Network Laboratory

Ruizhi Liao, Alex Bikfalvi, Jaume Barcelo

January 29, 2013

Contents

Chapter 1

About the course

1.1 Course Data

Code: 21728

Course name: "Laboratori de Xarxes i Serveis"

Teachers: Ruizhi Liao, Alex Bikfalvi and Jaume Barcelo

Credits: 4

Year: 2nd year

Trimester: Spring

1.2 Introduction

The goal of this course is to acquire hands-on experience with networking equipment such as access points, switches, routers and firewalls. The students are assumed to be familiar with the high-level functionality of each of these devices. Nevertheless, the actual configuration of the equipment and the construction of prototype networks will provide further insights on the operation of network devices. After the course, the student

will be ready to plan and configure a small network.

1.3 Syllabus

- Lectures
    1. Introduction to the Networking Laboratory
    2. Traffic analysis and IEEE 802.11 WLANs
    3. Virtual Local Area Networks and Spanning Tree Protocol
    4. Routers
    5. Firewalls
- Lab Assignments
    1. Traffic analysis
    2. IEEE 802.11 Wireless Local Area Networks (WLANs)
    3. Virtual local area networks (VLANs)
    4. Spanning Tree Protocol (STP)
    5. Routing
    6. Firewalls

1.4 Bibliography

TBD

1.5 Evaluation Criteria

The grading is distributed as follows:

- Lab assignments, 70%
- Continuous assessment quiz, 10%
- Final exam, 20%

It is necessary to obtain a decent mark (half of the available points) in all the different evaluation aspects.

1.6 Lab Report

For each lab assignment, it is necessary to prepare a lab report answering all the questions. The students are also expected to include additional information, explanation and comments besides those explicitly asked in the assignment.

1.7 Survival guide

1.7.1 Questions and doubts

We like to receive questions and comments. Normally, the best moment to express a doubt is during the class, as it is likely that many people in the class share the same doubt. If you feel that you have a question that needs to be discussed privately, we can discuss it right after the class.

1.7.2 Continuous feedback

At the end of lectures, we will ask you to provide some feedback on the course. In particular, we always want to know:

- What is the most interesting thing we have seen in class.
- What is the most confusing thing in the class.

- Any other comment you may want to add.

1.7.3 How to make you teachers happy

Avoid speaking while we are talking.

Chapter 2

Traffic Analysis

2.1 Introduction

The goal of this lab assignment is to know and use monitoring and traffic analysis tools. *Wireshark* and *tcpdump* will be used to study different layers of the TCP/IP architecture.

2.2 Preparation at home

Review the TCP/IP model and explain the function of each layer. Provide examples of the protocols at each layer of the protocol stack.

What is the purpose of ARP? Draw a sketch of the different messages being exchanged and the different steps involved. Is it possible to run this protocol between computers that are in different local area networks (LANs)?

What is the ICMP protocol? How does the *ping* command work? What does the *ping* command measure?

Explain and draw an SSL connection indicating how the protocol works and which messages are being exchanged.

2.3 WireShark Network Analyzer

Start the WireShark software and choose the right network interface. The option Capture/Interfaces starts the packet capture. It is also possible to configure the length of the capture and other details. What interface does WireShark detect? What is your IP address? And the corresponding MAC?

Configure the Capture/Interfaces options to perform a five minutes capture. Observe the results and answer the following questions:

What is the total number of captured packets? Are there lost packets? If yes, why?

Choose any packet. Observe the details and answer the following questions: What is the source and destination IP address? What are the source and destination MAC addresses? What is the number of bytes in the packet? What protocols can you see in the packet? Is there HTTP? If yes, what is the length of the HTTP message? What are the source and destination port?

In the menu "Analyze option/Enable protocol" it is possible to configure the protocols that WireShark will capture and show. Looking at the default protocols, find at least one protocol of each of the four upper layers of the TCP/IP stack (Application/Transport/Internet/Link). Include a brief description of the protocols you found.

Go to the menu "Statistics/Protocol Hierarchy" and observe the percentage of the following protocols: Ethernet, Internet Protocol, TCP, UDP, Logical Link Control, ARP, STP, IPv6, HTTP.

What are the differences between IP and IPv6?

2.4 the ARP protocol

The Address Resolution Protocol (ARP) protocol resolves the association between an IP address and a MAC address. It is used in IP over Ethernet networks. Capture traffic and analyze the ARP packets. You can filter the ARP packets writing "ARP" in the "Filter Toolbar".

What are the source and destination MAC addresses of the Ethernet frame that contains the ARP request message? Can you see the source and destination IP addresses in the ARP request frame?

Look for an ARP request-reply exchange and write the source and destination MAC and IP addresses.

Whats the time elapsing between an ARP request and reply messages?

Use the information available in WireShark to indicate the length of the ARP frames and draw the format of the messages.

To which layer does ARP belong?

2.5 HTTP and secure HTTP

Make a new 5 minutes capture and during this time visit a few webpages. After the capture is finished observe the different HTTP and HTTPS messages. Use the filter toolbar to filter the messages.

Observe an HTTP GET message and the corresponding response and answer the following questions:

What is the HTTP version of your web browser? And the HTTP version of the server? What language does the client request to the server?

Is it possible to find which are the URLs visited by the

user? At which layer is this information available?

The default destination port for web is 80. What is the source port of the get requests? Write the source number for different connections. At which layer can you find this information?

Find a DNS query/response pair. What is the function of DNS?

Use the option "Analyze -¿ Follow TCP Stream" to analyze a TCP session. Identify the three-way-handshake and the session tear-down.

If http is used, it is possible to observe the contents of the web using WireShark?

Now use HTTPs. Is it still possible to read the information that is being transmitted? (Look for SSL packets).

Identify a SSL handshake in WireShark.

2.6 ICMP-ping packet capture (Homework)

Close all the applications that use the network and ping four different webs in four different continents. Analyze the results.

What protocols are being use? Draw a frame and explain how the different packet are encapsulated in each other.

How many ping messages are transmitted by default?

Prepare a table with the source, destination, and average packet delay of the four different ping experiments.

What packet length is being used?

At which layers can we find source and destination addresses? Which kind of addresses?

Are the ping packets sent uniformly in time? What about

the answers? What are the reasons for different inter-arrival times for the answers?

What information is included in the data field of the ICMP packets? What about in the reply messages?

2.7 tcpdump

In this section we will use the tcpdump command in linux. Use "man tcpdump" to learn about the different parameters and options. With tcpdump it is also possible to filter the traffic according to the source or destination addresses, protocol, port number, etc.

Open a terminal and launch a tcpdump capture. Finish the capture using "Ctrl-C". What is the information provided by tcpdump and which format is being used? To which level does the information belong? (Remember that you can redirect the output using $ tcmpdump > my-file).

The first line of tcpdump specifies which interface is being used and it can be changed using the -i option. What interface are you using?

Describe the information provided for the ARP protocol (tcpdump arp).

Execute the same command again using the -e flag. Whats the difference with respect to the previous execution? Check the tcpdump manual if necessary.

Try new captures related to this assignment, such as "tcpdump stp", "tcpdump http", "tcpdump http", "tcpdump udp", "tcpdump ssl", "tcpdump ip", etc. Try also to make captures for a specific IP address.