Preparation for Lab3 & Lab4

Routing, Switching and Network Address Configuration
in Cisco Packet Tracer

Romaric Duvignau

February 8, 2023

Computer Communication Remote Lab
Department of Computer Science and Engineering,
with contributions and support from Hans-Martin Heyn,
Roman Melnik, Ali Salehson and Marina
Papatriantafilou.

CHALMERS

Network configurations in Packet Tracer

Packet Tracer is a Cisco free software that is used to simulate networks with different type of possible entities (routers, switches, PCs, laptops, smartphones, etc) that can be connected using different types of link (Ethernet, Wifi, Bluetooth, etc). Each entity can be customized (for instance installing additional network cards such as a bluetooth card on a PC) and configured using the usual network configuration tools (Graphical User Interface, command lines, etc). Hence, the tool reproduces with relatively good accuracy a "live" simulation of the corresponding network, sending packets between each entity in a similar fashion as what would have happened on a real-life network.

Goal: The goal of the lab is to learn and manipulate different network address configuration tools (IP addresses, subnet masks, etc) and to manipulate switches and Ethernet cables within the virtual environment offered by Packet Tracer.

Prerequisites: having completed the first lab (about Wireshark) and knowledge about IP configuration tools such as ip/ipconfig/ifconfig.

Reading: In **Chapter 4** of the course book, read especially **§4.3** about IP addressing.

Organization: After a short introduction about IP addressing, you'll install and do a test run of Packet Tracer. This preparation lab aims to take about 1h.

Contents

1 Introduction

Purpose

Lab3 and lab4 aim to understand how to address computers in a network, by building and configuring a local network with a number of PCs (*in a simulation tool*).

In the labs, you will be introduced to a basic configuration of an IP router that works with dynamic routing. You will also use the command programs **ping** and **tracert** as tools in the troubleshooting of TCP/IP-based networks.

In addition, you will create a network with a 24-bit prefix and an 8-bit host part that is with addresses of the form `aaa.bbb.ccc.ddd/24`. You will then configure two PCs to be connected to the other workplaces' PCs. You will proceed and divide the large network into several subnets.

Overview

The assignment should be performed according to the procedures outlined below with the use of the equipments provided in the virtual environment. The following tasks will be performed:

- Configuration of Windows PCs with connection to a peer-to-peer LAN.
- Building a larger network with several switches, and then applying IP subnetting.
- Running a number of commands to verify and diagnose the network.
- Use of *Packet Simulation and Inspection* to analyze and monitor local traffic.

At the end of the lab, you should be accustomed enough with network address configuration to set-up small to medium sizes **Local Area Networks** (LAN).

Preparatory Task 1. Try the following commands on your own system[a] which can be used for diagnosing a network: `ping`, `ipconfig`, `tracert` and `route`.

What do they do? Try to explain their functionality in words such that another student who has never seen the commands can understand what they do and why/when he/she would use it.

[a] For more details and macOS/Linux syntax, refer to the preparation instructions of Lab1.

Hint

These commands can be run on a Windows system (on Unix/Linux systems, **ip** or **ifconfig** and **traceroute** are used instead of **ipconfig** and **tracert**). More information about the commands can be obtained on Windows by hitting "F1" (help) on the desktop or by typing: for example, "**ping /?**" in a terminal window. On Unix-based systems, more information can be obtained from the on-line manuals: "**man ping**".

Local routing table

You can explore the routing table on your own machine. Try entering the commands "`route print`" (Windows) "`route`" (Unix), "`ip route`" (Linux or macOS with brew package iproute2mac), or "`netstat -r`" (Unix, now deprecated). Each row in the routing table you are seeing is telling "to reach a destination/netmask use next-hop (gateway) and packets are sent through this interface". This information is called a "route". As expected, at home your routing table will be very simple!

Tips

Don't be disappointed if the routing table of your host system at home is pretty simple, after all there is likely almost only one destination for all outgoing traffic!

