Part 1: Connectivity and Virtual PCs (VPCs).

VPC is a component of GNS3. It allows users to create virtual hosts with IP addresses and subnet masks and test for connectivity (with *pings*), as well as a few other actions.

1- Drag and drop one switch from the components area to the topology area (cf. figure 1).
2- Drag and drop two VPCs.

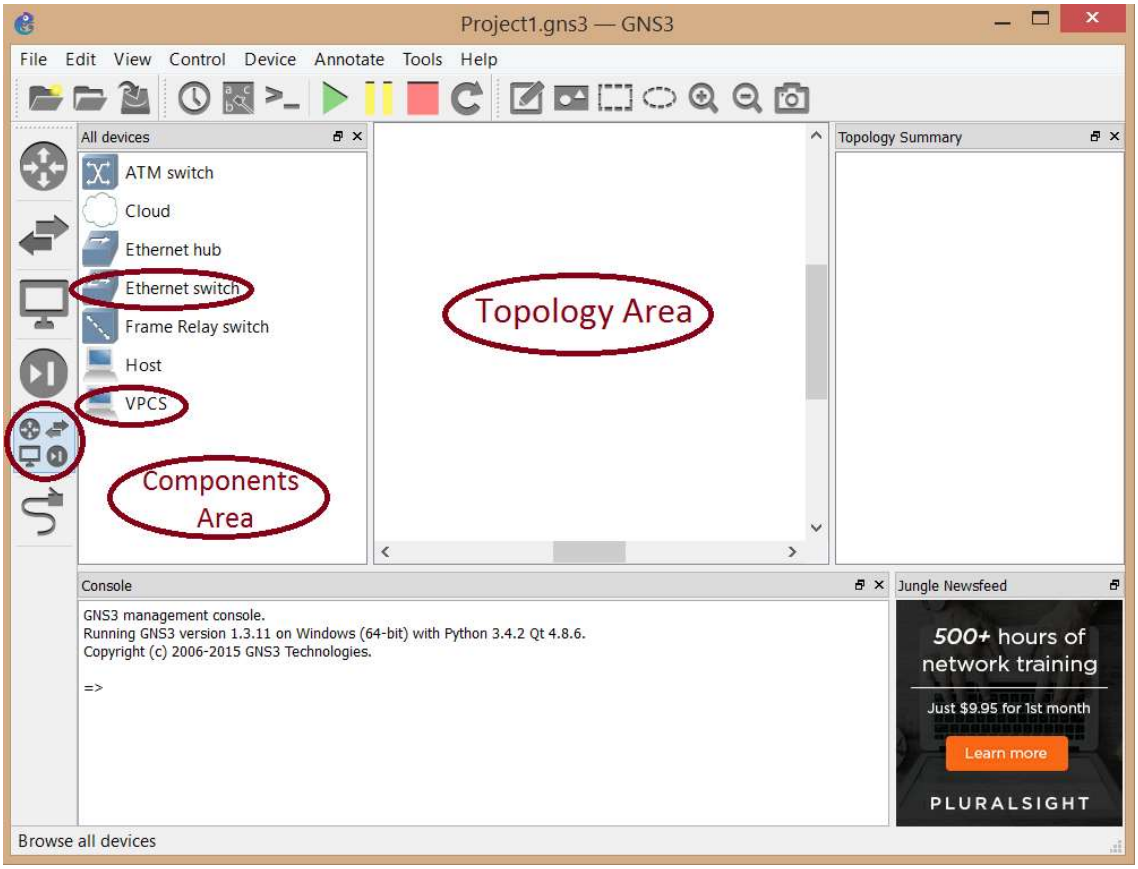

Figure 1: Main Interface

3- In this step you will connect the components you created. Click on “add a link” (cf. figure 2). Then, click on SW1; a menu appears, choose “1”. Immediately click on PC1; a menu appears with only one option “Ethernet0”, click on it. This connects PC1 to SW1. Now connect PC2 to SW1 (on interface “2” this time).

