FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Departamento de Engenharia Electrotécnica

Configuração e Gestão de Redes

2016 / 2017

Mestrado Integrado em Engenharia Electrotécnica
e de Computadores

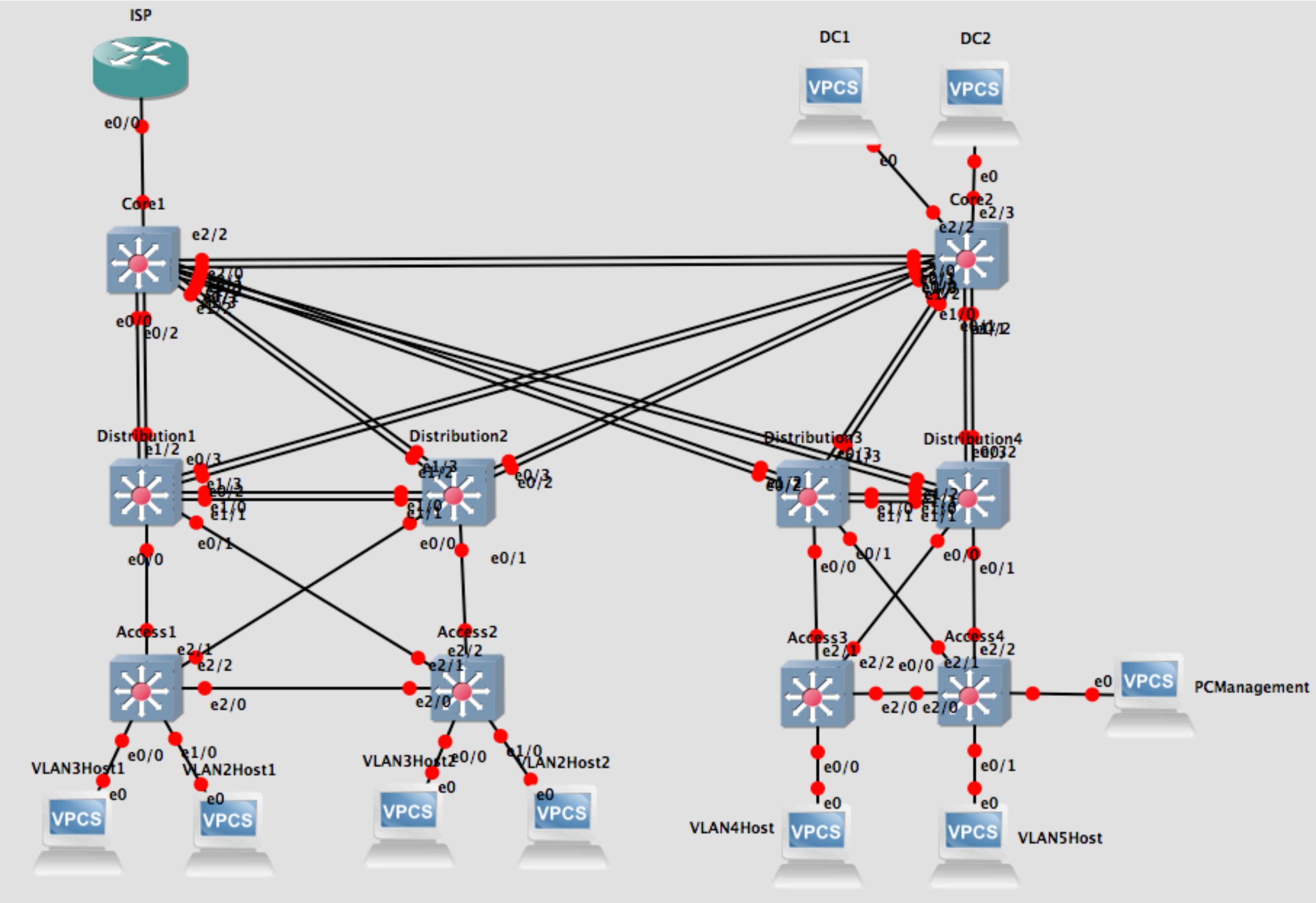
4º ano

1º Project:
CLI configuration: Enterprise scenario and Routing scenario

http://tele1.dee.fct.unl.pt/cgr **Pedro Amaral**

First part: Design and configure an enterprise network.

