Layer 2 Network Design Lab

Introduction

The purpose of these exercises is to build intra-building Layer 2 networks utilizing the concepts explained in today's design presentations. The exercises are focused on the 2nd layer of the OSI model, that is, switching. Students will see how star topology, aggregation, Virtual LANs, Spanning Tree Protocol, Port bundling and some switch security features are put to work.

There will be 5 groups of 6 students, with 4 switches per group. The distribution of IP address space for the building (Layer 2) networks will be as follows:

- Group 1: 10.10.64.0/24
- Group 2: 10.20.64.0/24
- Group 3: 10.30.64.0/24
- Group 4: 10.40.64.0/24
- Group 5: 10.50.64.0/24

Brief introduction to switch configuration

See Appendix A

Exercises

1. The first goal is to build a hierarchical switched network, so you will use one switch as your aggregation (or backbone) switch, and connect two access switches to it. Follow these instructions to configure each switch:

    1. The initial configuration for the backbone and edge switches can be found in Appendix B.
    2. Notice the lines with IP addresses and replace the “X” with the corresponding octet from your group’s IP prefix. Don’t forget to assign each switch a different IP address:
        1. Aggregation switch: 10.X0.64.4
        2. Access switch 1: 10.X0.64.6
        3. Access switch 2: 10.X0.64.7
    3. Connect port 24 of each access switch to ports 19 and 20 on the aggregation switch
    4. Configure IP addresses in you laptops and connect them to the access switches.
    5. Verify connectivity by pinging each laptop and switch. You should also be able to ssh to each switch as ‘admin’.

2. Take one patch cord and connect each end to two of the edge switches. What happens?
    1. Using your connection to the switch console, monitor the logs and watch the switch LEDs. Test connectivity from two edge machines using Ping.

3. We will now configure the **Spanning Tree Protocol** across all our switches.
    1. Use the configuration files in Appendix C.
    2. What is the main difference between the configurations of the backbone switch and the edge switches?
    3. Verify port roles and status
    4. Repeat the procedures in item 2. What happens now?
    5. Remove the loop
    6. Connect a computer to one of the edge ports. How long does it take to become active?
        1. Change the Spanning Tree Protocol version to RSTP on all switches
        2. Repeat the same test. How long does it take now?

4. What happens to the network if the aggregation switch dies? Let's now add **redundancy**.
    1. Add a second aggregation switch.
    2. Use the address 10.X0.64.5.
    3. Configure Spanning Tree with a priority of "2" on the second aggregation switch
    4. Connect port 23 from each edge switch to ports 19 and 20 on the second aggregation switch.
    5. Connect the aggregation switches to each other on port 24.
    6. Verify who is the root
    7. Verify port roles and status. Which ports are blocking?
    8. Turn off the first aggregation switch.
    9. Who is the root now? Verify port roles and status. Verify connectivity.
    10. Bring back the first aggregation switch
    11. Disable spanning tree in one of the aggregation switches. What happens?

5. We now want to protect the control plane of our switched network by separating the user traffic from the management traffic.
        1. Use the configurations in Appendix D to create a **management VLAN**.
        2. Remove the IP addresses from VLAN 1
        3. Verify connectivity between switches using the console connections
    2. From the laptops, try pinging any of the switches

6. We now want more capacity and link redundancy between the aggregation switches
    1. Use Appendix E to configure **Port Bundling**.
    2. What capacity do you have now?
    3. Remove one of the links in the bundle. What happens?

7. Suppose you wanted to load balance the traffic from the two VLANs across both aggregation switches. How can you achieve this?
    1. Configure MSTP using Appendix F.
    2. Verify status of each spanning tree instance. Notice the differences in port roles and status on the different instances.

8. If available, configure a computer as a DHCP server and connect it into one of the edge ports. Connect a second computer to another switch and check if you can get an IP address assigned. What happens if your users do this without your consent?
    1. Use the instructions in Appendix G to configure Rogue **DHCP prevention**.
        1. Can the client computer get an address now?
        2. Follow the rest of the instructions to make it work with a legitimate DHCP server.