

# Comprehensive CCNA Switch Lab (Draft)

## Overview

This lab gives you an opportunity to practice the configuration of many CCNA-level LAN switch features. At the end of the lab, you will have a working switch configuration that can then be used to perform additional experiments with STP. If you perform all the steps in this lab, you will configure:

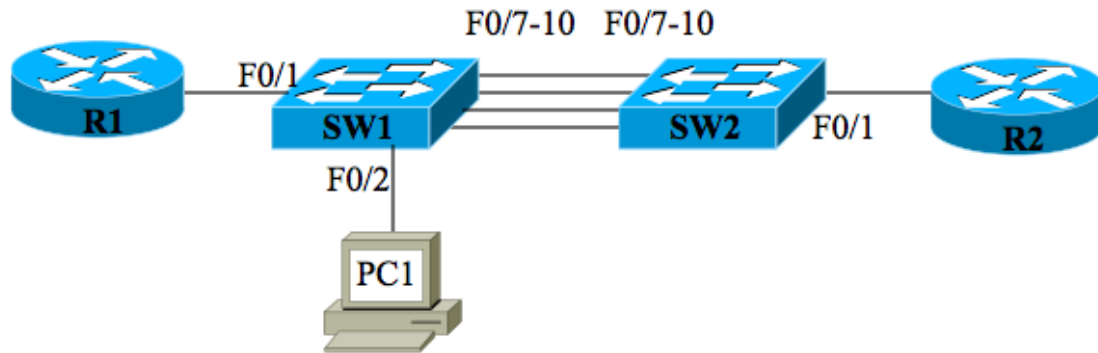
- Basic switch administrative settings
- Configure the switches for IP
- Port Security
- VTP
- VLANs
- VLAN trunking (switches and routers)
- Etherchannel

## Network World Blog

This lab document was built for use in conjunction with some blog discussions in early March 2010. To support the discussions in the post, you can ignore all the steps related to basic administration, configuring IP support on the switches, and for port security. The final four items must be configured before getting into the Spanning Tree Protocol (STP) discussions in those blog posts. ([www.nww.com/odom](http://www.nww.com/odom))

## Topology and Equipment

This lab assumes you have 2 LAN switches, 2 routers, and 1 PC. The lab assumes the following topology:



Switch requirements: Both switches must support 802.1Q trunking and Etherchannel. The configuration was/will be tested on a pair of 2950 switches.

Router requirements: Any routers, but with R2 supporting 802.1Q trunking.

PC: Any PC with an Ethernet NIC.

Other requirements: To match the lab solution and blog discussions, SW1 must have the lower base MAC address compared to SW2. Before cabling the two switches together, login to each switch. Use the **show spanning-tree** command, and find the bridge ID of each switch. Whichever has the lower number, use that switch as SW1. (If you forget, it's not a big deal, but some related spanning tree configurations assume SW1 has the lower MAC address.)

### CCNA Perspectives from Wendell

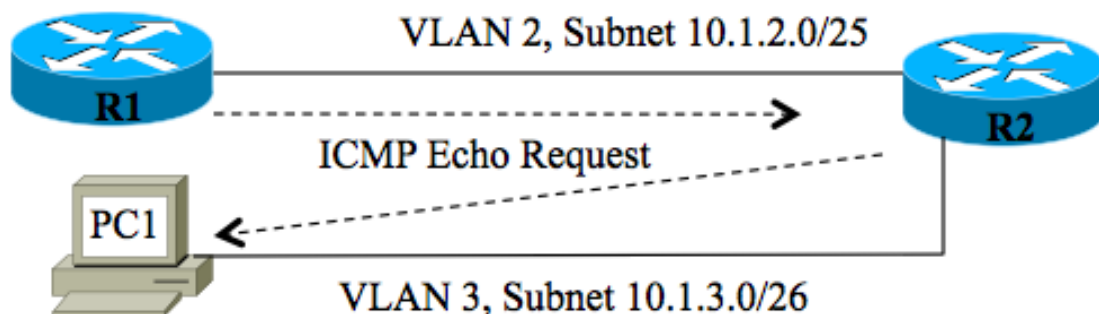
The configuration required for this lab touches on a large number of configuration commands. If you're someone studying for CCNA, you may not be able to configure everything without going back and reading, or looking at the solution (which isn't posted yet). So, treat this as a chance to learn, use the lab as you see fit. I just wanted to post it somewhere for anyone who wanted to use this for practice, and to have a backdrop from which to discuss STP in the blog.

## Lab Overview

In this lab, you will configure two LAN switches with a variety of features, and use two routers plus a PC to test by pinging. In this lab, you will configure the following:

1. Both switches to support VLANs 1, 2, and 3
2. IP connectivity to the switches to allow telnet into the switches from the routers
3. An Ethernet Channel (Etherchannel) using two links (F0/7-8) between switches
4. 802.1Q trunking on the Etherchannel, as well as on another single Ethernet link (F0/10) between switches
5. 802.1Q trunking between a switch and a router
6. Port security on the link between switch SW1 and router R1

By the end of this lab, you will be able to ping from router R1 to PC1, causing the packet to go from R1, through the two switches in VLAN2 to R2, with R2 forwarding the packet through VLAN 3 back to PC1.



## Lab Steps:

1. Begin with the two switches not cabled to any other devices.
2. Reset the switch configurations to factory default, including deleting all VLAN configuration and resetting both switches to VTP defaults (VTP server, null VTP domain name).
3. Determine which of the two switches has the lower default STP bridge ID, and use that switch as SW1 (to better match the solutions)
4. Reload the two switches.
5. Give each switch an IP address/mask in VLAN 1 (per the table below).
6. If you want to, configure any administrative settings for extra practice (hostnames, passwords, banners, etc).
7. Configure SW1 as VTP client, SW2 as VTP server, domain name "fred".

8. Configure portfast on the three ports connected to the routers and PC.
9. On the port connected to R1, configure port security, such that only R1's traffic is allowed into port F0/1 on the switch, and such that if a frame from another MAC is used, the port is not shutdown.
10. Configure each switch so that the pair of links on ports F0/7 and F0/8 form an Etherchannel.
11. Shutdown the F0/9 ports on each switch.
12. Configure the two switches so that both the Etherchannel and the F0/10 link both use 802.1Q trunking.
13. Create VLANs 2 and 3.
14. Configure the link from R2 to SW2 to use 802.1Q trunking, giving R2 an IP address in VLANs 1, 2, and 3 (see table)
15. Configure SW1 such that R1 is in VLAN2, and configure R1 with the IP address/mask in the table
16. Configure SW1 such that PC1 is in VLAN3, and give PC1 the IP address/mask and default gateway listed in the table.
17. Define on R1 a default route pointing to R2's VLAN2 IP address (so that pings from R1 to PC1 will work)
18. Complete any other tasks, including enabling interfaces, such that R1 can ping all three of R2's LAN IP addresses, and so that PC1 can ping those addresses as well.
19. Complete any other tasks required so that R1 can ping PC1, and vice versa.

Device	IP	mask	Default gateway	VLAN
SW1	10.1.1.1	/24	10.1.1.10 (R1)	1
SW2	10.1.1.2	/24	10.1.1.10 (R1)	1
PC1	10.1.3.1	/26	10.1.3.10	3
R1	10.1.2.1	/25	N/A	2
R2	10.1.1.10	/24	N/A	1
R2	10.1.2.10	/25	N/A	2
R2	10.1.3.10	/26	N/A	3