You should configure a hierarchical enterprise network. The network is divided into two different access pods that are composed by two access and two distribution switches. They can represent for example the networks of two different buildings of a campus. These two access pods are then connected via two core switches that are connected to a datacenter simulated here with two hosts and to an ISP via a router for Internet access. The following figure illustrates the topology:



The two access pods have different VLAN policies:

The Pod in the left of the topology has **an end to end VLAN policy** and **both switches** have access ports for **VLANs 2 and 3**. Both **Access 1 and Access 2** switches have also at least one port in access mode for a different VLAN for management purposes (management hosts can connect in that port using that VLAN).

In the Pod in the right there is a **local VLAN** policy where a VLAN resides only in one switch. In this case, the **Access 3** switch has access ports for **VLAN 4** and **Access 4** Switch for **VLAN 5** and there are **no more switches with access ports in those VLANs.** Has in the previous case in this pod **Access 3 and Access 4** switches also have at least one port in access mode for a management VLAN.

The goal is that end hosts in **all** VLANs (except the management VLANs) can communicate with each other, with the two servers connected to the core and to the Internet (simulated by a loopback interface in the router) via the ISP router.

Network management PCs might exist connected to one of the access switches in one of the management VLANs ports (the ones in the figure is merely illustrative).

Those PCs, should be able to reach all switches for remote management.

Security could be an issue here since hosts in the other VLANs can also reach switches that are operating in Layer 3 mode and have SVIs for the host VLAN, you should use an appropriate ACL to enforce that only hosts from the management VLANs can access the switches.

You should implement the following requirements:

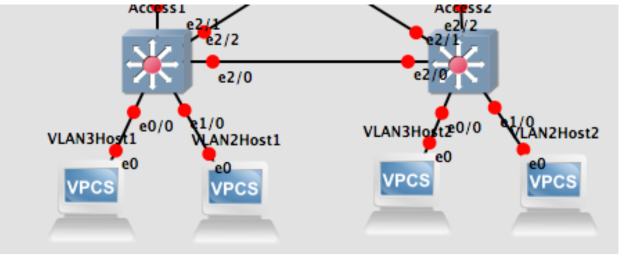
- The network has 4 access switches where end hosts connect. Dividing in two different VLAN policy access pods.
- There are 4 different end user VLANs 2,3,4,5.
- There is one management VLAN in each pod.
- **At least** the distribution and core part of the network work at layer 3, using EIRGP.
- Because of the last point. The management VLAN can **not be the same in both pods,** since there is no Layer 2 connectivity between the pods. Even if they have the same VLAN id (the VLAN number) they are two different VLANs since VLAN can only exist between devices with Layer 2 connectivity.
- VLAN 4 and 5 only have access ports in the respective switch. User-facing ports should be configured for access for the corresponding VLAN. With at least one left for the management VLAN.
- VLAN 2 and VLAN 3 have access ports in both access switch 1 and access switch 2, the available user-facing ports should be equally divided amongst both VLANs also with at least one port on each switch left for the management VLAN.
- Network management PCs can be connected to any of the access switches in an access port belonging to the management VLAN. The management PCs (and only those) should be able to reach all switches and the router in the network via telnet for management.
- The links between the access switches are for redundancy reasons and should be used in case both uplinks to the distribution layer fail in one of the access switches.
- Both servers connected in core switch 1 should be reached by users in any of the VLANs
- The Internet should be simulated via a loopback interface configured in the router with an IP network not used in the rest of the network. That network should be reachable from all hosts in all VLANs.
- Links between the distribution switches and core switches should be bundled together using etherchannel whenever possible.
- Use an addressing scheme based in subnets of the 10.1.0.0 /16 block.
- In the L3 part of the network (at least the distribution and core) you must configure EIGRP.
- You should configure AS number 10 for EIRGP and configure EIGRP to route all relevant networks.
- The core 1 switch should inject a default route, so that any traffic not known is directed to the ISP router.
- The distribution routers should summarise the networks of the POD VLANs in the announcements to the core routers. You should choose contiguous Subnets for the VLANs of a POD so that you can perform this summarisation.

Work Plan and links for examples

1. You should start by installing the GNS 3 simulator for your operating system following the instruction at https://gns3.com/support/docs/quick-start-guide-for-windows-us then you should download and run in a virtualisation hypervisor the GNS3-VM see instructions in https://gns3.com/support/docs/download-the-gns3-vm, finally you should have the images and licence file available at http://tele1.dee.fct.unl.pt/cgr_2016_2017/secure/Material.zip.

