Network Laboratory

Ruizhi Liao, Alex Bikfalvi, Jaume Barcelo

February 14, 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 [**?**, rfc827]*

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 and pay attention to your browser

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

If you decide to use firefox to connect to the AP during the assignment, it might be necessary to disable the proxy settings and to uncheck the "offline navigation".

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 "Security" > "SSID Manager" select "Set Infrastructure SSID" (choose the current 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.

Chapter 4

Virtual LANs (VLANs)

4.1   Switch user manual

The user manual for the switch is available here:

   http://www.jaumebarcelo.info/teaching/lxs/wlan/manual_vlan.pdf

4.2   Introduction

In this lab assignment the switches will be configured to create different VLANs. The
IPs of the switches are 192.168.1.110, 192.168.1.111 and 192.168.1.112. An sketch on
the blackboard specifies the switch to which your PC is connected. Each VLAN has a
unique identifier that takes values between 0 and 4094. In this assignment we will use
the identifiers 10 and 20.

Each group will use three PCs. One of the PCs is for managing the switch and needs
an IP address of the same range as the IP of the switch (check the blackboard for the
details). The IPs of the other two switches must belong to the range of the VLAN that
you are going to use (192.168.{10,20}.XX).

4.3   Creation of a VLAN

Table 4.1 describes the four possible modes of interaction with the switch. The first one
offers limited information about the switch. It is possible to find more detailed informa-
tion in the second (privileged EXEC) mode. The third mode allows the configuration of
general aspects of the switch while and the last one is to configure a specific interface.
The commands available in each of the modes are different. Make sure you are in the
right mode before issuing a command. It is possible to move to the previous mode using
the "exit" command.

Use a telnet client to connect to the switch and observe which is the initial mode.
You can use the command "?" to obtain information about the possible commands in a
given mode. Additionally, you can also follow a partial command by "?" to obtain more

Table 4.1: Command modes

Command Mode	Access	Prompt
User EXEC	Connecting to the switch	Switch¿
Privileged EXEC	Using the enable command in the "User EXEC" mode	Switch#
Global Configuration	Using the "configure terminal" command in the "Privileged EXEC" mode	Switch(config)#
Interface Configuration	Using the "interface <interface-name>" command in the "Global Configuration" mode specifying the interface that we want to configure, e.g. FastEthernet0/4	Switch(config-if)#

information about how to use the command and the required parameters. For example "ip address ?" would give you information about the parameters you could use after address.

Enter the mode *privileged* EXEC and use the command `show running-config` to see the current configuration of the switch. Answer the following questions. *How many VLANs can you observe? (Note that this is not necessarily the number of VLANs in the switch). How many Fast Ethernet interfaces are available? What is the VLAN1 administrative address?*

There exists a *default* VLAN which has the number 1. Use the command `show vlan` or `show vlan id <id >`. *What is the status of VLAN1? How many VLANs are there in the switch?* For each of the VLANs identify the ID, the name, the status, the assigned ports and the type. Include this information in the report.

Enter the config mode and try to delete the default VLAN: `Switch-B(config)#no vlan 1`. *What happens?*

In the config mode, use the "?" to find which commands can be used in this mode. Use the `vlan <id>` to create a new VLAN. The type is Ethernet and the id must be set according to the sketch on the blackboard. Include the exact command that you used and the reply message of the router in your report.

Verify the new configuration using the command `show vlan` in the privileged EXEC mode. *What is the default name of the new VLAN?*

Delete the VLAN that you have just created using `no vlan <id>`, verify that it has been deleted and created again. Include in your report the sequence of commands that you used and the output of the switch after each command. You can use the command `show vlan brief`.

In the global configuration mode, use the command `vlan <id>` to configure the VLAN that you have created. In the VLAN configuration mode use the name command to

Table 4.2: Command modes

	Same Switch	Different Switch
Same VLAN	ok/ko	ok/ko
Different VLAN	ok/ko	ok/ko

change the name of the VLAN `Switch-B(config-vlan)#name test`.

Name your VLAN vlanXX-GroupX-switchX. Verify the changes. Include in your report the exact commands that you used and the output of the switch. *Which other parameters can be changed in the vlan configuration mode?*

In the priviliged EXEC mode, take a look at the running configuration and compare it with the start-up configuration. *Are they equal?* Find which is the command that is needed to copy the running configuration to the start-up configuration. You will need this command when you make changes to the configuration that you want to save.

