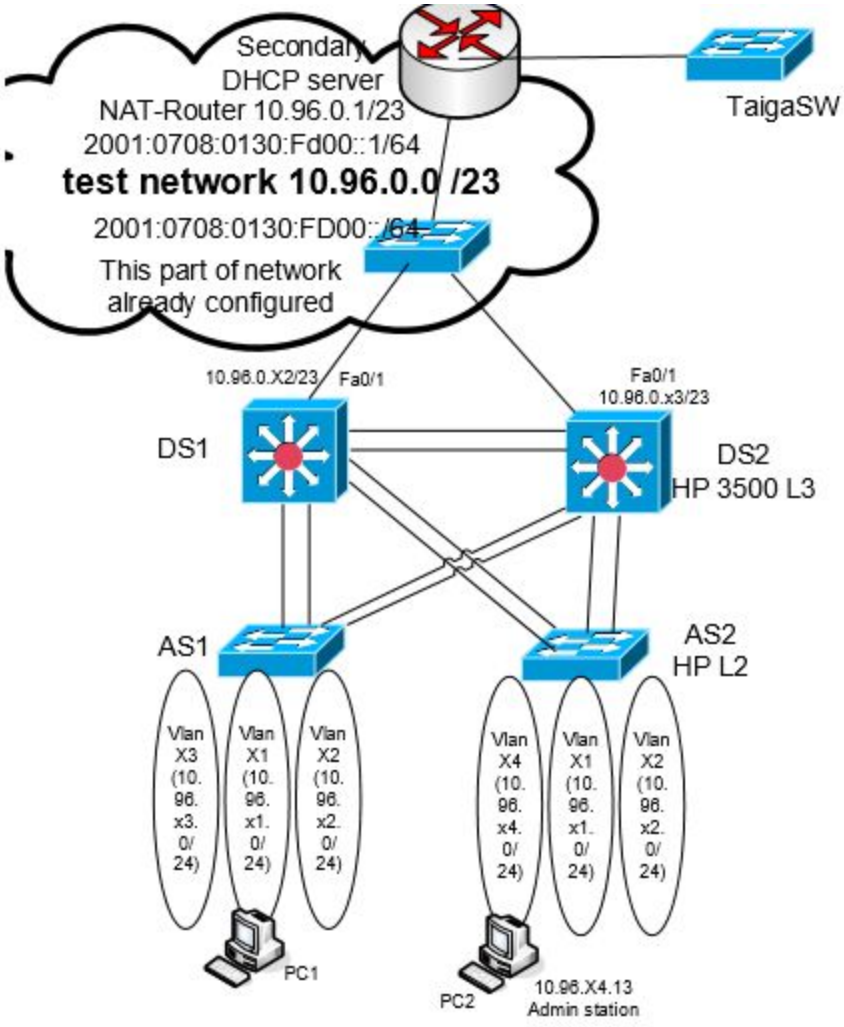
CaseStudy



DS1 must be running IOS version 12.2(58) so that it supports VRRP. DS2 switch is HP Procurve 3500 or 3800 series L3 switch. AS2 is HP 2610 or 2620 series L2 switch.

All double links between switches shall be configured as EtherChannels (Aggregated ethernet, Trunk in HP terminology). Network must be configured to use MST (Multiple Spanning Tree) protocol and DS1 must be root for VLANs X1,and X2 and DS2 for VLANs X2,X4 and X5. Configure at least three interfaces on both access-switches statically as access ports assigned to each VLAN. Configure those ports as spanning-tree edge ports (spanning-tree portfast on Cisco switch)

Information on how to configure HP-switches can be found on Tuubi and on internet. VLAN X1 is named as Staff, VLAN X2 VOIP, VLAN X3 students, X4 servers, and X5 MGT . Devices DS1,DS2, AS1 and AS2 management addresses will be assigned to VLAN X5, and we have IP address range 10.95.X5.0/24. All VLANs are manually configured to all switches.