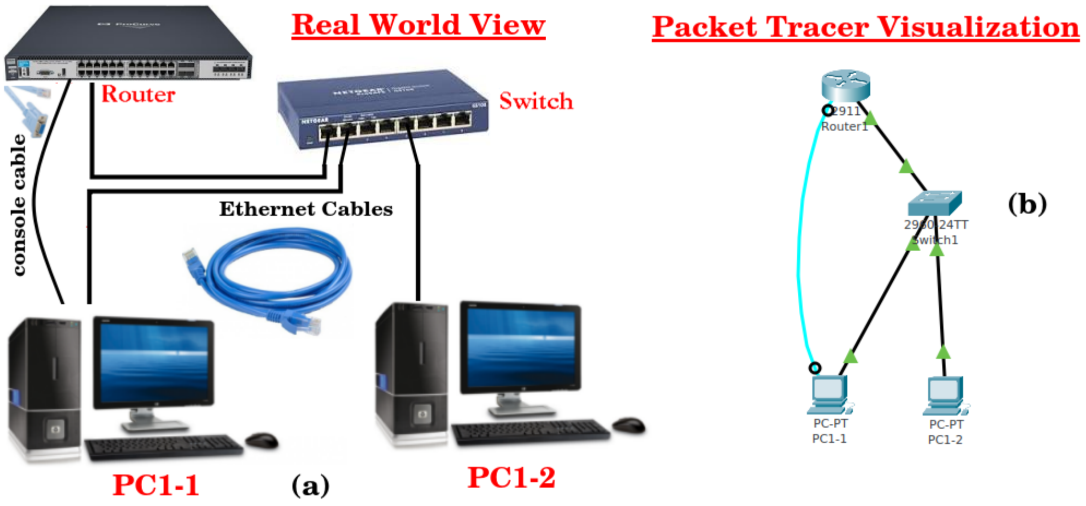


Figure 1: **(a)** "Physical" representation of each workspace: 2 computers connected to a switch, itself connected to a router; **(b)** similar set-up within the *Packet Tracer* network simulator.

The virtual lab room: 8 workstations

You will be working in a virtual environment that reproduces the configuration of the (historical) lab rooms at Chalmers. The room has 8 workspaces where each one has 2 workstations interconnected to a switch, itself connected to a dedicated router; all routers are then connected in a ring topology (i.e. they are interconnected while forming a ring). The equipment are working in a closed environment where the devices have no connection to the external world. The two PCs labelled **PCX-1** and **PCX-2** will be the computers used ($X \in \{1..8\}$). Figure 1 shows the equipments at every workplace in the virtual room and how the elements look like in Packet Tracer: the lines represent network links.

2 Packet Tracer: A Quick Tour

2.1 Installation

The first step is to install the Packet Tracer program, and before installing it, of course you need to download it first! The Packet Tracer program is free and can be obtained though Cisco NetAd official website after enrolling in the free course "Introduction to Packet Tracer": `https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer`. The course goes through all main functionalities of the packet tracer software and could be of interest to follow.

However, you might find it much easier to just go to the unofficial page "Computer Networking Notes" and download it from there: `https://www.computernetworkingnotes.com/ccna-study-guide/download-packet-tracer-for-windows-and-linux.html`, where you'll find download links for all main operating systems (Windows, Linux and macOS) and even small tutorials how to install it. You should hardly need such guides as you can install it by just executing the downloaded binary file and follow the usual installation procedure for your system, but you might want to check the ubuntu guide if you run into troubles.

Select the latest version of **Packet Tracer (7.3.1)** for your system and install it. Only one student per group needs to have it on her/his machine but it is better if all students have it, so to better organize the work in the group and alternate roles of manipulating and writing the report.

