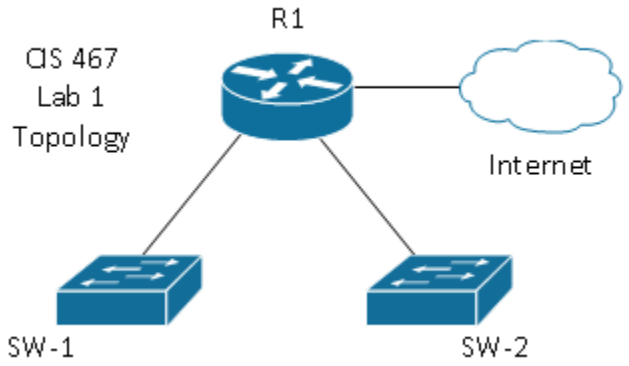
California State Polytechnic University – Pomona
CIS 467 Network Security
James Schneider

Using a Cisco router & two Cisco Switches (Layer 2) with IOS software or Simulation software such as GNS-3, or Cisco's Packet Tracer, perform the below outlined tasks. You may use reference materials obtained from Cisco Systems website, books from Ciscopress, or material obtained from 3rd party training institutions. You may not, however, obtain assistance from any student, colleague, or outside professional other than your instructor.

Once you have completed the lab, submit either the PacketTracer file or the exported configurations from each device. If submitting configuration files, please check them for content, and be sure to perform a 'write' on the device before exporting.

Lab Topology:



Lab Tasks:

1. Boot your systems and console into them. Ensure that the software boot and perform a password recovery if needed.
2. Give your Router the Hostname R1. Give one switch the hostname SW-1 and the other SW-2.
3. Setup the following users with the appropriate privilege level and passwords on all devices.
    a. Username Admin – Password cisco – Privilege Level 1
    b. Username Root – Password root – Privilege Level 15
    c. Username Guest – Password changeme –Privilege Level 1
4. On R1, Give the Link to SW-1 the IP address 192.168.20.1/24, On a different interface, give it the IP address 204.186.29.1/29 and link it to SW-2
5. Setup VLAN 10 on SW-1and give the VLAN 10 interface IP address 192.168.20.254/24, On SW-2, setup VLAN 20 and give theVLAN 20 interface an IP of 204.186.29.2/29
6. On R1, Set a static default route to 204.186.29.3
7. Setup DHCP on your router (R1)to support the 192.168.20.0/24 network with the following:
    a. Addresses .1 - .25 are Excluded from the scope
    b. Useable addresses are .26-.253
    c. Address .254 is Excluded from the scope
    d. DNS Server will be 192.168.20.16
8. Setup a standard access list on R1 to deny any IP traffic from the 117.23.54.0/24 network inbound from the public interface / internet.
9. Setup your router, and switches to use SSH on your VTY lines and authenticate with your local users you set up in step 3. Make sure you test this!
10. On ALL devices, lock out your Aux port, disable your http engine, set a password of cisco123 on your console port and finally disable Cisco Discovery Protocol system wide.