2. You can familiarize yourself with IOS by following the instructions in the document "IOS introduction" in http://tele1.dee.fct.unl.pt/cgr_2016_2017/files/IOSintro.pdf.

3. You should then start by configuring the Access Switches in the left. You should configure the VTP protocol with both switches in the same domain and both in transparent mode. Create the host VLANs as well as the management VLAN in both switches, configure the access ports in access mode and attribute them to the respective VLANs. If that is your choice configure the link between both switches as an 802.1.Q trunk that allows all the relevant VLANs. You can find configuration examples in the document "VLANs, Trunks, VTP" in http://tele1.dee.fct.unl.pt/cgr_2016_2017/files/VLANsTrunksVTPmodes.pdf.

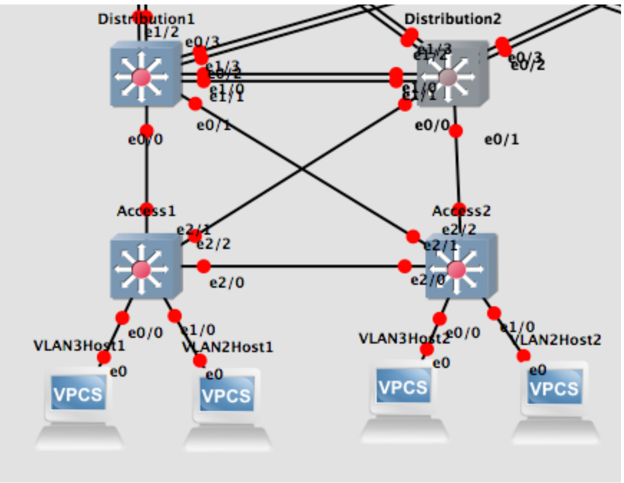


NOTE: GNS3 projects do not store configuration when you save the project, it merely stores the topology file. In order to maintain the configuration between sessions you should use the command

copy running-config unix:initial-config.cfg

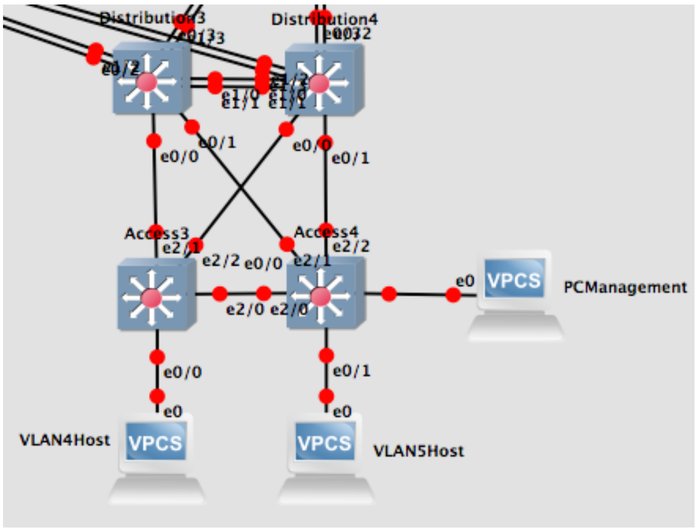
in the routers/switches this stores the running config in an initial configuration file inside the GNS3 VM. You are also advised to keep local text files with the configurations of each device as a backup.

