Universität Zürich[UZH]

0690 - Communication Systems Lab Course

Exercise 1

1) Introduction
2) Cabling
3) Wireshark

September 20, 2022

Assistants: Christian Killer, Jan von der Assen, Dr. Alberto Huertas

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH—8050 Zürich, Switzerland

1 Introduction

This course will consolidate and deepen your understanding of computer networks. With practical tasks that mostly solved through the terminal on a unix shell, you will gain insights to different technologies, protocols, and applications that are crucial for computer networks and in particular, today's internet infrastructure. More precisely, this course touches upon some of the following areas:

- Networking basics
- LAN configuration and Setup
- Routing
- Domain Name System (DNS)
- Information Security, Web Application Security, Wargames and Firewalls
- IPv6
- Blockchain Basics and Smart Contracts Basics
- Container Networking

1.1 Organization

The communication systems lab course consists of eleven exercise sessions that contain several tasks dedicated to one of the topics outlined above (but not limited to). The lessons procure practical experience, as the solution of the exercises requires close interaction with the Linux system, mostly by shell commands. Students form groups of 2 to work on the exercises with the technical setup that is described in the subsequent section. On the 12th exercise session, each student will give a talk of 15 minutes on a topic discussed during the semester, thus demonstrating the knowledge gained during the course.

1.2 Topology

As shown in Figure 1, each group will get two Linux machines with multiple network interface cards. Students can connect to the lab network by connecting the machines to the RJ45 plugs in the wall. From there, the machines are connected to the lab router via a switch. This router provides the uplink to the internet and basic networking services like DHCP and DNS.

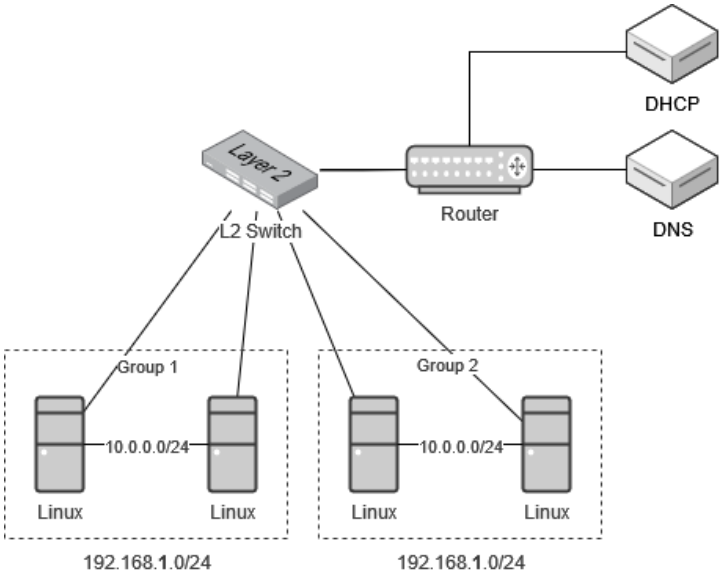

Figure 1: Topology of the Lab Infrastructure

2 Cabling

The goal of the first task is to manufacture an Ethernet cable that allows a direct connection between the two Linux machines. To create the cable, the tools shown in Figure 2 are needed.

