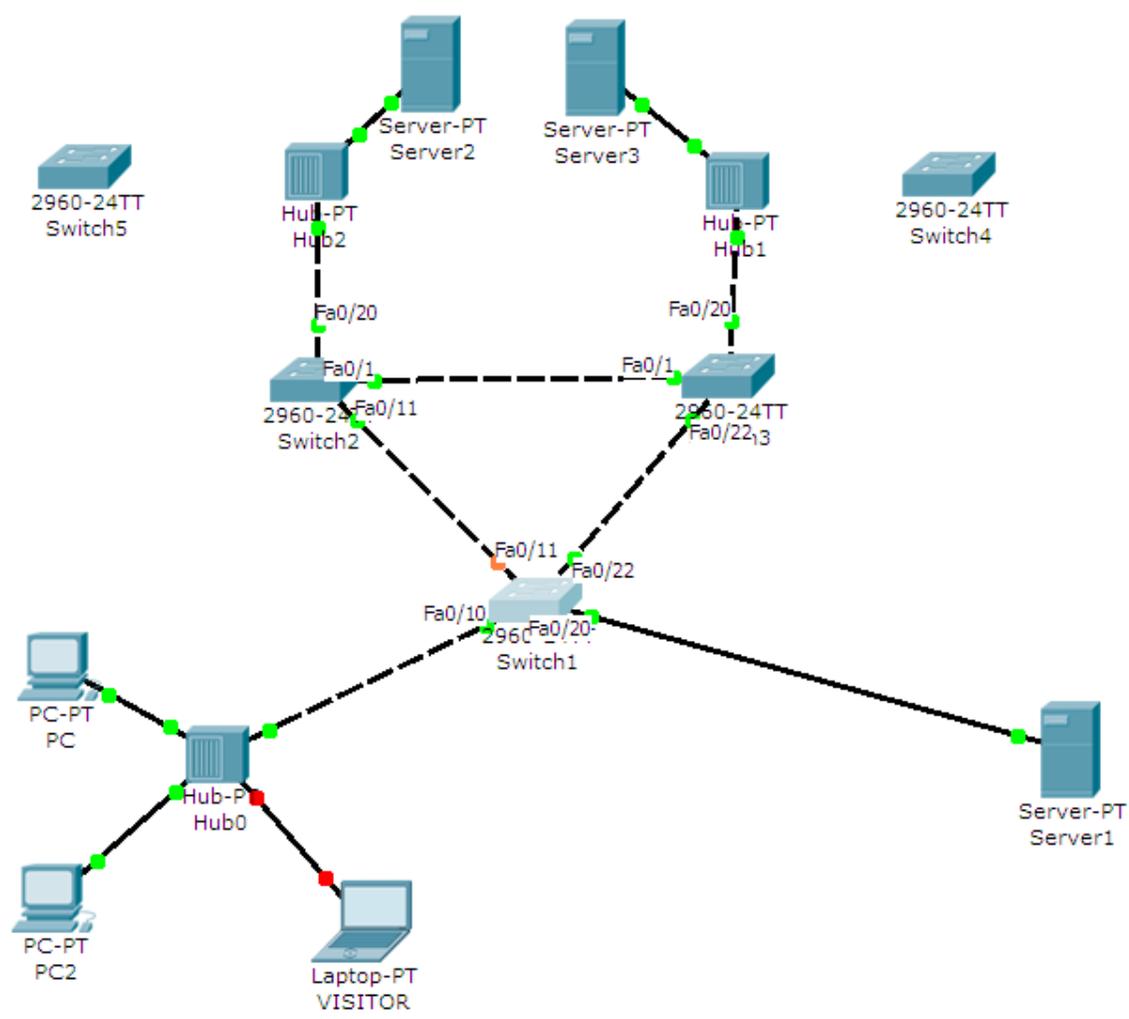# Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

Securizarea Calculatoarelor și a Rețelelor

22. Implementarea securității în rețele locale

Endpoint Security

Tasks

Open the `Labweek7-Topology.net` file.

Important! Non-persistent tasks:
- Some tasks will as you to intentionally cause an error in the configuration/topology. If you wish to continue with the following tasks and you need to correct the error, make sure you paste in a text file the required command outputs that prove that the previous tasks have been correctly solved.

Important! Configuring this lab:
- DO NOT change the topology (not even port numbers for connected cables).
- DO NOT attempt to configure anything on the hubs.
- DO NOT add any extra connections unless excplicitely mentioned by an exercise.
- DO NOT attempt to configure any Layer 3 information on the switches [except for the bonus task].

Useful show commands:
„show interface switchport"
„show spanning-tree summary"
„show spanning-tree interface fastethernet x/y"
„show port security"

1. [+1.5=6.5p] You want your network traffic patterns to be predictable. One step towards this is to ensure that no other switch will become the root bridge and no user will be able to spoof BPDUs in order to receive all switched traffic, as would a real root bridge do. Protect all three switches against superior BPDUs (BPDUs that are better than the ones of the root bridge's).
   Hint: To test, connect SW4 to Hub1 (any port to any port) using a cross-over cable.

2. [+1.5=8p] You are worried about users that might connect switches to your topology and cause disruptions in your topology. Configure non-trunking ports to shut down automatically when they receive a BPDU.
   Hint: To test, connect SW5 to Hub2 (any port to any port) using a cross-over cable.

3. [+2=10p] Configure port security on SW1 so that only two MAC addresses will be learned on port Fa0/10 and will be automatically stored in the running configuration. If a third MAC address is detected, alert messages will be sent and the packets from the unaccepted MAC address discarded.
   Hint: To test, turn on PC „VISITOR", assign it an IP address and send some traffic.

   Hint: Packet Tracer might not show the syslog messages; check the port security violation counter instead.

4. [BONUS] [+1=11p] Call the lab assistant to check your progress before attempting this task. Add a 3560 multilayer switch in the topology. Disconnect the cables in ports Fa0/10 and Fa0/20 from SW1 and connect them to the 3560. Configure the segment on the left (hub+3 hosts) in VLAN 10

and Server1 in VLAN 20. Provide inter-VLAN connectivity using switched virtual interfaces (SVIs) on the 3560..

Hint: Change Server1's IP address, so that it will belong to a different subnet than the one of VLAN10.

Hint: your connections should look like this: