# Data Communications and Networking
# Lab 1 - Connectivity, VPCs, Subnets, VLANs

Hani Ragab, Adam Sampson and Zi Hau Chin
School of Mathematical and Computer Sciences, Heriot-Watt University

## Introduction

This is the first assessed lab exercise. The first four exercises together make up 10% of your final mark for the course.

You should work through the worksheet below in the week before the lab, taking a screenshot of the network(s) that you have built at the end of each Part of the instructions. When the instructions ask you to answer a question (e.g. “Can they ping each other?”), make a note of your answer. We suggest you put your notes and screenshots into a word processor like LibreOffice, then you can easily produce a single PDF file to submit.

## Terminology: IPv4 addresses

We will look at IP addresses in more detail in the lectures, but here's a quick reminder.

We connect computers and other devices to networks using **network interfaces**. For example, you might have a laptop with two network interfaces: a wired Ethernet socket, and a WiFi radio connection.

When it's connected to an IPv4 network, each interface is identified by an **IP address**. A device can have several IP addresses, if it has multiple network interfaces.

An IP address is a 32-bit binary number. We normally break the address into four groups of 8 bits each, and write them as decimal numbers separated by dots. So the binary address `11111111 00000000 00000000 00000001` would be written as `127.0.0.1`.

IP addresses are assigned in a hierarchical way. If you have several interfaces connected to the same local network (**subnet**), they will all have addresses that start with the same prefix. So we divide the 32 bits of an IP address into a **network ID** and a **host ID**.

For example, your home network might have interfaces with the addresses `192.168.1.1`, `192.168.1.4` and `192.168.1.15`. In this case, the first 24 bits (`192.168.1`) are the network ID, and the last 8 bits are the host ID.

So when we're describing addresses on a local network, we need to know how many bits make up the network ID. We can include this when writing an IP address — `192.168.1.0/24` means that the network ID is the first 24 bits.

We can also describe this using a **network mask** (**netmask**), which is a 32-bit number with 1s in the places that make up the network ID. For a `/24` network, the network mask is `255.255.255.0` — in binary, that's `11111111 11111111 11111111 00000000`.

## 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. A VPC can test for connectivity (by sending **ping** messages), as well as a few other actions.

