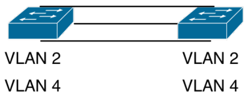
NOVA SCHOOL OF SCIENCE & TECHNOLOGY
Department of Electrical Engineering and Computers

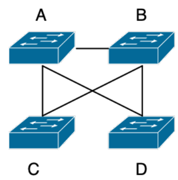
Configuração e Gestão de Redes
Mestrado Integrado em Engenharia Electrotécnica e Computadores
Pedro Amaral
21 de Outubro de 2019
1º Teste

Duração: uma hora e meia + meia hora de tolerância

1. A host 1 connected to switch A on an access port of VLAN 2 is configured with IP address 10.4.2.1/29 and gateway 10.4.2.6 (an SVI also on switch A). Host 1 sends an IP packet to a host 2 configured with IP 10.4.2.9/29 and which is connected to a second switch B, host 1's ARP table is empty.
   a. Is the destination host on the same VLAN? What is the IP address that the Host tries to resolve with ARP (what is the target IP of the ARP request)? Justify.
   b. Consider now that the two switches are linked with a single link. Indicate justifying whether the link that connects them must be in Layer 2 or Layer 3 for the packet to reach its destination.



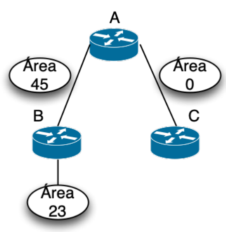
2. In the figure on the side there are three links connecting the two switches using interfaces f0/1, f0/2 and f0/3 (on both), VLANs 2 and 4 exist on both switches and the three links are in trunk mode allowing VLANS 2 and 4. Assume that the rapid per-VLAN Spanning protocol is running. Is there any way to assure that no links are blocked due to loops? Justify indicating the necessary method so that the 3 links are not seen as loops in this situation.



3. In the network shown in the figure, VLAN 4 and VLAN 5 have access ports both on switch C and switch D. Communication should be possible between hosts in VLAN 4 and VLAN 5 as well as between hosts in the same VLAN. In this scenario:
   a. Should the ports connecting access switches C and D to aggregation switches A and B be in trunk (Layer 2) or routed (Layer 3) mode? Justify your answer.
   b. Now consider that there are SVIs for VLAN 4 and 5 on switch C and that there are also SVIs for VLAN 4 and 5 on switch D. Is any further configuration required to achieve the intended connectivity? Justify indicating the path of packets in communications on the same VLAN as well as between different VLANs and on which Layer the links operate.
   c. Answer the same question as in point b. but consider now that there is only one SVI from VLAN 4 that is on switch A, and that there is only one SVI from VLAN 5 that is on switch B.

4. An EIGRP router has in its Topology Table 4 routes to the same destination with the following values of Feasible Distance (FD) and Advertised Distance (AD). Route 1 FD 400 AD 100; Route 2 FD 150 AD 50; Route 3 FD 350 AD 120 and Route 4 FD 550 AD 50. Which route is chosen as (current) successor? If the max-paths 4 and variance 2 commands are introduced which routes can be used simultaneously for load balancing? What if the variance 2 command is withdrawn? Justify the answer in both cases.

5. Consider the two Interior Gateway Protocol (IGP) routing protocols studied in the chair: EIGRP and OSPF. Explain what the differences between them in two aspects i) The information that is exchanged between two neighboring routers after the establishment of a neighborhood ii) how the best routes are calculated.



6. Consider the scenario in the figure with routers A, B and C that are using OSPF. Router A has Interfaces: F0/1: 10.4.45.1/30 in area 45 and F0/2 IP: 10.4.0.1/30 in area 0. Router B has interfaces F0/1: 10.4.45.2/30 in area 45 and F0/2: 10.4.23.1/24 in area 23 finally router C has interface F0/1: 10.4.0.2/30 in area 0
   a. In the routing tables of routers A and C there are no entries for network 10.4.23.0/24 in area 23, why? Justify this absence by indicating how it can be resolved. In the answer indicate which are the router IDs of router A and B.
   b. B. Indicate the necessary steps to configure OSPF on router A according to the interfaces and areas described above.