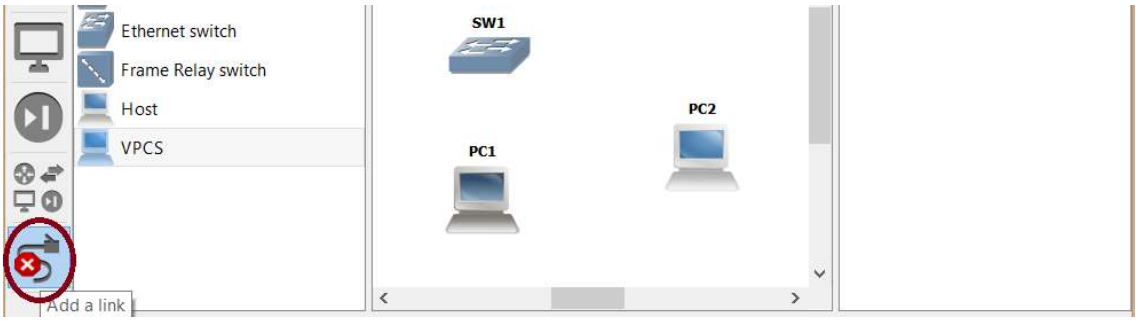

Figure 2: Add a link

4- Click on the green button on the top to start all devices (cf. figure 3). The topology summary to the right will change the colours of PC1 and PC2 from red to green.

Figure 3: Start all devices

5- Right-click on PC1, and choose “Console”. Type “ip 192.168.1.1/24” and enter. Do the same with PC2 but this time use “ip 192.168.1.2/24” instead.
6- Ping 192.168.1.1 from PC2.

Part 2: Subnets.

1- Add two VPCs, PC3 and PC4. Set their IP address to 192.168.1.129/25 and 192.168.1.130/25, respectively make sure they can ping each other.
2- Change the network mask of the first two PCs from /24 to /25. Can they ping each other?
3- Can you ping PC3 or PC4 from PC1? Why?

Part 3: VLANs

Virtual LAN, or VLAN for short, is a technique used to separate traffic at switch level. It will usually separate traffic with different requirements (whether QoS or Security). For example, VoIP traffic (generated by IP phones) generates light-weight traffic, but requires very short delay. Whereas Internet browsing traffic generated by computers generates much more traffic, but can tolerate higher delays. Switches can “tag” different traffic streams differently. So, say, VoIP traffic will be tagged as traffic 10, PC traffic will be tagged as traffic 20. Switches can now treat them differently, e.g. deliver a frame from tag 10 even if frames from tag 20 are already queued ahead (thus, reducing its delay). Traffic tagged 10 is said to be on VLAN10, traffic tagged 20 is on VLAN20.

1- Right-click on the switch, then click on “configure”; a window appears, click on “SW1” on the left pane, cf. figure 4.
2- Assuming PC3 and PC4 are connected to ports 3 and 4, change the VLAN of ports 3 and 4 to VLAN20 (you will need to click on “add” to apply your modifications).
3- Make sure that pings between PC1 and PC2 work.
4- Now put all the PCs on the same network (192.168.1.1-4/24).
5- Try to ping PC1 from PC2, then PC3 from PC1, then PC4 from PC2, then PC4 from PC3. How would you explain your findings?

