CCNA Lab Recommendations

Prepared By: Jeremy Archer

Version 0.1 <Draft>
Notable Items Missing:
Labs on WLANs, SDM, VPNs
Recommended Topologies

The following list was compiled for my personal use. It may not accurately represent CCNA exam topics. This document is not intended to teach you how to do anything. Its purpose is to provide a list of the things that you should already know how to do.

Important Notes:

- These lab recommendations have been prepared with no specific IP addressing requirements or recommendations. Determining the best IP address plan should be a consideration for each lab.
- Debugging is highly encouraged throughout these labs. If you're unfamiliar with the debugging tools / commands use IOS help or consult other resources.
- The labs assume you understand these features and technologies. No attempts are made to explain their purpose or steps necessary to configure them.
- Many labs can be done together (e.g. frame-relay configuration along with OSPF). Look for these types of labs and combine them so as to limit the amount of time dedicated to initial switch/router configuration, cabling, etc.
- Recommended topologies will be added in a future version.

1. Basic Router / Switch Configuration

Complete these labs prior to starting the "Switch" or "Routing" sections.

a. Configure hostname
b. Compare start-up and running configurations ("show running-config" vs. "show start-config")
c. View the contents of the flash.
d. View 'show version' information and note important output sections.
e. Configure password encryption
f. Configure the enable password and enable secret password.
g. Configure SSH and Telnet Access w/ passwords and with local username/password access.
h. Configure ACLs for remote telnet/ssh access
i. Configure Console access password
j. Upgrade/downgrade IOS image
k. Copy IOS image and start-config to/from TFTP Server
l. Configure config-register and observe boot behavior
m. Configure boot system variable
n. Walk through router setup mode.

o. Enable / Disable 'ip subnet-zero' and observe behavior by setting adding an interface to an "zero subnet" address.
p. Test behavior difference between "ip classless" and "no ip classless".
q. Configure local usernames and passwords.
r. Set up terminal history and view history
s. Suspend, resume and view ssh/telnet session information.
t. Identify configuration modes (global, int, router, etc)
u. Save configuration changes (copy run start)
v. Erase the start-config
w. Reload the switch/router and observe the boot process.
x. Document and troubleshoot network topology issues with CDP.
y. Set up interface descriptions
z. Create a login, exec and motd banner.
aa. Enable logging timestamps ('service timestamps')
bb. Create a local DHCP server on the router or switch and view DHCP leases.

2. Switching

a. Interface parameters and basic Switch Operation

Prior to these labs, complete the "Basic Router / Switch Configuration" lab.

i. Set interface description
ii. Set interface speed and duplex
iii. View CDP neighbors through interface (provided connected host supports CDP)
iv. View MAC address-table for interface to determine MAC address of connected host.
v. Set up management VLAN with VLAN interface and assigned IP Address.
vi. Set a default-gateway.
vii. Observe the LEDs on the front of the switch and their behavior.

viii. Display the contents of the MAC address-table.
ix. Set the switch's default gateway.

b. VLANs

i. Create multiple VLANs on L2 (or L3) switch and set their names.
ii. Add switch ports (access ports) to VLANs
    1. Practice with the 'int range xxx xxx' command.
iii. Create dot1q trunk ports between multiple switches
    1. Using both 'switch mode trunk' and dynamic desirable and dynamic auto.
    2. Set up allowed VLAN trunks.
iv. Set up VTP
    1. Add switches in server, client and transparent mode.
    2. Configure VTP parameters including domain, password and VTP pruning.
    3. Set the VTP version number
    4. Create and delete VLANs and confirm changes on other VTP participants.
    5. Manage the vlans.dat file
    6. Examine 'show vtp status' output
v. Create VLAN interfaces and confirm connectivity to those interfaces via client ping on associated VLAN interface.
vi. Establish L3 interVLAN routing on L3 switch.
    1. Add hosts to access vlan ports on different IP subnets w/ L3 switch as default GW. Ping between hosts to confirm interVLAN routing.

c. EtherChannel

i. Create EtherChannel port group between switches
    1. Add and remove interfaces to/from port-channel\

2. Combine this lab with the STP lab and observe the cost for an EtherChannel trunk.
3. Unplug one cable of the EtherChannel trunk and observe switch behavior.

d. Spanning Tree

The following lab is best configured with 3 switches, each connected to the other two (Switch1 connected to Switch2 and Switch3. Switch2 connected to Switch1 and Switch3, etc). In this way, it is easy to see the STP port states and alter the behavior of STP.

Also, be sure to use 'debug spanning-tree events'

i. Configure a root bridge
    1. By setting VLAN id root primary and root secondary
    2. By altering VLAN id priority value
ii. Disconnect a forwarding port and observe the behavior of a port as it moves through the STP port states.
iii. Configure host ports for STP portfast
iv. Configure BPDU guard for some interfaces and see the results (esp. when connected to another STP-enabled switch).
v. Set up Per VLAN Spanning-Tree load balancing between trunk ports.
vi. Alter interface cost to manipulate STP port selection.
vii. Alter the STP type (RSTP vs. 802.1d) and observe the differences in "show spanning-tree vlan x' and the port states as interfaces come up/down.

e. Port Security

i. Set up static MAC address port security
ii. Set up dynamic MAC address security
iii. Set up 'sticky' MAC address security
iv. Set up port-security violation policy.
v. Best practices for port security
    1. Create black hole VLAN (e.g. VLAN 666)