4.4 Static assignment of ports to a VLAN

After having created one or more VLANs, the next step is to assign ports to the VLANs. The simplest assignment is the "static" assignment.

Go to the global configuration mode. Find out which are the ports that you want to modify (e.g., 0/1, 0/2, etc.). Change the ports to which your two auxiliary PCs are connected. Make sure that you do not change the port that you are using for the telnet connection.

To make the changes, you first have to go into to interface configuration mode. Now check the options of the `switchport` command and use the switch user manual if you require extra information.

After making the changes go back to the privileged execution mode. Verify which are the changes that you have made comparing the running config to the start-up config. Save your changes.

Use the `ping` command to test the connectivity between the two auxiliary PCs. Then try the connectivity between the configuration PC (the one with the telnet connection) to the auxiliary PCs. Finally, try the connectivity between your PCs and other groups PCs. Explain the results and the conclusions of the experiments.

Try to complete Table 4.2.

Which devices are reached if you use a broadcast packet? How can a packet travel from one VLAN to a different VLAN?

4.5 Trunk ports

A trunk port can carry traffic of different VLANs between two switches. You will find which are the trunking ports on the blackboard. In the privileged EXEC mode use the

command `show interfaces <trunk interface> switchport`. Write down the following parameters:

- Administrative mode

- Operational mode

- Administrative trunking encapsulation

- Trunking native mode

- Trunking VLAN enabled

- Trunking VLAN active

Use the `show vlan` command to check the status of the ports. *Where can you find the trunk ports?*

4.6 Defining the VLANs carried by a given trunk port

By default, a trunk port carries traffic of all VLANs. It is possible to configure which VLANs are allowed in a given trunk port.

From the privileged EXEC mode, check which are the VLANs in the trunk port of your switch. *Which command do you use?*

In the global configuration mode, enter into the configuration of the trunk port. Specify the command that you use.

Now we are going to configure the trunk port to allow the traffic of our VLAN. Check the options of the command `switchport trunk allowed vlan [remove,add] vlan-list`. The parameter `vlan-list` is a list of VLAN identifiers (or names) separated by a hyphen (or a comma, respectively).

Exit the configuration mode and move back to the privileged EXEC mode. Use the commands `show interface interface-id status` or `show interface status` to see the configuration of one or all the interfaces. *What are the results?*.

Try also the `show interfaces trunk` command and write down the results.

4.7 Connectivity test

Verify whether the following connections are possible and explain why.

- Ping a PC of the same VLAN connected to a different switch.

- Ping a switch of a different VLAN.

- Perform additional tests.

Compare the results that you obtain now with the results obtained in Section 4.4. Fill in the connectivity table again.

Are there any differences? Why

Change the IP address of one of your auxiliary PCs to an address belonging to the range of the other VLAN. Perform connectivity tests again. *What happens? Why?*

4.8 Network topology

Draw the network topology, both from the physical point of view and the logical point of view.

4.9 Preparing the report

These are aspects that you may want to cover in your report:

- What is a VLAN and what is used for?

- What are the differences among the different modes of the switch?

- Relation between the active VLANs and the different ports.

- Differences between access ports and trunk ports.

- Connectivity in the different situations.

- Remote management using telnet and VLAN 1.

4.10 Changing the native VLAN (Optional)

For security reasons, it is recommended to change the native VLAN (e.g., to 666) of the switches and leave no ports assigned to the VLAN, except for administration.

4.11 Speed and duplexing (Optional)

Change the speed of the port and the duplexing and perform tests using iperf.

4.12 Administrative shutdown of interface (Optional)

Try to administratively disable access ports and trunking ports and describe the results.

Table 5.1: Spanning Tree

Switch ID	MAC	Port	Role	State
Switch B				
...	...	...	...	...