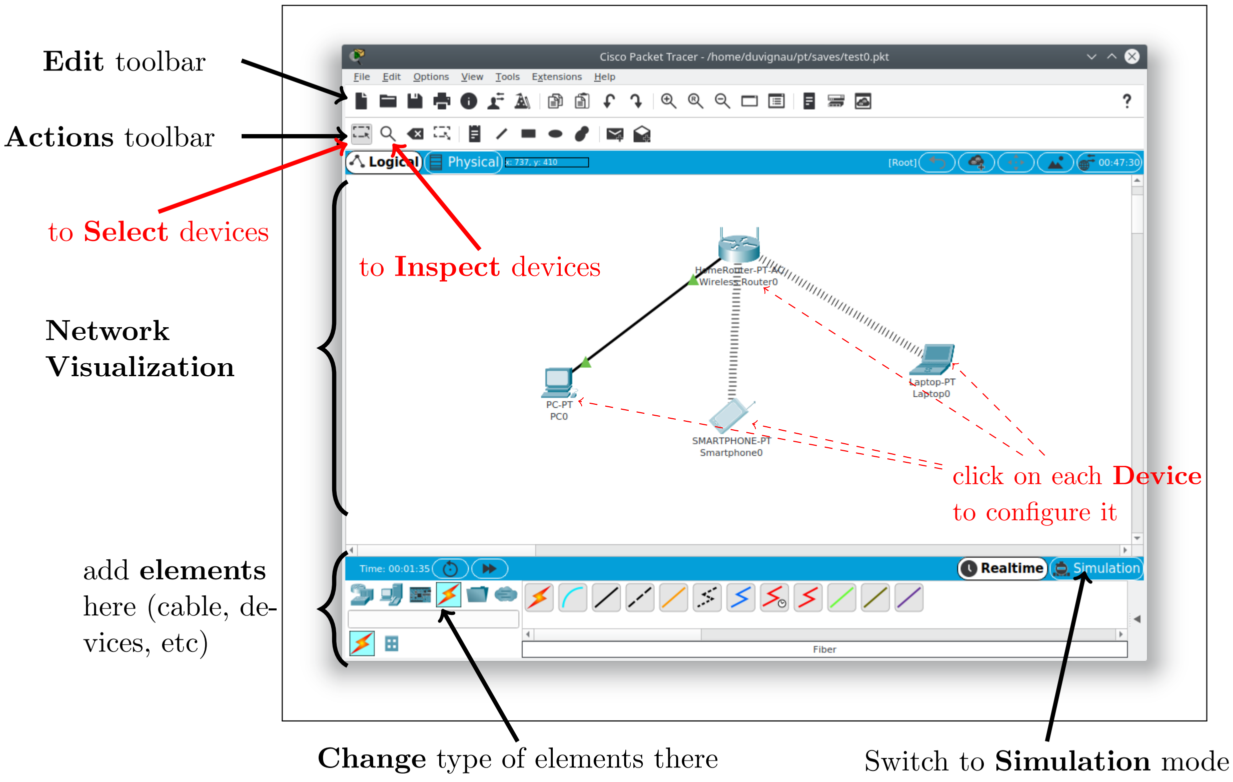


Figure 2: Tiny network displayed in Packet Tracer, Cisco's Network Simulator (v7.3.0).

2.2 Test run

Download the test file: go to `http://www.cse.chalmers.se/~duvignau/packet-tracer-lab` and download testfile.pkt, then open it with Packet Tracer[1]. After about 10-15 seconds, you will see the wireless links appear as in Figure 2. This is because every time a new file is opened, you need to wait that the system configures itself before the connections are established, as when you plug your home router at home!

2.2.1 On login: should I pick "NetAd Account' or "Guest Login"?

There are 2 options upon opening *Packet Tracer*: either you log in using a **NetAd account** or you pick the option **Guest Login**.

Guest Login: this option allows you to access Packet Tracer without using a NetAd account, but **you are limited to 3 saves in total**. To complete all mandatory parts of the lab, you **do not need** to create/use a Cisco NetAd account as there aren't any tasks forcing you to save your work. You can just click on *Guest Login* upon starting Packet Tracer, wait about 15 seconds then click *Confirm Guest*, and finally get access to the interface as shown in Figure 2. We will recommend 3 places to save your work after you have modified the provided network in the lab instructions so keep your saves possibilities for later if you are using a guest account.

NetAcad account: using a *NetAcad account* allows the user to save more than 3 times the current work in *Packet Tracer*, which can be particularly useful to any interesting students planning to use it beyond the lab, and more importantly Packet tracer will not bother you with a login prompt every time you open it! With a NetAcad account, you will also have access to

[1] The extension might be already associated with Wireshark on your system. In that case, just use "Open with..." in the context menu and pick the **packettracer** program.

the 10h online course "*Introduction to Packet Tracer*"[2]. Since, we will use only basic features of *Packet Tracer*, there is no need to follow the course, just register to it to get your free NetAcad account and feel free to de-register and delete your account at the end of the course.

2.2.2 Basic Interface

In Packet Tracer, the top bar below the menu contains classic edit operations (open, save, undo/redo etc) while the bar just below allows you to change the way you are interacting with the network (select, inspect, delete, resize, place note, etc).

The main window in Figure 2 shows a simple network of 3 devices and a router: a PC, a laptop and a smartphone, all connected to a home router. The PC is connected with an **Ethernet** cable while the laptop and smartphone use **Wifi**. By hovering over each device, you can see some useful information: for each of their interface, the MAC address and IPv4/IPv6 addresses associated with the interface.

Preparatory Task 2. Click on ***PC0*** → ***Desktop*** **Tab (top bar)** → **IP Configurations** → **turn DHCP on** instead of static IP. Wait a second, and check that PC0 has now indeed got an IP address!

Hint

You can access IP configurations the same way you will do it on your computer: through command-lines! Try with the freshly obtained IP address of **PC0**, by clicking on the device, then **Desktop** tab then **Command Prompt**[a], then try the famous `ipconfig`. Note that Packet Tracer's command prompt offers only a limited set of commands: you can obtain the list of all of them by typing "?" as a command. As usual, use ↑ to recover the last command executed.