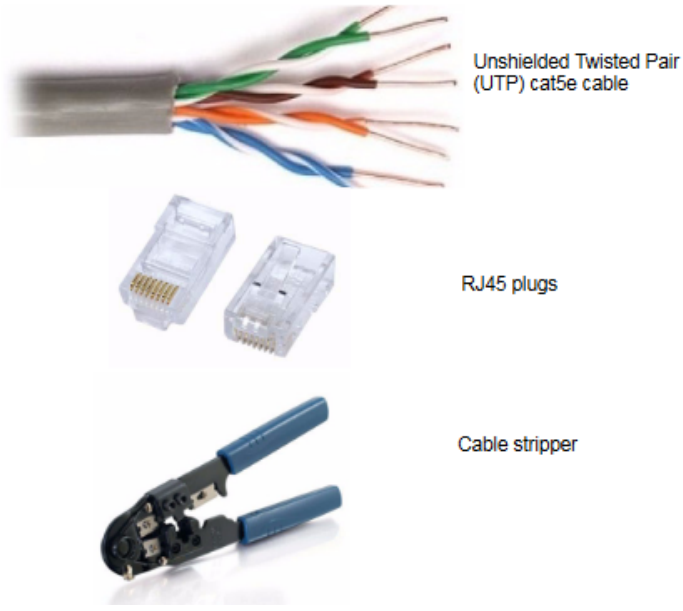

Figure 2: UTP Cable, RJ45 Plugs and Cable Stripper

In order to manufacture your cable, follow these steps:

1. Considering the two possible ways of ordering wires for your cable as shown in Figure 3, do some initial research online to figure out which order is required.
2. Cut as much cable you need in order to connect your machines.
3. Carefully remove approximately 12 mm of the outer shell of the cable. There are 4 pairs of wires (white-orange and orange, white-green and green, white-blue and blue, white-brown and brown). Name this side of the cable side *A*.
4. Order wires based on their color according to Figure 3 depending on usage and make sure that all wires have the same size.
5. Hold the RJ45 plug with the clip side facing down and number pins from 1 to 8 starting from the left side.
6. Carefully place all wires in the RJ45 plug, keeping the same order of steps 3 and 4.
7. Place the RJ45 plug in the stripper and press it hard.
8. Repeat the previous steps for the side *B* of the cable.
9. Check the cable with the two Linux machines. *Hint:* The LEDs on the network interface cards may help you determine if your cable is working as intended or faulty.
10. Pick a private subnet (*e.g.,* see Figure 1) for the point-to-point link you just created between the two devices, and configure it on both machines. Test that the connection works by `ping`-ing one machine from the other one.

Type	**straight-through**		**cross-over**	
Side	**A**	**B**	**A**	**B**
1	white-orange	white-orange	white-orange	white-green
2	orange	orange	orange	green
3	white-green	white-green	white-green	white-orange
4	blue	blue	blue	blue
5	white-blue	white-blue	white-blue	white-blue
6	green	green	green	orange
7	white-brown	white-brown	white-brown	white-brown
8	brown	brown	brown	brown

Figure 3: Wire Order for Straight-through and Cross-over Cables

2.1 Questions and Tasks

Please answer and document the following questions.

- What is the bandwidth and what the most common use of the Cat5e UTP cable?
- What is the difference between a Cat5 and a Cat5e cable?
- When do we use which wire order (*e.g.,* straight-through and cross-over)? Are theses orders required by today's standards?
- Document your output of the ping command and the configuration steps you applied.

3 Wireshark

Wireshark is a network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. First, install Wireshark by (1) ensuring you have internet access and (2) then running `sudo apt-get update && sudo apt-get install wireshark`. In order to start capturing packets, run Wireshark with elevated privileges and choose the right interface to capture packets on, as shown in Figure 4.

Figure 4: Wireshark Interface List

3.1 Wireshark Fields

There are five fields on the Wireshark screen, which you can see on Figure 5. Each field groups a set of actions. Find a brief description of the fields in the next subsections.