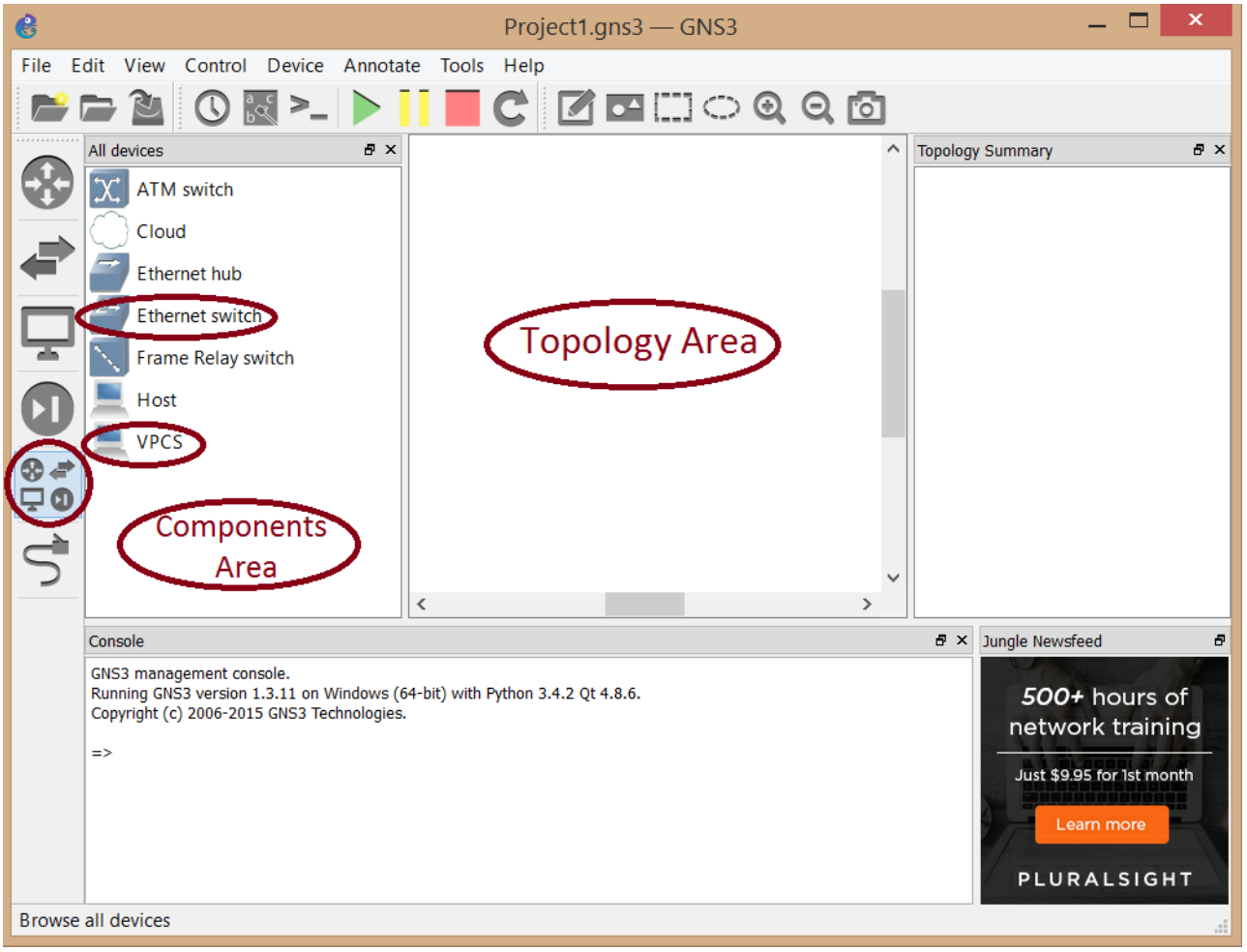


**Figure 1**: Main interface

- Drag and drop one switch from the components area to the topology area (see Figure 1).
- Drag and drop two VPCs.

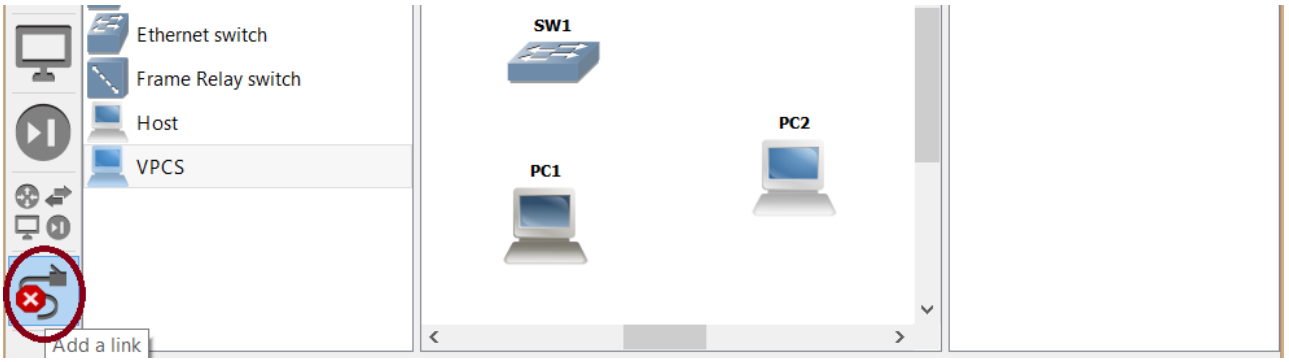


**Figure 2**: Add a link

- In this step you will connect the components you created. Click on **Add a link** (see 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 3**: Start all devices

- Click on the green button on the top to start all devices (see Figure 3). The topology summary to the right will change the colours of PC1 and PC2 from red to green.
- Right-click on PC1, and choose **Console**. Type `ip 192.168.1.1/24` and press enter. Do the same with PC2 but this time use `ip 192.168.1.2/24` instead.
- Ping `192.168.1.1` from PC2.

## Part 2: Subnets

- 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.
- Change the network mask of the first two PCs from `/24` to `/25`. Can they ping each other?
- Can you ping PC3 or PC4 from PC1? Why?

## Part 3: VLANs

Virtual LANs (**VLANs**) are used to separate traffic within a switch by dividing it into multiple virtual networks.

They are used to separate traffic with different requirements, such as quality of service (QoS) or security. For example, VoIP traffic generated by IP phones generates a small volume of traffic, but requires very short delay, whereas Internet browsing traffic generated by computers generates much more traffic, but can tolerate higher delays. And you probably don't want your local phones to be connected to the Internet! So a typical office would use separate VLANs for computers and phones.

When a switch receives a frame, it applies a VLAN **tag** to it to indicate which virtual network it belongs to. So, say, VoIP traffic will be tagged as VLAN 10, and PC traffic will be tagged as VLAN 20. The switch will only deliver traffic to ports that belong to the same VLAN. Switches can also treat frames differently, e.g. deliver a frame from VLAN 10 even if frames from VLAN 20 are already queued ahead of them (thus reducing its delay).

