INR Lab 3 - VLANs & Fault Tolerance

> Be sure to take a snapshot of your infrastructure before you start

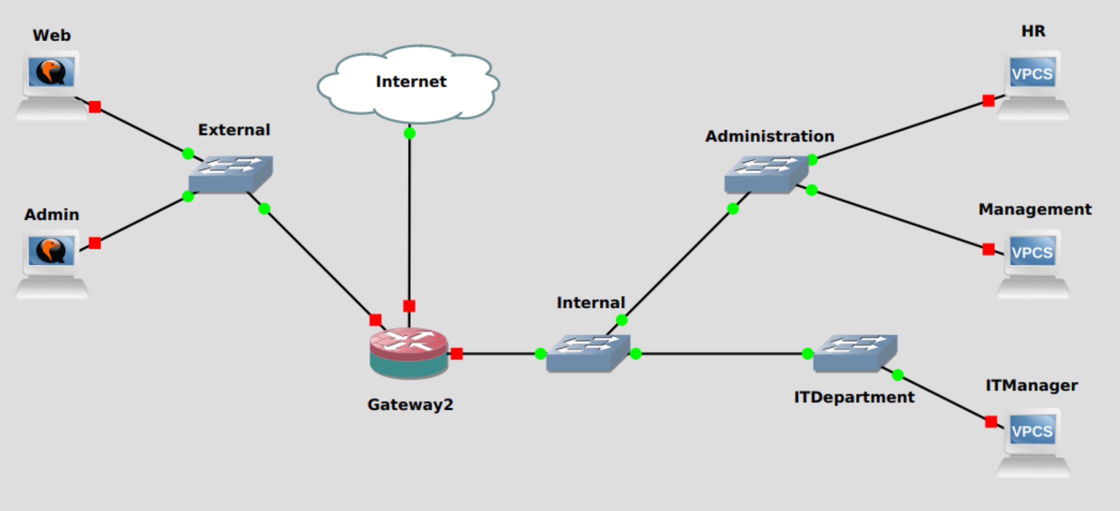
Overview

In this lab, you will take a look at some of the more advanced topics in switching. You will be learning about and configuring two aspects of those topics: virtual local area networks and fault tolerance. Virtual LANs (VLANs) is dividing the network at a Layer 2 level and Fault tolerance is making sure your network is up most of the time. Those aspects are very important when we are talking about enterprise-grade networks but they are not very complicated.

Task 1 - VLANs

In some networks, you might need to share a switch between different services that shouldn't be able to communicate with eachother for security, bandwidth or administration reasons. You will be doing that to your network but first you will need to extend it.

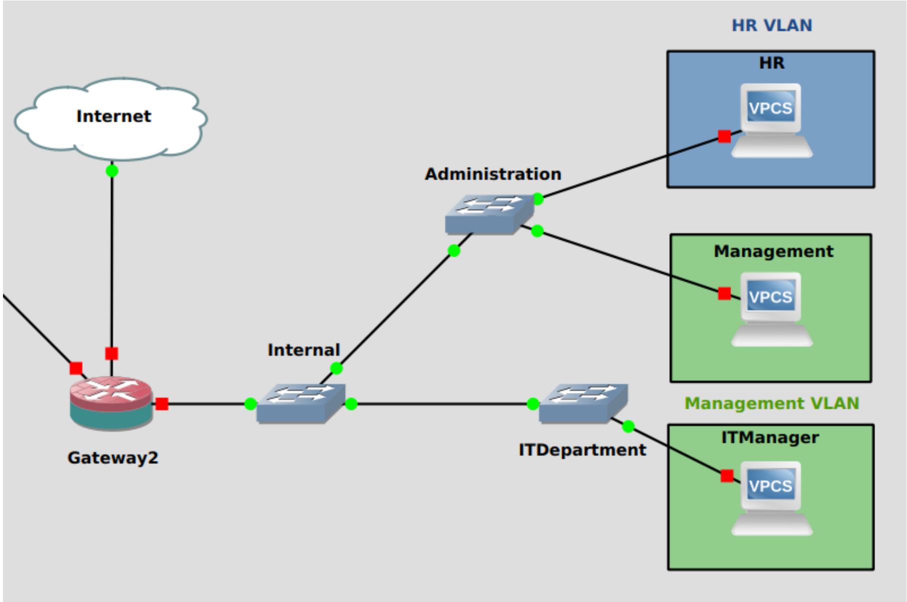
1. Change the topology of your network to as follows, make the necessary configs:



2. Exchange the defualt switches *Cumulus VX* instances.
3. Configure the switches and make sure you have connectivity between the hosts.
4. How do VLANs work at a packet level ?

   What are the two major protocols used for this ?

   What do we mean by *Native VLAN* ?
5. Configure the VLANs on the switches to isolate the two virtual networks shown below:



6. Ping between *ITManager* and *HR* , do you have replies ?

   Ping between *ITManager* and *Management* , do you have replies ?