2. Add unused ports to black hole VLAN
3. Shutdown unused ports
4. Set unused ports to 'switchport access vlan 666'

3. WANs

This is also a good section to practice your VLSM.

a. Point to Point Serial Connections

i. Serial point to point connections using PPP and HDLC
    1. Configure HDLC between two routers
        a. Adjust clock rate and bandwidth
    2. Configure PPP between two routers
        a. Set up PPP CHAP and PAP authentication
        b. Adjust clock rate and bandwidth

b. Frame-Relay Connections

i. Create fully meshed frame relay network with a single interface and single IP subnet with any DLCI configuration (rely on Inverse ARP and LMI) for the virtual circuits.
ii. Using the same topology, use frame relay maps to map IP addresses and DLCI (disable Inverse ARP).
iii. Using the same topology, use an interface DLCI to establish the PVC.
iv. Practice changing the LMI type on all frame-relay connected routers.
v. Practice the same configurations (items above) with Serial point-to-point sub-interfaces.
vi. Configure multipoint sub-interface and reconfigure the network accordingly.
vii. Configure frame relay network between 3 locations using multipoint sub-interface

4. Routing

If you built a frame-relay network prior to this lab, that network will most likely work well for the routing labs. During these labs, repeatedly use the 'show ip route', 'show ip route <*routing protocol*>', and 'show ip protocols' commands to view the results of your work. I also recommend using a local loopback interface during your labs. This will allow you to see IP routing in action as the loopback networks begin appearing (and disappearing!) in your route table.
This is also a good section to practice your VLSM.

a. Connected networks

i. Configure IP addresses on the router and observe the output of "show ip route"

b. Static Routing

i. Create default route using both next-hop and interface variables.
ii. Create static route for one non-connected subnet.
iii. Create weighted static route (sometimes called floating static route).

c. RIP

i. Enable RIP
ii. Set RIP version
iii. Add networks to RIP
iv. Set up at least one interface as passive.
v. Configure manual IP route summarization
vi. Practicing debugging RIP with 'debug ip rip'

d. EIGRP

i. Enable EIGRP on the router and select AS number.
ii. Add networks to EIGRP configuration
iii. Configure manual IP route summarization
iv. Set the 'ip hello-interval eigrp' and 'ip hold-time eigrp *asn time*' interface commands if necessary.
v. Confirm interface bandwidth is set properly (you can practice altering this during the lab to view potential route changes). This is not a recommended practice!
vi. Alter the **delay** value of an interface and observe the metric change in the ip routing table.

vii. Practice interpreting the output of 'show ip eigrp topology' and 'show ip eigrp topology all-links'.
viii. Configure EIGRP authentication between two routers.
ix.

e. OSPF

i. Throughout the lab, observe the output of 'show ip ospf neighbor', 'show ip database' and 'show ip route'.
ii. Configure OSFP on a point-to-point link (serial PPP) and a broadcast network (e.g. Ethernet). Observe the differences between the two with regards to the DR and BDR.
iii. Configure each router's router-id.
iv. Configure each OSPF process with the appropriate 'network' statements
v. 'show ip ospf interface *interface-name* to view the hello and dead timers for each connected interface.
vi. Adjust the hello and dead time intervals.
vii. Practice configuring OSFP with routers in two separate areas (loopback interfaces will work well for this).
viii. Configure OSFP with two equal cost path. Obverse OSFP load balancing behavior and confirm both routes exist in the 'show ip route' output.

5. ACLs

This lab is best done with two hosts connected (or more) to two different interfaces on a route. Apply the ACLs to the router. Also, loopback addresses can help here for adding additional "hosts" on the other side of the router.

a. Standard Access Lists (numbered)
   i. Create *standard* ACL (with a number) and identified source address and add a few lines to the ACL, including a remark.
   ii. Apply the ACL to an interface and test your results.
   iii. Practice altering the ACL by adding / removing lines, testing the results each time.
   iv.
b. Standard Access Lists (named)

i. Create *standard* ACL (with a name) and identified source address and add a few lines to the ACL, including a remark.
ii. Apply the ACL to an interface and test your results.
iii. Practice altering the ACL by adding / removing lines, testing the results each time.
iv.

c. Extended Access Lists (numbered)
    i. Create *an extended* ACL (with a number) and identified source, protocol type and destination port and address and add a few lines to the ACL, including a remark.
    ii. Apply the ACL to an interface and test your results.
    iii. Practice altering the ACL by adding / removing lines, testing the results each time.
d. Extended Access Lists (named)
    i. Create *an extended* ACL (with a name) and identified source, protocol type and destination port and address and add a few lines to the ACL, including a remark.
    ii. Apply the ACL to an interface and test your results.
    iii. Practice altering the ACL by adding / removing lines, testing the results each time.
e. Reflexive Access List (optional)

6. NAT

a. Static NAT
    i. Translate inside host to public IP address.
b. Dynamic NAT w/ pool and ACLs
    i. Translate inside hosts to pool of public IP addresses dynamically using an ACL to identify inside hosts and a pool to identify public IP addresses
c. Dynamic NAT w/ interface, ACLs and Overload (PAT)

i. Translate inside hosts to public interface address using overloading (PAT)

7. IPv6

a. Enable IPv6 Routing ('*ipv6 unicast-routing*')
b. Enable IPv6 cef
c. Assign an IPv6 address to an interface using EUI-64 and without.
d. Configure simple network (two routers connected with a Ethernet connection, each with an IPv6 loopback address) and test ping and simple static routes and 'ipv6 router rip' configuration.