**Part A. Design your own network**

☐ 1. Draw your network using a network diagramming tool such as draw.io, LucidCharts, or MS Visio.

At a minimum, your network should include:  
  X a. 2 private routers  
  X b. 1 internet service provider router  
  X c. Follow one of the following hierarchical designs  
       X - 3 Tier  
        - 2 Tier  
        - Spine/ Leaf

  X d. At least 1 host device on every network (subnet)

**Part B. Configure your network in Packet Tracer**

X 1. Create your network's physical topology in Packet Tracer  
☐ 2. Configure devices to the best of your ability so that your network is logically represented as accurately as possible (\*\*If a device from your Network Diagram is preventing your ability to meet the "Configuration minimum requirements," just leave that device out of the Packet Tracer simulation.)

Configuration minimum requirements:

Layer 2 Switches:  
Basic Configuration:

☐ 1)     Prevent the router from attempting to resolve incorrectly entered commands as domain names  
☐ 2)     Switch name  
☐ 3)     Encrypted privileged EXEC secret password  
☐ 4)     Console access password  
☐ 5)     Set the minimum password length to 10 characters  
☐ 6)     Encrypt the clear text passwords  
☐ 7)     Configure an appropriate MOTD Banner

Private Routers:  
Basic Configuration:

☐ 1)     Prevent the router from attempting to resolve incorrectly entered commands as domain names  
☐ 2)     Router name  
☐ 3)     Encrypted privileged EXEC secret password  
☐ 4)     Console access password  
☐ 5)     Set the minimum password length to 10 characters  
☐ 6)     Encrypt the clear text passwords  
☐ 7)     Configure an appropriate MOTD Banner  
☐ 8)     Configure SSH.  
 ☐ - Domain name: cisco.com  
             ☐ - Create an administrative user in the local database:  
             ☐ - Username: cisco  
             ☐ - Secret Password: cisco123  
             ☐ - Set login on VTY lines to use the local database  
             ☐ - Set VTY lines to accept SSH connections only  
             ☐ - Use an RSA crypto key with a 1024 bits modulus  
             ☐ - Enable SSH using version 2

OSPF Configuration:

☐ 1)     Configure the OSPF routing process: Use process id 1.  
☐ 2)     Manually configure the router ids  
☐ 3)     Configure network statements for the appropriate networks (use any method you want).  
☐ 4)     Configure the appropriate interfaces to not forward OSPF updates where they are not required.  
☐ 5)     Configure the reference bandwidth: Adjust the reference bandwidth to 1 Gigabit.  
☐ 6)     Configure the hello time for 30 seconds.

NAT Configuration:

☐ 1)      Configure dynamic NAT between at least one of your private routers and the internet router      
 - Use IP range 209.165.202.140 - 209.165.202.150 as your NAT pool

ACL Configuration:  
☐ 1)      Create a standard ACL to allow only one PC to access the VTY lines of your private routers   
☐ 2)      Create an extended ACL to deny all SSH and FTP connections from the internet - All other traffic from the internet should be permitted