   Capture the traffic of the last ping and show in the packet the VLANs indication.

In some cases, you might need to allow a specifc traffic to go between VLANs. This is doable but requries going through Layer 3 and is called *Inter-VLAN Routing* .

7. Configure Inter-VLAN Routing between *Management VLAN* and *HR VLAN* .
8. Show that you can now ping between them.
9. Capture the traffic going to and out of the router and show the different traffic of the sub-interfaces.

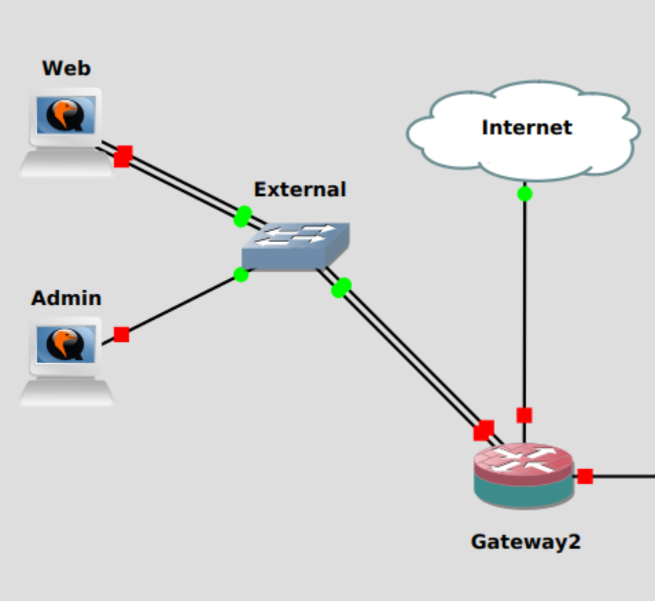
Task 2 - Fault Tolerance

Fault tolerence is important in a network but cables, routers and sotfware can be very unreliable. To mitigate this, we often rely on redundancy i.e. doubling everything. You'll be learning how to do this and what problems come out of it.

1. What is Link Agregation ?

   How does it work (breifly.) ?

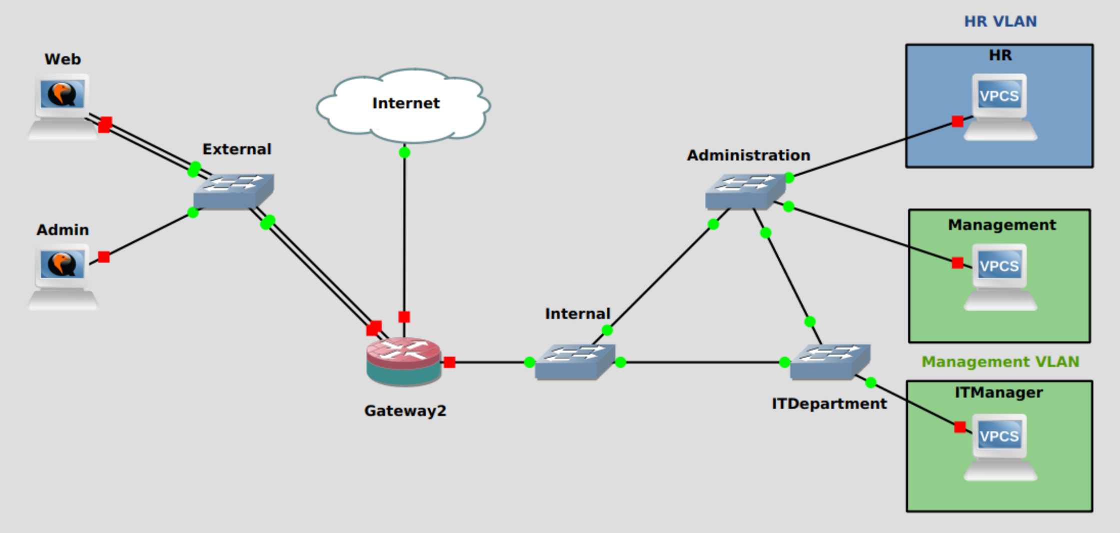
   What are the possible configuration modes ?
2. Use link agregation between *Web* and the *Gateway* so that you have *Load Balancing* and *Fault Tolerance* .



3. Test the Fault Tolerance by stoping one of the cables and see if you have any down time.

Now that you dealt with cables, it is time to deal with network equipment. Usually, network equipment failures is reson for downtime. Just like with cables, we can double the switches/routers and have two paths, however, this can generate some problems as you will see.

5. Disable *STP* on the Switches under *Internal* .
6. Change the topology to have two paths as show below:



7. Capture the traffic send a boradcast ping request to the PCs connected to the Internal Network.

   What can you notice ?

   Why did this happen ?

   What are the implications of this on the network ?
8. Enable back *STP* on the Switches and do the experiment again.

   Can you see *STP* traffic ? Explain it breifly.

   Configure the switches to have the *Internal* as the Root switch.
9. Would we need STP between routers ?