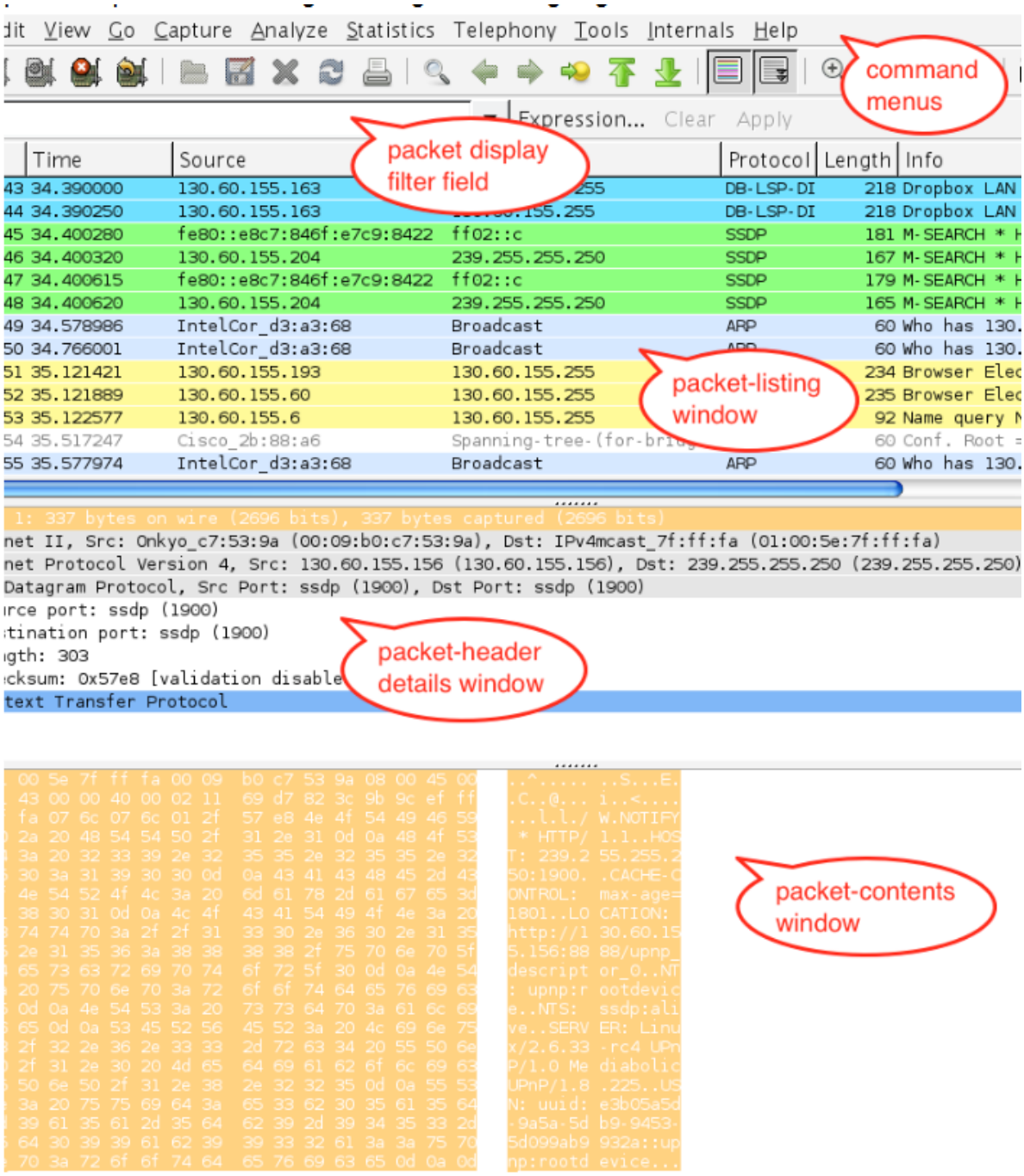

Figure 5: Wireshark Overview

3.1.1 The Command Menu

The command menu is placed on top of the screen and contains the usual File, Edit, View options. For now, please focus on the File and Capture option. In the File menu you can find an Open sub-menu where you can open previously saved packet captures if needed. On the Capture menu, you can begin and stop packets capturing.

3.1.2 The Packet Display Filter Field

The packet display filter field allow the user to add some constraints concerning the packets presented or captured. Spend the next 10 minutes to read the basic filters described in the manpages[1] and get familiar with the format of filters expressions.

3.1.3 The Packet Listing Window

The packet listing window field presents in each line a short information summary of each packet captured concerning incoming and/or outgoing traffic.

3.1.4 The Packet Header Details Window

In this field, all the fields of each packet's header in the full protocol stack are presented. Thus, this field is one of the most important, and it will be heavily used during this course.

3.1.5 The Packet Contents Window

The packet contents window presents in ASCII and hexadecimal format the content of a frame. This field will not be used that much during this course.

