Network Laboratory

Ruizhi Liao, Alex Bikfalvi, Jaume Barcelo

February 5, 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 should be familiar with the high-level functionality of each of these devices. However, the actual configuration of the equipment and the construction of prototype networks will provide further insights into the operation of these 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 final grade is distributed as follows:

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

The students need to obtain a passing mark (half of the available points) in all the different evaluation aspects.

1.6 Group Work

The assignments are done in groups of three students. A single report is delivered for each group. It is important that all the members of the group participate in the experiments and the preparation of the report. The teachers may ask individual questions to the students in the labs, and the both the quiz and the final exam are performed individually.

1.7 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.

1.8 The Lab

The networking lab has PCs, wireless access points, switches, routers, firewalls and a patch panel to make the connections. The password for the computers is "pompeulab". The root password for linux is "root_labx".

1.9 Survival guide

1.9.1 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.

1.9.2 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.

1.9.3 How to Make Your 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. We shall use the *Wireshark* and *tcpdump* software tools to study different layers of the TCP/IP architecture.

2.2 Home Preparation

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 Disable your local firewall

On a Linux machine, your local firewall can interfere with the assignment. Disable it using the command `service iptables stop` with root permissions.

2.4 WireShark Network Analyzer

Start your computer in Linux. Start the WireShark software program and choose the correct network interface from the *Capture* > *Interfaces* dialog. Use it to start 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? What is the corresponding MAC address?

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?

Select a (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 (the payload of the TCP segment or segments)? What are the source and destination port?

In the dialog *Analyze > Enable Protocols...*, it is possible to configure the protocols that WireShark will capture and display. 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.

Include IPv6 practice with a ping to the local-link IPv6 address of a neighbor. Use: `ping6 -I iface addr` **or a failed ping to** `ping6 ipv6.google.com`**.**

What are the differences between IPv4 and IPv6?

2.5 The ARP Protocol

The Address Resolution Protocol (ARP) 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?

Clear the ARP cache `sudo ip neighbour flush all`**.**

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

What is 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?

2.6 HTTP and Secure HTTP

Make a new 5 minutes capture and during this time visit a few web sites. 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.

The filter for HTTP or HTTPS should be `http or ssl`.

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 or 8080 when using a web proxy.

What is the source port of the get requests? Write the source port 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? Hint: look for SSL packets.

Identify a SSL handshake in WireShark.

2.7 ICMP Ping Packet Capture (Homework)

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

What protocols are used?

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 is the packet length? 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?

2.8 tcpdump

In this section we will use the `tcpdump` command in Linux. Use `man tcpdump` to learn about the different parameters and options of this command. 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? Hint: remember that you can redirect the output using the command `$ 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` option. What is the difference with respect to the previous execution? Check the `tcpdump` manual if necessary.

Try several 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.

Chapter 3

LAN and WLAN

3.1 Home exercise

Connect to the web configuration interface of your home access point and find:

- The name of the wireless network (SSID or ESSID).
- Frequency channel.
- PHY layer data rates.
- Supported security protocols.
- Possibility of QoS differentiation.

Do a survey and find the information of available wireless networks (name, channel, security settings). You can use Netstumbler or the command "sudo iwlist wlan1 scan".

3.2 Equipment

Each group requires at least two PCs. If possible, three PCs are better than two. Boot one PC in Windows and the other one in Linux. The hardware you are going to use is the Cisco Aironet 1200 access point. The user guide can be downloaded here: http://www.jaumebarcelo.info/teaching/lxs/wlan/WLAN_manual.pdf The firmware of the access point is CISCO IOS Version 12.3(8)JA2.

Install an FTP server in one of the computers (e.g., *Filezilla* in Windows or *vsftpd* in Linux). You may use a web browser as an FTP client.

On Windows Install and open Filezilla, and connect locally from the same PC using the loopback interface 127.0.0.1. Create a new user (username `test` and password `test`) and share a local folder with several large files. Do not forget to remove the proxy configuration, or select not to use a proxy server for local addresses.

On Linux Install *vsftpd* with the command line `sudo yum install vsftpd`. Once installed, you can find and modify the FTP server configuration in the file `/etc/vsftpd/vsftpd.conf`. If you need to change the configuration, do not forget to restart the FTP server with the command `sudo services vsftpd restart`. The server allows by default anonymous access, and therefore you do not neet to create a new user. The default shared folder is `/var/ftp`.

3.3 Disable your local firewall

On a Linux machine, your local firewall can interfere with the assignment. Disable it using the command `service iptables stop` with root permissions.

