1. Access Ports  
   1.1. Configure VLAN 10 on SW1’s link to R10.  
   1.2. Configure VLAN 11 on SW1’s link to R11.  
   1.3. Configure VLAN 12 on SW1’s link to R12.  
   1.4. Using Rapid Spanning Tree, these ports should immediately transition from disabled to forwarding when enabled.  
   1.5. Once complete you should be able to ping SW1’s SVI interfaces 165.1.X.21/24, where X is the VLAN number.
2. Trunk Ports  
   2.1. Configure 802.1q Trunk Ports between SW2, SW3, SW4, and SW5.  
   2.2. Only allow VLANs 30 & 40 on the ports between these switches.
3. VTP  
   3.1. Configure VTPv3 between SW2, SW3, SW4, and SW5, and create VLANs 13, 30, and 40.  
   3.2. SW5 should be the master server and all other switches should be configured as clients.
4. Access Ports  
   4.1. Configure SW2's link to R13 as an access port in VLAN 13.  
   4.2. This port should not be subject to STP convergence.
5. EtherChannel  
   5.1. Configure a Port-Channel between SW2 and SW5 using open standards negotiation.  
   5.2. Traffic should be load balanced based on layer 4 header information.
6. SVIs  
   6.1. Configure SVIs on SW2, SW3, SW4, and SW5 for VLANs 10 and 20 with IP addressing 165.1.10.X/24 and 165.1.20.X/24 where X is 22 for SW2, 23 for SW3, 24 for SW4, and 25 for SW5.
7. STP Root Bridge Placement  
   7.1. Configure SW4 as the STP root bridge for VLAN 30, and the backup root for VLAN 40.  
   7.2. Configure SW3 as the STP root bridge for VLAN 40, and the backup root for VLAN 30.
8. STP Path Selection  
   9.1. Modify the network so that traffic from SW5 to the VLAN 30 & 40 root bridges first transits through SW2.
9. First Hop Redundancy  
   10.1. Configure HSRP between SW3 and SW4 for VLAN 30 with a Virtual IP address of 165.1.30.254. SW3 should be the primary gateway, but if its uplinks to SW2 go down, SW4 should take over the active status.  
   10.2. Configure VRRP between SW3 and SW4 for VLAN 40 with a Virtual IP address of 165.1.40.254. SW4 should be the primary gateway, but if its uplinks to SW2 go down, SW3 should take over the active status.
10. STP Protection  
    11.1. Configure SW1 so that if any of the devices on its attached access ports begin running Spanning-Tree Protocol, the ports are disabled for 5 minutes.
11. STP Root Protection  
    12.1. Configure SW3 and SW4 so that if SW5 begins to announce itself as the root bridge, the links to this device are disabled.
12. Multiple Spanning-Tree Protocol  
    13.1. Transition SW2, SW3, SW4, and SW5 to Multiple Spanning-Tree Protocol.  
    13.2. VLAN 30 should be in STP Instance 1.  
    13.3. VLAN 40 should be in STP Instance 2.  
    13.4. All other VLANs should be in the default instance.  
    13.5. Ensure to maintain the Root Bridge placement and the traffic engineering defined in the previous sections.  
    13.6. The MST information should be advertised through VTPv3 from SW5 to the VTP clients.
13. Router-on-a-Stick  
    14.1. Create VLANs 79 and 89 on SW6.  
    14.2. The link to R7 should be an access port in VLAN 79, and should not be subject to STP convergence.  
    14.3. The link to R8 should be an access port in VLAN 89, and should not be subject to STP convergence.  
    14.4. Trunk VLANs 79 and 89 from SW6 to R9, but do not allow them to be subject to STP convergence.  
    14.5. Once complete you should have connectivity within VLANs 79 and 89 between R7, R8, R9 and SW6.