[a] and not **Terminal** (the Linux name for the command-line interface program) that is something completely different!

Tips

Feel free to explore the interface a bit further before continuing (move the devices, etc).

2.2.3 Add/remove device and links

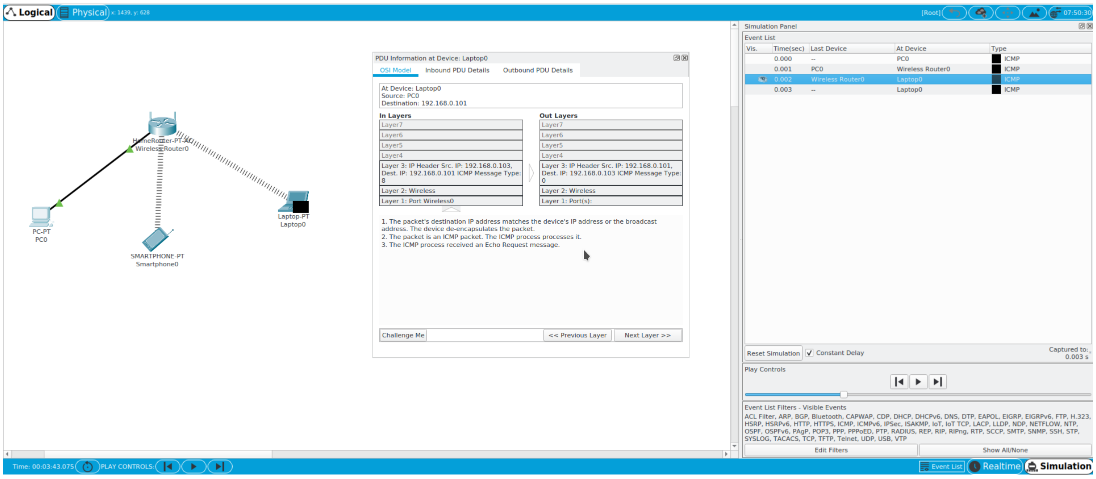
You can add devices in the lower left corner of Packet Tracer (cf. Figure 2). You will find PCs, Laptops and Smartphones (called *Smart Devices*) in the **End Devices** section, cables in **Connections** and the home router can be found in **Network Devices** → **Wireless Devices** → **Home Router**.

Preparatory Task 3. Add a new PC to our home network and connect it to the home router using an Ethernet cable (in a similar way as PC0). Test the connectivity by pinging it from *Laptop0*.

Hint

You need to pick the right interface on each entity (FastEthernet for the new PC and GigabitEthernet for the home router) and don't forget that, similarly to PC0, **your new PC also needs an IP address on its own**!

[2] https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer.



PDU Information at Device: Laptop0

OSI Model | Inbound PDU Details | Outbound PDU Details

At Device: Laptop0
Source: PC0
Destination: 192.168.0.101

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.0.103, Dest. IP: 192.168.0.101 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 192.168.0.101, Dest. IP: 192.168.0.103 ICMP Message Type: 0
Layer 2: Wireless	Layer 2: Wireless
Layer 1: Port Wireless0	Layer 1: Port(s):

1. The packet's destination IP address matches the device's IP address or the broadcast address. The device de-encapsulates the packet.
2. The packet is an ICMP packet. The ICMP process processes it.
3. The ICMP process received an Echo Request message.

Challenge Me | << Previous Layer | Next Layer >>

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	■ ICMP
	0.001	PC0	Wireless Router0	■ ICMP
👁	0.002	Wireless Router0	Laptop0	■ ICMP
	0.003	--	Laptop0	■ ICMP

Reset Simulation ☑ Constant Delay Captured to: 0.003 s

Play Controls

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters | Show All/None

Figure 3: Packet Tracer Simulation mode: inspection of an ICMP packet at *Layer 3*.

Tips

Important trick: to copy-paste IP addresses in packet tracer, click on the magnifying glass (inspect button, cf. Figure 2), then "Port Status Summary Table" then you can select the IP address and right-click "Copy"; then you can use right-click "Paste" in the command prompt.

At last, to delete devices, use the **Delete** action next to Inspect in the action bar, or press **Del** key. You will be able to delete devices and cables that way, to remove wireless links you can turn off their interface (eg for the smartphone, **Config** → **Interface** → **Port Status** → **On/Off**).