3.4 Basic LAN Configuration

Interconnect the windows box and the Linux box using a cross-over cable. — ask Jaume Check layer-2 connectivity using the LED or the `mii` command in Linux. Check layer-3 connectivity and measure round-trip-time using ping. Configure the interfaces if needed. Estimate the available bandwidth using FTP transfer or iperf. Change the speed to 10 Mbps (full duplex) and estimate the bandwidth again.

Is the maximum transmission speed reached? Why?

3.5 WLAN Basic Configuration

WLANs can be used as an access point to LANs. They can also be used to interconnect to LANs using WDS.

First connect the AP to the PC using Windows. This can be either a direct connection or a connection using the patch panel. You will find the AP's IP on a post-it, and the administrator user is `Cisco` and the password field is `Cisco`.

Use the express set-up to configure the AP. AP Name: LABXARXES_GRUP_XX. SSID: grupXX. Channel: default. Transmit power: default.

Make sure that the radio interface is up. Indicate what are the security options available. Try different settings and configurations and then connect the AP to the laboratory switch.

Connect the WiFi interface to the Linux box and connect the computer to the AP that you have just configured. Disable the wired interface in order to make sure that you are using the wireless interface. Check that you have network connectivity and use the `ifconfig` or `ipconfig` command to look at the interface configuration.

If you have network connectivity, you should be able to ping the other computers of your group (the ones with wired connection) and also be able to connect to the Internet.

Perform measurements from the wireless computer to the wired one and the other way around. Measure the round-trip-time using ping. Also the throughput using FTP to

transfer a large file. *Can you reach the PHY rate maximum throughput? Why?. Do you observe the same values for the uplink and downlink?* Write down any other observations you find interesting.

Use either "Netstumbler" or "iwlist" to detect the available wireless networks. Write down their configuration.

Draw a sketch of the computers, access point and other networking devices in your setting.

3.6 Hot-Standby

The hot-standby is a feature to offer high availability. A backup AP (AP-standby) takes over if the primary AP (AP-root) fails.

Collaborate with another group. One of the groups will configure the AP-root and the other the AP-standby. Make sure that you replicate the same configuration (with the exception of the IP address) in both devices. Same SSID, same network mask and same security setting.

In the AP-root, go to "Network Interfaces", "Radio 802.11g", and select "Access Point (Fallback to radio shutdown)".

In the AP-standby select "Services", "Hot Standby". Click enable and specify the MAC address that the AP will be monitoring (the radio interface of the root-AP). If the configuration is correct, you should be able to see the status that will appear below on the screen.

Draw a sketch of all the involved network devices and connections and test that it actually works. To test that it is working, disable the radio interface of AP-root ("Network interfaces","802.11g","settings"). After the time-out expires, the AP-standby takes over with the same SSID and security settings.

To gather more information about what is going on, you can run ping tests while the takeover takes place. You can also check the logs in the "Home" page of the AP configuration interface. Finally, you can check the log of the Filezilla server.

How long does it take for the PC to recover the connection after AP-root's radio is disabled? Will the user notice that the connection switches from one AP to the other? How? Do you think that the default time-out setting are appropriate? Why? How is the network affected if we change this parameters?

Now re-enable the radio interface of AP-root. Then, at the AP-standby, click "Restart". Check the information that appears in the "Home" page of the APs to determine to which AP is the client connected.

After you have verified that the client is connected to the AP-root device, disconnect the ethernet cable of AP-root. *What happens? Does the AP-standby take over? Why?*

3.7 Configuring an AP as a Repeater

A repeater AP is not connected to the wired LAN. It is situated within the coverage range of another AP to extend the covered area. Just in the previous exercise, both APs must share the same configuration (with the exception of the IP address).

In the AP-root, select the option "role in radio network" and then choose "access point". In the AP-repeater (former AP-standby) disable the hot-standby option. Configure the SSID and at the end of the page select "Set Infrastructure SSID". In the "express setup" select "Repeater" in the option "role in radio network".

At this point, your home screen should show the configuration of your network and the repeater, and the clients connected to each AP. Your client is probably connected to the AP-root. Click on "clients" and you will see the list of associated clients. You can de-associate a particular client if you select it. The client will automatically re-connect to the repeater.

To verify that is working, repeat the round-trip-time and bandwidth tests that you have performed before. Do the tests while connected on AP-root and AP-repeater. *Can you observe any difference?* Repeat the ping tests while a file is being transferred.