3.2 Examples

In the following Figures, there are two examples of the packet display filter, the packet listing window and the packet header details window. Note that in Figure 6 in the packet display filter window there is an `http` tag, so only packets that are related to the HTTP protocol are being displayed in the packet listing window. On the packet listing window, you can see a `GET` message request from the IP 130.60.155.221 to the IP 130.60.127.170. In the packet header details window, under the HTTP header details, you can see that the site that was visited was the main web page of the University of Zurich on URL www.uzh.ch and that the browser that was used was Safari.

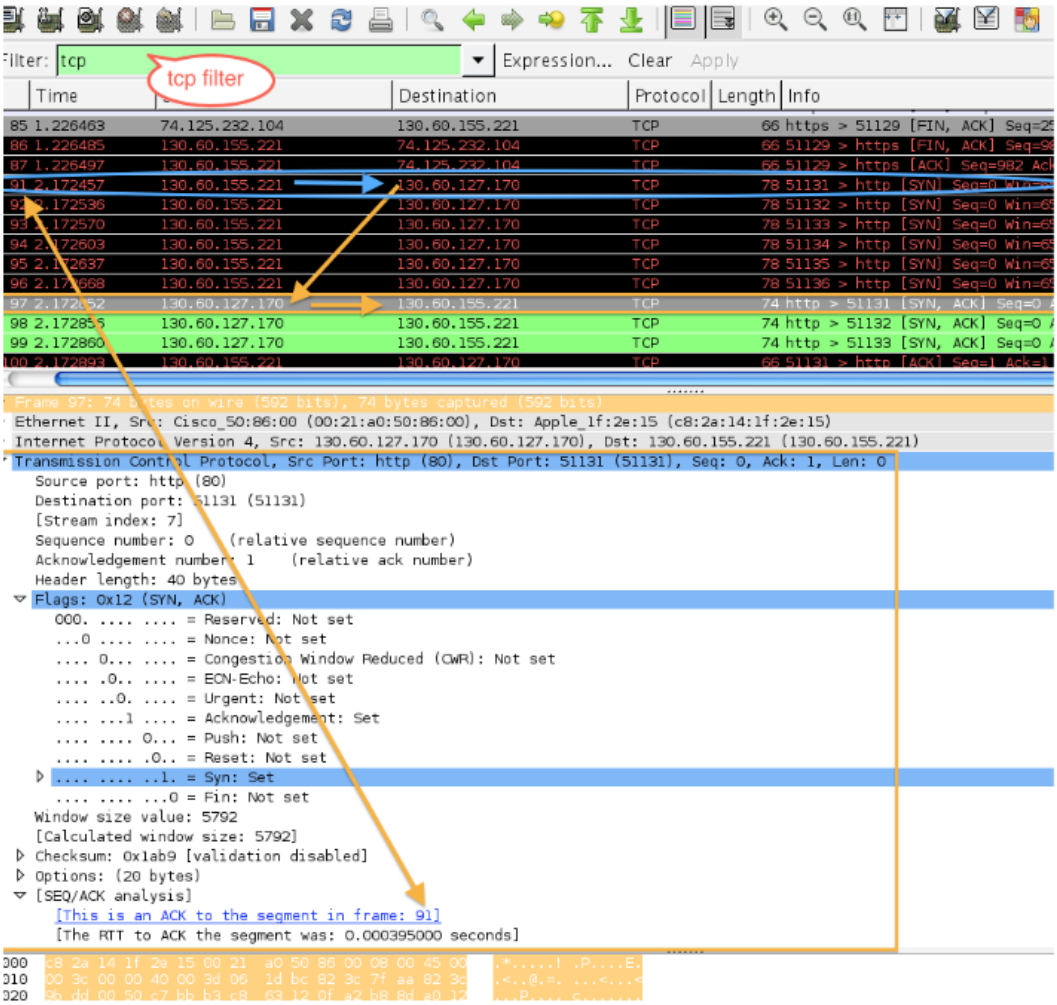

Figure 6: Wireshark TCP Filtering

In Figure 7 the filter that is applied in the packet display filter is a `tcp` tag. Thus, only packets that use the TCP protocol are displayed in the packet listing window. Observe the three-way handshake procedure between 130.60.155.221 and 130.60.127.170.