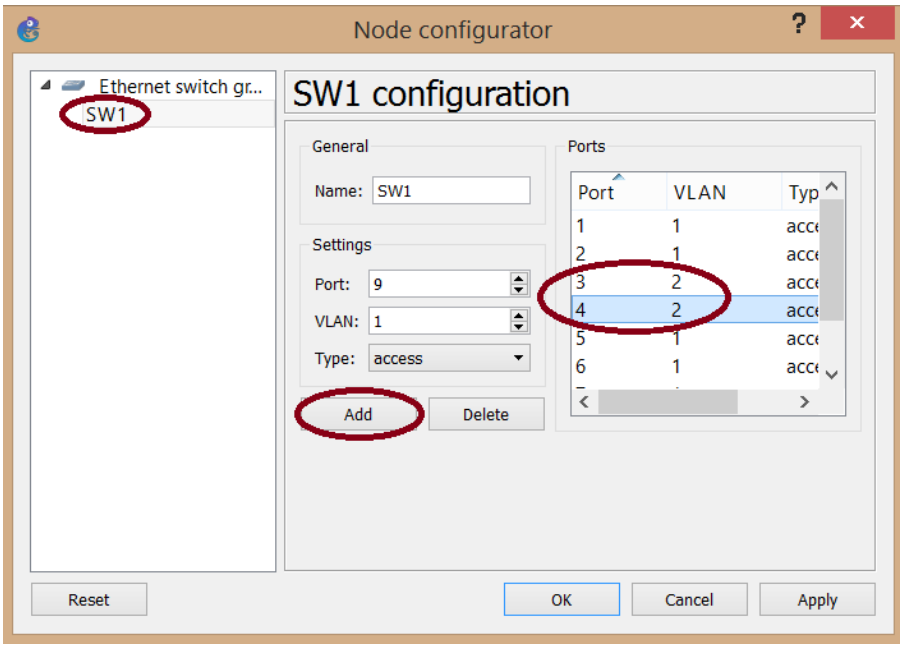


**Figure 4**: Configuring VLANs on an Ethernet switch

- Right-click on the switch, then click on **Configure**; a window appears. Click on **SW1** on the left pane (see Figure 4).
- Assuming PC3 and PC4 are connected to ports 3 and 4, change the VLAN of ports 3 and 4 to VLAN2 (you will need to click on **Add** to apply your modifications).
- Make sure that pings between PC1 and PC2 work.

- Now put all the PCs on the same network (`192.168.1.1-4/24`).
- Try to ping PC1 from PC2, then PC3 from PC1, then PC4 from PC2, then PC4 from PC3. How would you explain your findings?

## Part 4: Wireshark

Wireshark is a **packet sniffing** tool. It shows you the messages passing across a network link, and lets you explore their contents.

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 (see Figure 5) and click on **Start capture**. A window appears with a menu that has one option; click on **OK**. Then right-click again on the link and choose **Start Wireshark**.

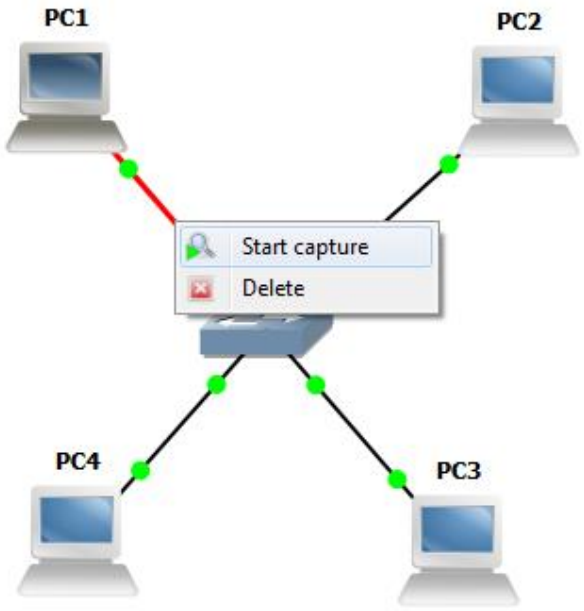


**Figure 5**: Starting capture on an interface

- Reconfigure PCs 1, 2, and 3 to be on the same network.
- Start a continuous ping from PC1 to 2 (by adding the `-t` option at the end of the ping command).
- Start sniffing on PC1's link using Wireshark. Which protocol is used for pings?
- Start sniffing on PC3's link using Wireshark. Can you see the pings from there? Why?
- Now replace the switch by a hub and try the previous steps in this part again. You now (really) know what the difference between a switch and a hub is!

## Submission and marking

When you have completed the exercise, submit your screenshots and notes to the Lab 1 assignment on Canvas (preferably as a single PDF file). You are allowed to submit multiple times.

We will go through these screenshots and answers with you individually in the lab and give you feedback on them.