4. You can then add the Distribution switches of the left pod



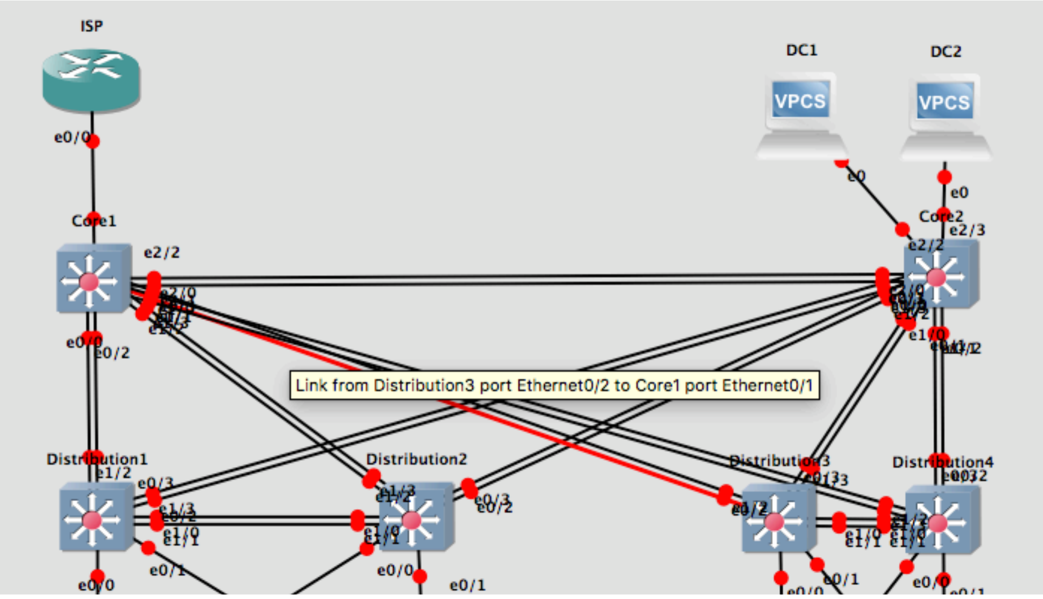
1. Perform the same basic configurations that you performed for the access switches.
2. If you choose to have layer 2 up to the distribution switches you need to create the VLANs in the distribution switches add them to the same VTP domain of the access switches (also in transparent mode), the links between the access and distribution switches are in that case 802.1Q trunks. Once again you can find examples in the "VLANs, Trunks, VTP" document in the link : http://tele1.dee.fct.unl.pt/cgr_2016_2017/files/VLANsTrunksVTPmodes.pdf.
3. You might need to configure the links between Distribution 1 and 2 has either a trunk or a layer 3 link in either case they should be group together in an EtherCannel. You can find examples of Etherchannel creation in the document "Etherchannels and Inter-VLAN routing" in: http://tele1.dee.fct.unl.pt/cgr_2016_2017/files/InterVLANrouting.pdf.
4. Finally you should create the SVIs for the VLANs in the distribution switches, thus defining the IP subnets for each VLAN and then enable routing in this switches. You can find examples in the "Etherchannels and Inter-VLAN routing" in http://tele1.dee.fct.unl.pt/cgr_2016_2017/files/InterVLANrouting.pdf.
5. You should test connectivity by assigning IP addresses to the hosts belonging to the corresponding VLAN IP subnet and configuring the hosts gateway to the IP address of the SVIs in the distribution switches. You can also configure the distribution switches as DHCP servers so tha this configuration is automatic in the hosts.
6. Finally with the links between Access and distribution switches in layer 2 you can change the STP protocol to Rapid per VLAN STP and define the most suitable root bridges. You can find configuration examples in the document "STP configuration" in: http://tele1.dee.fct.unl.pt/cgr_2016_2017/files/STP.pdf.

5. Perform the same operation in the right hand pod



1. In this case the SVIs can be in the access switches and the links between them and the distribution switches can be in Layer 3 and use routing. In this case the access switches have to support routing and therefore should be of the same model as the distribution switches. This means that the links between the switches must be in their one IP subnet, that EIGRP should be configured with the appropriate AS number and networks. You can find configuration examples for EIGRP in the documents "EIRGP scenario 1" in http://tele1.dee.fct.unl.pt/cgr_2016_2017/files/EIGRP1.pdf and "EIRGP scenario 2" in http://tele1.dee.fct.unl.pt/cgr_2016_2017/files/EIGRP2.pdf.

6. Finally configure the core layer switches and interconnections with the pods



1. Here you should configure Layer 3 Etherchannels aggregating the links between the distribution and core switches, each aggregate should be in its own IP subnet. You should enable routing EIGRP and configure (examples can be found in the documents “EIRGP scenario 1” in http://tele1.dee.fct.unl.pt/cgr_2016_2017/files/EIGRP1.pdf and “EIRGP scenario 2” in http://tele1.dee.fct.unl.pt/cgr_2016_2017/files/EIGRP2.pdf):
    1. The appropriate networks to announce
    2. The summarisation of the addresses announced from the aggregation switches
    3. The generation of a default route by the core 1 switch.

7. The final step is to insert an ACL in all switches that only allows telnet connections from the management VLANs. You should then test connectivity between al hosts, all hosts and the data center servers and all hosts and the ISP loopback address simulating the Internet addresses.