VLANs X1, X2,X3,X4 and X5 have VRRP configured so that DS1 is active router for VLANs X1 and X2 and DS2 to all other VLANs. If DS1 connectivity to 10.94.61.254 through fa0/1 (measured with ping) fails, then active router status must be changed to DS2. Also if DS2 connectivity to 10.94.61.254 through fa0/1 fails then the active router will change to DS1. Try to optimize VRRP timers so that this transition happens as fast as practically possible.

Configure multi-area OSPF so that connection to TEST-network is the backbone connection (area0) and all other VLANS are in area 51. You should be able to access internet from all devices in your network.

We want to limit spanning tree on to our pod and therefore we disable spanning tree on port connected to TESTnetwork. We can do this on cisco by configuring DS1 fa0/1 port as routed port. Unfortunately HP does not support configuring port as routed port so in DS2 we must find another way to disable spanning tree on interface fa0/1. Disable proxy arp on L3 switches.

All user ports should have port-security enabled so that only one Mac-address is allowed and violation causes port to shutdown. Ports that will have a IP-phone connected two MAC-addresses are allowed. If port is shut down because of multiple mac addresses, try to implement procedures that try bring it up after 20 minutes. This can be done in Cisco devices by using errdisable recovery command. HP switches used in lab do not have this error disable recovery function and this function could be achieved by using suitable Network management software, but this is not needed in this case study. First 32 IP-addresses in each VLAN are reserved for network devices and other devices needing static addresses, all remaining addresses are to be provided by DHCP. For redundancy reason we are going to have two separate DHCP servers. One DHCP server is already configured in NAT_Router and it is providing addresses 33-133 whereas DS1 is to be configured to provide addresses 134-254 in VLANs X1, X2, X3 and X4. DHCP server shall give users also information about DNS (10.94.61.253), NTP(=10.94.1.4) and in VOIP VLAN a option to provide information about TFTP-server must also be configured so that IP-telephones could get their configuration from TFTPserver (=10.95.254.211, TFTP=option 66 in DHCP).

As this secondary DHCP-server is not directly connected to those VLANs it is serving you must configure DS2 to forward DHCP broadcast to this server by using IP-helper address command.

You must secure DHCP by enabling DHCP-snooping and configure only ports between active devices and towards NAT_Router as trusted ports.

Synchronize all clocks in active devices by using NTP (servers 10.94.1.4 and 10.95.254.252). Configure also correct time zones (EET) and also summertime transition rules (EEST

Configure all devices to log in debug level all messages to local 64000 bytes circular buffer (logging buffered 64000) and also to admin station (10.94.x4.13) where you must have a

suitable log-server configured (TFTPD64 can be configured to act as syslog server). Try to have all syslog messages with date and time with millisecond resolution.

All access-ports must be configured with portfast and BPDU-guard. All links between switches should have UDLD enabled. Disable all unused services on active devices (HTTP-server etc.). Configure all switches to support SSH and disable telnet to them. For login authentication on switches configure all switches to support both remote RADIUS server (10.94.x4.13) and local database (database must have a user cisco with password ciscoeigrp configured). Limit remote management connections only from devices in VLAN X4.

Test your implementation of case study and write a Group 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 shortcoming found during testing. Include all configurations from all network devices as appendix to your report. Answer questions presented at the end of this case study. This Case study has 25% weight on the grade of this course.

Questions: 1. What links are in forwarding state in each switch for spanning tree instances
2. What is the route of ping from PC1 to PC2? What switches support l2 traceroute?
3. How many links will DS1 see in spanning-tree?
4. Send a UDP stream with JPERF test program between PC1 and PC2 and disable on link on a ether channel where this stream goes, can you observe any packet loss?
5. If you disable both links in this EtherChannel, how long time does it take for traffic to take alternate route. How could this time be reduced?
6. How long does it take to use alternate route if you power down the active router?
7. Where there any requirements in this Case Study that you were unable to fulfill?
8. How you could improve security and performance of the network in your implementation of case study