Solution

1.

a. The destination host is not in the same VLAN since the mask is 29 bits long which means that the network of VLAN 2 goes from address 10.4.2.0 (network address) to address 10.4.2.7 (broadcast address). This means that the address of host 2 is from the 10.4.2.8 /29 network and therefore from a different network. So the IP address that host 1 tries to resolve is from its Gateway (10.4.2.6) sending an ARP request with the destination MAC address FF:FF:FF:FF (Broadcast) that arrives without problems at the destination once the gateway is on the same switch as the host.
b. For the packet to reach the destination, the gateway of host 1 must forward it to the network of host 2, which is on switch B, but this implies one of two hypotheses (both correct):
   • Hypothesis 1 Switch A has no SVI for host 2's VLAN and therefore does not know host 2's network, so the only chance the packet will reach the destination is by learning that the network is on the neighboring switch through a forwarding protocol which implies that the connection between both switches must be in Layer 3 and that there must be an SVI of the other VLAN on switch B.
   • Hypothesis 2 Switch A has a second SVI configured for host 2's VLAN, in this case host 2's network is directly connected associated with the ports of the respective VLAN, the link between the two switches could then be a layer 2 trunk where both VLANs pass

2.

If the 3 links are viewed independently they form two loops in Layer 2 so the spanning tree will cut ports in order to undo those loops. The only way to have no cut ports is to aggregate the 3 links in a port-channel so that they are seen as a single virtual port. Since the configuration of the 3 links is the same (trunks with VLANs 2 and 4) it would be enough to insert the command (channel-group) to create the Etherchannel on both ports.

3.

a. The. The ports between C, D and A,B must be in Layer 2, otherwise there is no connection in Layer 2 between hosts of the same VLAN on switches C and D, which would make communication between them impossible. (Ex., an ARP request from a host on VLAN 4 in C would not reach the destination if the IP target is from a Host that is on Switch D).

b. B. In this case with SVis for both VLANs in both C and D, Switches C and D would know both networks as directly connected (turning on IP Routing). So forwarding between VLANs is possible on each Switch passing packets from one VLAN to the other. Links to A and B can remain Layer 2. Forwarding within the same VLAN is also possible as the VLANs span both access switches. The path of a packet between VLANs starts at the host that sends it to the respective access switch C or D (where the SVI that is its gateway is) then at the access switch it passes to the ports of the other VLAN if the destination host is on the other access switch, the packet gets there through trunks and switches A and B (which act only as Layer 2 switches). The path of a packet within the same VLAN is similar but without VLAN switching on switches C and D.

c. In this case the link between A and B will be necessary and will have to be in Layer 3. As the SVIs are in A and B, only they know the networks and each one only knows one of the networks. This implies that to communicate between VLANs A learns the network that exists in B and vice versa. This is only possible using a routing protocol, which implies a layer 3 connection between A and B through which to carry out the neighborhood. The packet path within the same VLAN is similar to the previous question. The path of a packet between different VLANs starts at the host, goes through Layer 2 links to Switch A or B (whichever has the SVI with the corresponding gateway) and then through the A-B link to the other side where the other switch has directly connected to the other VLAN's network.

4.

The route chosen as Current Successor is the route with the best FD, ie route 2. With the max-paths 4 and variance 2 commands, up to 3 routes can be chosen as Feasible Successors by joining the Current Successor to make 4 routes. Feasible Successors must have their AD < FD of Current Successor and with variance 2 command their FD cannot be more than 2 times greater than the FD of Current Successor. So no route can be used as a Feasible Successor because although they all have an AD < FD they all have a FD greater than twice the best FD. If the variance 2 command is removed all can be used as they all have AD<FD.

5.

The EIGRP protocol is a distance vector protocol, which means that the information exchanged between neighbors is a distance vector containing the networks reachable by the router and the respective distances to them, the route calculation is then done by the router that receives the vector. of distances that adds the distance to the neighbor and then selects the smallest distances.
The OSPF protocol is a link-state protocol. In this case, the information exchanged with the neighbors is the list of links and respective networks that are directly connected to the routers, and the routers flood this information to all other neighbors. This allows each router to build an entire topology view. Paths are then computed over that topology by each node using a shortest path tree computation algorithm (eg Dijkstra).

6.

a. This happens because area 23 is not connected to the backbone area (area 0). To solve the issue, you will have to create an OSPF virtual-link that places an interface in area 0 on one of the routers in area 23. In this case, you would have to create a virtual-link between B (which is in area 23 and in area 45) and A (which is also in area 45 but has an interface in area 0). The virtual-link crosses area 45 and its configuration is done using the router-ids of A and B. As these are not explicitly configured, they will be determined by the IPs of the Interfaces. If there are no loopback interfaces, the router-id will be the highest IP address among the various router interfaces. So for router A it will be 10.4.45.1 and for router B 10.4.45.2

B. We start by configuring the routing process (eg router ospf 1). Then, in the configuration mode of the routing process, the network commands are introduced in order to create the matching rules to include interfaces in the respective areas, in this case it would be, for example:

```
network 10.4.45.0   0.0.0.255 area 45
network 10.4.0.0    0.0.0.255 area 0
```