Chapter 5

Spanning Tree Protocol

5.1 Switch Manual

The user manual for the switch is available here:

    `http://www.jaumebarcelo.info/teaching/lxs/stp/manual_spantree.pdf`

5.2 Introduction

In this assignment you will configure the Spanning Tree Protocol. This protocol is used in Ethernet networks to establish which are the active link and therefore which is the path that data packets will follow. The switches that you will use are the same as the ones in the previous assignment. Have your VLAN report handy just in case you need to consult it to refresh which are the basic commands to interact with the switch.

5.3 Theoretical construction of the tree

The switches are connected as depicted in Fig. 5.1.

Find the BridgeId of each switch. Compute which is the spanning tree and draw it. Which switch is the root? Which is the role of each port? Which ports are activated?
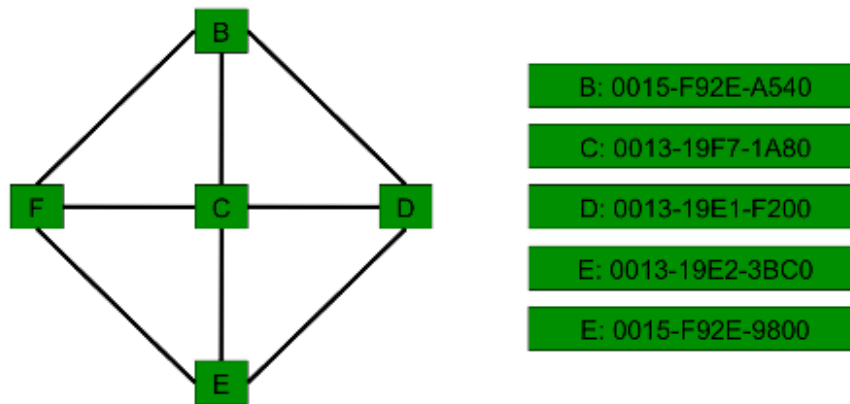
Fill in Table 5.1.

B: 0015-F92E-A540

C: 0013-19F7-1A80

D: 0013-19E1-F200

E: 0013-19E2-3BC0

E: 0015-F92E-9800

Figure 5.1: Network topology

5.4 Practical verification

Now you will verify that the STP constructed by the switches is in fact the one you computed in the previous section.

Use the VLAN 1 to connect to the five switches (B, C, D, E, F). It is recommended to open five windows and telnet one of the switches in each of them.

Each group will work in a different VLAN. The teacher will assign a VLAN to each group. Make sure that your VLAN is included in all the trunk ports. Each group will have a different STP, as the network creates a tree for each VLAN.

In each of the switches, enter the privileged EXEC mode and use the command `show spanning-tree vlan XX`. What can you see? Observe all the fields and make sure you understand them.

Find the BridgeId of each switch. Compute which is the spanning tree and draw it. Which switch is the root? Which is the role of each port? Which ports are activated?

Fill in Table 5.1 and compare practical results to the theoretical computation.

5.5 Changing the STP configuration

Now that you are familiar with the STP parameter, you will make some changes that will result in the computation of a new tree. In the global configuration mode use the command `spanning-tree vlan XXX` (alternatively you can use `interface VLAN XXX` and `spanning-tree`) to see which parameters are susceptible to be configured. Use the question mark `?` to see all the available parameters and make sure you understand them.

The exercise that we propose is to change the priority of one of the switches different from the root switch. The default behaviour is that the switch with the lowest MAC address is selected as a root. The reason is that, in the default configuration, the priority of all the switches is 32768. By changing the priority of one of the switches to a lower value, we can force that that particular switch becomes the root.

Go ahead and change the root switch and observe the new configuration of the tree. Fill in Table **??** for this new configuration and draw the new tree.

5.6   Link failure

This exercise cannot be started until all the groups have finished the previous one. If you reach this exercise before the other groups, move on to the next exercise while you wait for all the groups to be ready for the link failure.

Now we will disconnect one of the links to simulate a link failure. Compute in advance your new spanning tree after the link failure. Ask your teacher which is the cable that will be disconnected.

After the disconnection, check which is the new configuration and compare it with the one that you have predicted. Explain what happened.

5.7   BPDUs

Use a computer connected to the VLAN 1 (administration) and capture the traffic for several seconds using Wireshark. Observed the received STP frames and identify the different fields of the packet. Write them down to include them in your report and find out which is the meaning of the information in each of the fields.

Why are you receiving this frames at your computer?

Bibliography