your device.txt; i.e. **6ASW3.txt**

xASWy#**copy run tftp**
Address or name of remote host []? **10.53.7.5**
Destination filename [running-config]? **xASWy.txt**
!!
1094 bytes copied in 0.997 secs
xASWy#

Step 3: Save the DSW configuration. Go to your DSW and send its configuration file to the tftp server. Our naming convention for configuration files is the name of your device.txt; i.e. 6DSW1.cfg

xDSWy#**copy run tftp**
Address or name of remote host []? **10.53.7.5**
Destination filename [running-config]? **xDSWy.txt**
!!
1094 bytes copied in 0.997 secs
xDSWy#

Step 4: Save the ROUTER configuration. Go to your ROUTER and send its configuration file to the tftp server. Our naming convention for configuration files is the name of your device.txt; i.e. 6ROUTER7.txt

xROUTERy>**en**
xROUTERy#**copy run tftp**
Address or name of remote host []? **10.53.7.5**
Destination filename [running-config]?..<**cr**>

Task 2: Establish privilege levels to limit access to your router, ASW and DSW.

Step 5: Go to your router and create an account that will permit the account holder to perform a "show interfaces" and "show ip route", but nothing else. The name of this account will be "troublemaker".

xROUTERy(config)#**username administrator privilege 15** (do not forget this command!!)
xROUTERy(config)#**username troublemaker privilege 2**
xROUTERy(config)#**privilege exec level 2 show interfaces**
xROUTERy(config)#**privilege exec level 2 show ip route**
xROUTERy(config)# **privilege exec level 2 show**
xROUTERy(config)#**line con 0**
xROUTERy(config-line)#**login local**
xROUTERy(config-line)#**line vty 0 4**
xROUTERy(config-line)#**login local**
xROUTERy(config-line)#**end**
DO NOT DO A COPY RUN START or a WRITE MEM at this time

Step 6: To prevent troublemaker from doing the rest of the "show" commands from "exec level 2", enter the command:

xROUTERy(config)#**privilege exec level 1 show**

Step 7: Open a telnet session from your laptop to your router

User Access Verification

Username: **troublemaker**
Password: **<enter>**
xROUTERy#

You will get a privileged prompt even though you have not truly entered enable mode. This indicates that you have different privileges than an average user because they were specifically defined.

After you do a "**show interfaces**" and a "**show ip route**" try to look at the running-config or any other command. Then type:

xROUTERy#**login**

When prompted put in the name "**administrator**"
the password is just your <enter> key

Now do a "**show run**" or any other command. You are a level 15 user now.

Step 8: Remove the administrative level configuration from the router

xROUTERy#**conf t**
xROUTERy(config)#**no username troublemaker privilege 2**
xROUTERy(config)#**no privilege exec level 2 show interfaces**
xROUTERy(config)#**no privilege exec level 2 show ip route**
xROUTERy(config)# **no privilege exec level 1 show**
xROUTERy(config)#**line con 0**
xROUTERy(config-line)#**no login local**
xROUTERy(config-line)#**line vty 0 4**
xROUTERy(config-line)#**no login local**
xROUTERy(config-line)#**end**

Step 9: Create and apply an access list to limit access to your ASW. This access list will permit your own pc to telnet in, but nothing else (not even your DSW). You will also have to add a vty password so that you can telnet in.

xASWy#**conf t**
xASWy(config)#**access-list 1 permit 10.___.___.___** (insert the ip address of your pc)
xASWy(config)#**line vty 0 4**
xASWy(config)#**login**
xASWy(config)#**password cisco**
xASWy(config-line)#**access-class 1 in**
xASWy(config-line)#**end**
DO NOT DO A COPY RUN START or a WRITE MEM at this time

Step 10: Can you telnet into your ASW from your pc? _____

Can you telnet into your ASW from your DSW? _____

Task 3: Configuration wipe out

PLEASE TAKE THE TIME TO DO THIS AFTER BOTH PARTNERS HAVE COMPLETED TASK 2–THANK YOU!

Please do these steps in the order listed

Step 11: Wipe out the DSW configuration and vlan database.

xDSWy#**erase start**
xDSWy#**delete flash:vlan.dat** This command is necessary to remove any vtp domain name and vlans that were created and return your DSW to vlan factory defaults.

PLEASE….**DO NOT** enter the command "erase flash:" because this will erase everything from flash, including your entire operating system. If you then did a reload, your switch would not have its operating system.

Step 12: Wipe out the ASW configuration and vlan database.

xASWy#**erase start**
xASWy#**delete flash:vlan.dat**

Step 17: Go to your ROUTER and wipe out its configuration

xROUTERy#**erase start**
xROUTERy#**exit**

Thank you!