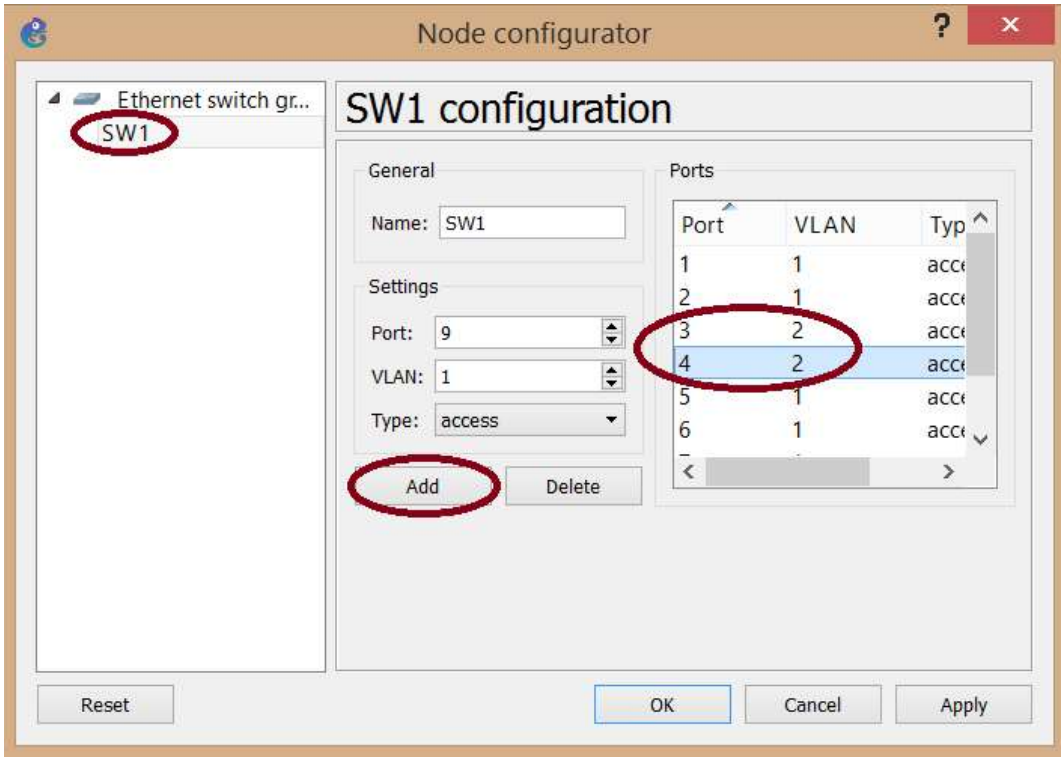

Figure 4: Configuring VLANs on an Ethernet Switch.

Part 4: Wireshark

Wireshark is a sniffing tool we used in an earlier lab. Wireshark comes bundled and configured with GNS3. It can be easily used to sniff on a link of your topology. Simply right-click on a link (cf. figure 5) and click on “start capture”. A windows appears with a dropping menu that has one option, click on OK. Then right-click again on the link and choose “Start Wireshark”.

1- Reconfigure PC 1, 2, and 3 to be on the same network.
2- Start a continuous ping from PC1 to 2 (by adding the –t option at the end of the ping command).
3- Start sniffing on PC1’s link using Wireshark. Which protocol is used for pings?
4- Start sniffing on PC3’s link using Wireshark. Can you see the pings from there? Why?
5- Now replace the switch by a hub and redo questions 2 to 4.

You now (really) know what the difference between a switch and a hub is!

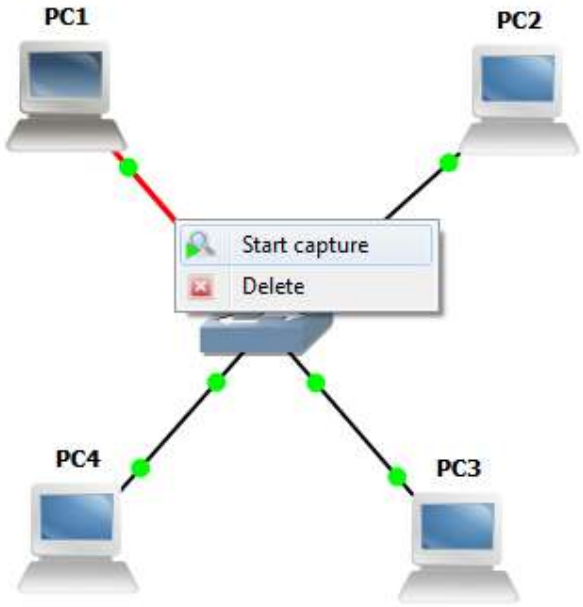

Figure 5: Starting capture on an interface.