2.2.4 Simulation Mode

Packet tracer can work in a *simulation mode* which will let you see packets being transferred. This mode will allow you to inspect "capture" and "inspect" packets in a similar fashion as in Wireshark but here, since it is a simulation, we will be able to see packets in the full network and not only on one host. Do the following:

- Open the *Simulation Mode* by clinking on **Simulation** in the bottom right of Packet Tracer (see Figure 2). Go to **Edit Filters** and uncheck **IPv6** → **NDP** and **Misc** → **STP & DTP** to reduce the number of displayed packets.
- **Ping** the smartphone from PC1 (remember **Command Prompt** is in the **Desktop** tab, the above trick to quickly copy-paste IP addresses and don't forget that the smartphone has a local IP address on the LAN and another IP for its 3G/4G interface).
- Use the ⏭ button in the *simulation panel* to jump to next simulated packet. Generate packets till PC1 receives a first answer. Note how ICMP messages were sent to everyone before ARP's tables were updated and how packets transmitted on wireless links are sent to everyone (shared link).
- Use the sliding bar to change animation speed and ▶ to have the simulation automatically progressing to next packet, and observe now the ping command terminates (4 answers) and packets being sent and received (you may need to go to window mode to be able to have both packet tracer main window and the command prompt displayed at the same time).

Tips

On a device, to **Quit** the current program in the **Desktop** tab, click on the cross at the right of the program's name (top bar).

To inspect particular packets in the simulation panel, click on the packet in the **Event list** (you may click actually anywhere on the packet's line). To obtain the information you want, you may need to look at different layers so use the **Next Layer** button when inspecting a packet in the simulation panel and

Preparatory Task 4. What is the reason *Laptop0* dropped the ICMP ping packet coming from PC1?

Hint

In the packet list, click on a ICMP packet (black packets in the list) where *Laptop0* is in the column "At device", then click a few times on **Next Layer** and you'll find the reason why the packet was dropped.

To come back to the normal mode click on "**Realtime**" just next to the simulation button; the simulation is then reset.

3 Practice IP addressing

Let us first make an example of network partitioning. Consider the following task.

Preparatory Task 5. Assume hypothetically that you are given an address subspace denoted by 200.150.100.0/24, which will be used later on to configure the local network in the lab.

(a) Write the IP in binary.

(b) What would be the class for the network address 200.150.100.0/24 according to the classful scheme?

(c) What is the subnet mask in decimal notation?

Hint

IP addresses can be divided into 5 classes:

- Class A: Addresses starting by 0, subnets of 8 bits (16,777,216 host addresses).
- Class B: Addresses starting by 10, subnets of 16 bits (65,536 host addresses).
- Class C: Addresses starting by 110, subnets of 24 bits (256 host addresses).
- Class D: Addresses starting by 1110. Reserved for multicast groups.
- Class E: Addresses starting by 1111; Reserved for future use.

Refer to your course book pages 366-367 for more details.

Tips

The subnet mask is traditionally expressed in dot-decimal notation, for example the IP prefix `198.77.48.0/23` has 23 bits allocated for the network prefix and 32-23 = 9 bits allocated for the host part of the address, and in this case the subnet mask being `11111111.11111111.11111110.0000000` becomes in dot-decimal notation `255.255.254.0`.

So the answers to the previous task are:

1. `200.150.100.0` written in binary gives `11001000.10010110.01100100.00000000`.

2. According to classification of IP addresses in different classes, this is an IP address of class C (starting by 110), it is meant for being used with subnets of 24 bits allowing up to 256 hosts.

3. The subnet mask in dot-decimal notation is `255.255.255.0` as the first 24 bits should be set to 1 and the last 8 bits are set to 0. The subnet mask allows to apply a quick bitwise and "&" operator to the address to get the network part of the address.

In order to practice subnetting, perform the following tasks as a preparation before starting the mandatory parts:

Preparatory Task 6. A network has been given the CIDR block `198.77.48.0/23`, so that IP addresses within the block should be be assigned to hosts/interfaces connected in the network. Assume that the network is divided into four equal-size subnets.

(a) How many host addresses will be available for each subnet?

(b) Give in order the IP address of each of these four subnets.

(c) What is the subnet mask?

(d) Give the range of IP addresses of the second subnet in order.

Tips

When we say "smaller IP" or "in order" for IP addresses, the leftmost number (first 0-255 number in an IP address) is checked first (most important), then the second if they are equal, then third and finally fourth. For example `1.2.3.4` < `2.255.255.255` < `3.0.255.0` < `3.1.0.3` < `3.2.0.2`...