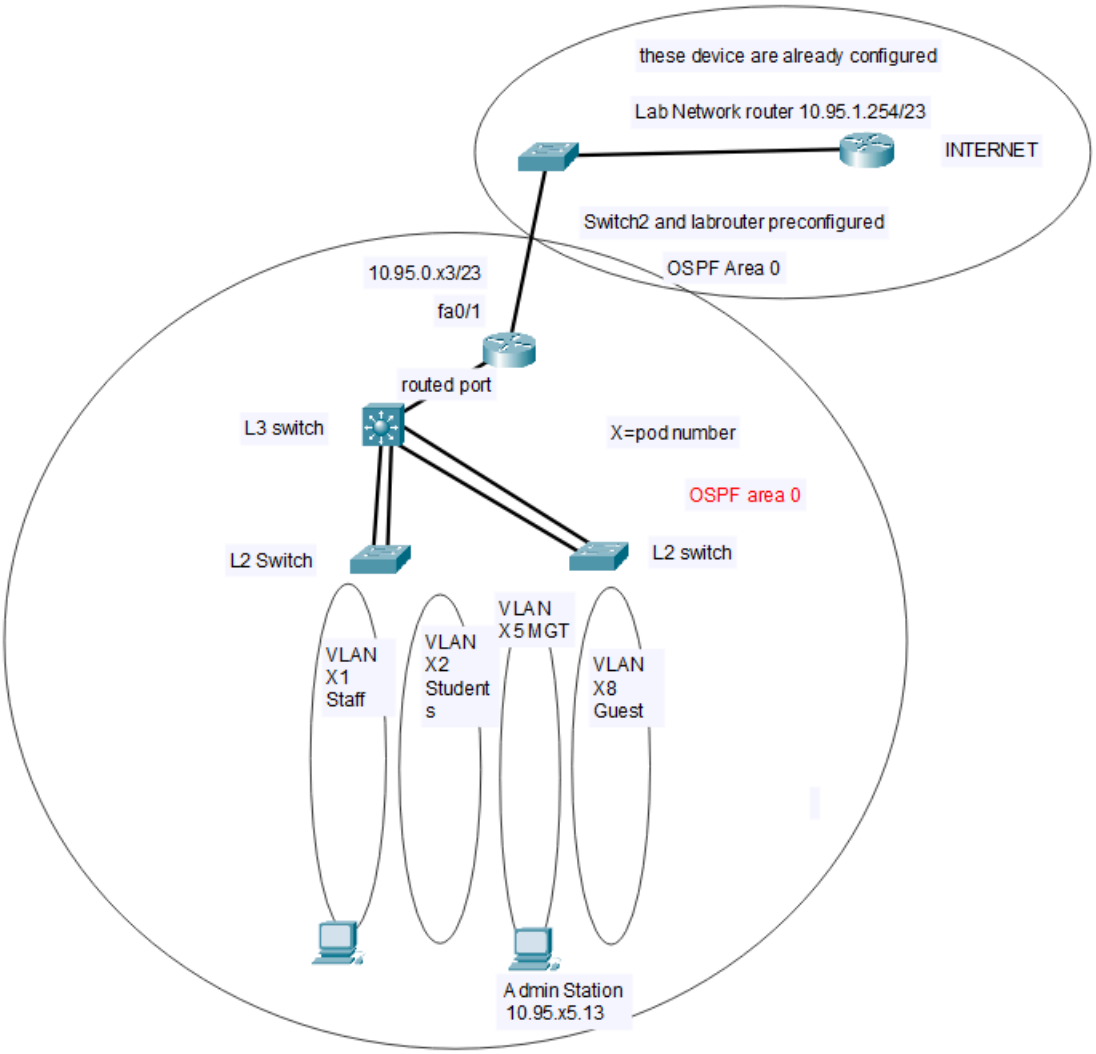
CCNA3 Case Study v.1.07 Spring 2025
Group work with a maximum of three students.

Design and configure network for Acme Ltd. Use real equipment on Lab KMD658. Switch2 and labrouter are preconfigured. Connection to Labnetwork is through RJ45 connectors named Labnetwork 10.95.0.0/23).



Each group has own IP address range available according to the pod number. For example pod 7 has IP addresses 10.95.70.0 -10.95.79.255 available plus the IP for connection to Labnetwork 10.95.0.71/23.

1. Use Per VLAN Spanning tree plus as Spanning Tree protocol
2. Routing protocol used in this Case Study is single area OSPF. You should receive default route and other routes to access Labnetwork and Internet from Labrouter.
3. Configure parallel Ethernet links as Etherchannels
4. Configure all used device connected ports as access ports with port security enabled and configure as spanning tree edge ports. Maximum number of MAC addresses per access port is 2 to allow a Bridged Virtual machine. Portsecurity violation should cause the port to shutdown state.
5. Ports fa0/1-5 should be configured for VLAN X1, Ports fa0/6-10 for VLAN X2, Ports fa0/11-12 for VLAN X8 and Port 13 for VLAN X5 on both AS switches.

6. There are following types of users (Staff, Students, Management and Guest) that need to be connected to separate VLANS. Prepare to have at least 300 users in Students VLAN. For VLANs you can use following IP address range 10.95.X[0-9].0 where X is the POD number (1-14). For example for pod 3 You can use the networks from 10.95.30.0 /24 -10.95.39.0/24.
7. In every VLAN there has to be a DHCP server. Reserve 31 IP-addresses in each VLAN for devices with static IP addresses

8. Configure NTP to synchronize clocks between Switches and end devices and configure also correct time zones (EET) and also summertime transition rules (EEST). Configure two NTP servers: 10.94.1.3 and 10.94.4.254)
9. All access-ports must be configured with portfast and BPDU-guard and port security with only two mac addresses allowed per port.
10. Configure all switches to support SSH version 2 and disable telnet to them. For login authentication on switches configure all switches to use local database (database must have a user cisco with password class configured for privilege level 1 access and a second user admin with password ciscoeigrp for privilege level 15 access).
11. Limit remote management connections only from devices in MGT VLAN
12. When everything is working configure an access-list on RX that only allows HTTP, HTTPS, DNS, SSH and ICMP traffic out. To the inside direction only return traffic for previously mentioned protocols is allowed.

Test your implementation of case study and write a comprehensive report where you explain how the requirements were configured to devices (what command were used and their possible limitations) and also explain how and what test were performed and any shortcomings found during testing**. Include all configurations from all network devices as appendix to your report**. Include also a network diagram with IP addresses clearly visible in it. Answer questions presented at the end of this case study.

If You are uncertain about requirements of this Case Study or if you get stuck in some problems when implementing, don't hesitate to contact me for advice: tel +358 50 3535 975 or email: marko.uusitalo@metropolia.fi.

When you answer following questions, include the relevant IoS command with output of it:

1. How many links will DS1 see in spanning-tree?
2. What is the router ID of labrouter?
3. How many OSPF routes did the Rx receive?
4. How many OSPF neighbors did Rx have?
5. Where there any requirements in this Case Study that you were unable to fulfill?
6. How you could improve security and performance of the network in your implementation of case study
7. How much time did this Case Study take?