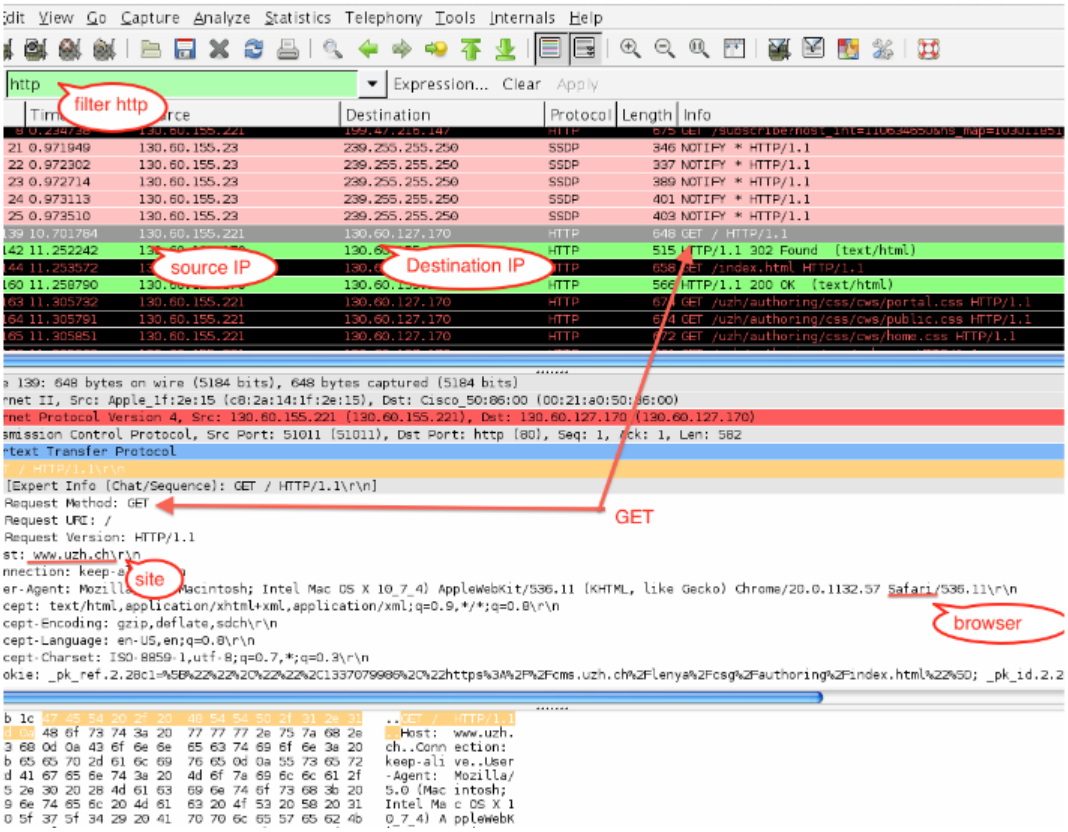

Figure 7: Wireshark HTTP Filtering

3.3 Questions

Please document your answers to the following questions:

1. Assume that your IP address is 10.0.0.1, and you are visiting a web page hosted by 10.0.0.2 what is the display filter that will show only traffic between those two machines irrespective of the protocol used?

2. Craft a filter, such that you can display only packets with source address the IP of the server that hosts www.uzh.ch and as destination your IP address. Begin the capturing procedure in Wireshark. and then open a browser and visit www.uzh.ch. In the first SYN, ACK package expand the TCP properties. What is the TCP header size? What is the maximum segment size defined in options? Now expand the IP properties. What is the version and the Time-to-live (TTL) of the IP package?

3. While capturing packets, keep the filter of the previous question and add another rule so only Internet Control Message Protocol (ICMP) packets will appear. What is the filter you applied? Now, ping the IP of the server that hosts www.uzh.ch and. What is the total length of the IP packet? What is the IP header length, and finally, what is the ICMP data length?

References

[1] wireshark. wireshark(1) manual page. https://www.wireshark.org/docs/man-pages/wireshark.html. Accessed: 19.09.2022.