# Network Laboratory

Ruizhi Liao, Alex Bikfalvi, Jaume Barcelo, Albert Rabassa

Spring 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.

| Evaluation Method | Weight |
|---|---|
| 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 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 learn about 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.

| Questions and Tasks |
|---|
| What is the purpose of ARP? Tip: Use the RFC826 standard to answer this question [**?**]. |
| 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 following command with root permissions.

```
service iptables stop
```

## 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.

| Questions |
| --- |
| 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.

| 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.

| 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? |
| Did you capture an HTTP packet? 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... you can configure the protocols that Wireshark captures and displays. 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 and link). Include a brief description of the protocols you found.

Select 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`**.**

| Questions |
| --- |
| What are the differences between IPv4 and IPv6? |

## 2.5 The Address Resolution Protocol (ARP)

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

If you do not capture any ARP packets, clear your ARP cache and then ping or browse to any preferred destination. You can use the following command to delete all ARP entries. On a Windows computer use.

```
arp -d *
```

On a Linux computer use.

```
sudo ip neighbour flush all
```

| Questions |
| --- |
| What are the source and destination MAC addresses of the Ethernet frame that contains the ARP request message? |
| What are the source and destination IP addresses in the ARP request and response frames? |
| What are the source and destination MAC addresses in the ARP request and response frames? |
| 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.

| Question |
| --- |
| To which layer does ARP belong? |

## 2.6 HTTP and Secure HTTP

Begin a new 5 minutes capture and during this time visit a few web sites, such as `http://www.upf.edu` and `https://www.google.com`. After the capture finishes, observe the HTTP and HTTPS messages by typing `http or ssl` in the filter toolbar. Observe an HTTP GET message and the corresponding response and answer the following questions.

| Questions |
| --- |
| What is the HTTP version of your web browser? |
| What is 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.

| Questions |
| --- |
| 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 message pair. Use `dns` in the *Wireshark* filter.

| Question |
| --- |
| 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.

| Question |
| --- |
| When using HTTP, it is possible to observe the contents of the web using Wireshark? |

Now use HTTPS.

| Question |
| --- |
| Is it still possible to read the information that is being transmitted? Tip: Search for SSL packets. |

Identify a SSL handshake in *Wireshark*.

## 2.7 ICMP Ping Packet Capture (Homework)

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

| Question |
| --- |
| What are protocols used? |

Draw a frame and explain how the different packet are encapsulated in each other.

| Question |
| --- |
| 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.

| Questions |
| --- |
| What is the packet length? |
| At which layers can we find source and destination addresses? |
| What are the addresses types? |
| Are the ping ICMP query packets sent at constant time intervals in time? |
| What about the ICMP replies? |
| What are the reasons for different inter-arrival times for the ICMP reply? |
| 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 shall 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 begin a new `tcpdump` capture. Enter the Ctrl+C keys to finish the capture.

**Questions**

What is the information provided by `tcpdump` and what is the format used?

To which level does the information belong? Tip: Remember that you can redirect the output to a file using the following command `tcpdump >file_name`.

The first line of `tcpdump` specifies the network interface used during the capture. To change it, use the `-i` option.

**Question**

What is the interface that you are using?

Describe the information provided for the ARP protocol using the following command.

```
tcpdump arp
```

Then, execute the same command again using the `-e` option.

**Question**

What is the difference with respect to the previous execution? Tip: Use the `tcpdump` manual, if necessary.

Try several new captures related to this assignment, such as

```
tcpdump stp
tcpdump http
tcpdump udp
tcpdump ssl
tcpdump ip
```

Try also to make captures for a specific IP address.

Chapter 3

# LAN and WLAN

## 3.1 Home Preparation

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). On a Windows computer, you can use NetStumbler, whereas on Linux computer you can use the following command:

```
sudo iwlist <wlan_interface> scan
```

## 3.2 Equipment

Each group requires at least *two* (2) computers. However, if possible, *three* (3) computers are better than two. Start one computer in Windows and the other one in Linux. The hardware we shall use during this lab is the *Cisco Aironet 1200* access point. The firmware of the access point is *CISCO IOS Version 12.3(8)JA2*, and you can download the corresponding at the following link:

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

To test copying a file across the wireless network, install an FTP server on one of the computers, such as *Filezilla* in Windows and *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 following command:

```
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 need 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 following command:

```
sudo service iptables stop
```

If you decide to use *Firefox* to connect to the access point during the assignment, it might be necessary to disable the proxy settings and to uncheck the *offline navigation* option.

## 3.4 Basic LAN Configuration

Connect the Windows and the Linux computers using a cross-over cable. 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.

Next, you need to estimate the available bandwidth using an FTP file transfer or the `iperf` tool. Change the Ethernet connection speed to 10 Mbps (full duplex) and estimate the bandwidth again.

I believe the mii tool is obsolete - update? Include instructions on how to change the connection speed in Windows/Linux.

| Questions |
| --- |
| Is the maximum transmission speed reached? Why? |

## 3.5 WLAN Basic Configuration

WLANs can be used as an access point (AP) to LANs. They can also be used to interconnect to LANs using WDS. What's this?

First connect the AP to the Windows computer. You may use either a direct connection or a connection using the patch panel. The address is available on the AP, and the administrator user is `Cisco` and the password is `Cisco`.

Use the express set-up to configure the AP with the following settings.

| Setting | Value |
|---|---|
| AP Name | LABXARXES_GRUP_XX |
| SSID | grupXX |
| Channel | default |
| Transmit power | default |

After completing the configuration, verify 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.

Plug-in the WiFi interface into the Linux computer 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 `ipconfig` (on Windows) or `ifconfig` (on Linux) commands 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. Measure the throughput using FTP to transfer a large file.

| Questions and Tasks |
|---|
| 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. It consists of a backup AP (*AP-standby*) which takes over if the primary AP (*AP-root*) fails.

*During this assignment, 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: SSID, network mask and 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* go to Services >Hot Standby. Select 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 from 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 happening, 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.

| Questions |
| --- |
| 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.

| Questions |
| --- |
| 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. Similar to the previous exercise, both APs must share the same configuration (with the exception of the IP address). In this exercise, we shall use the previous *AP-standby* as a repeater.

- In the *AP-root*, select the option Role in radio network and then choose Access point.
- In the *AP-repeater* (the former *AP-standby*), disable the hot-standby option. Configure the SSID, and at the bottom of the page Security >SSID Manager select Set Infrastructure SSID and entering the current SSID. In the Express Setup, choose Repeater for the option Role in radio network.

After the configuration changes have been completed, your home screen should show the configuration of your network and the repeater, and the clients connected to each AP. Initially, the client computer is probably connected to the *AP-root*.

By selecting the Clients options, you will see the list of associated clients. You can manually de-associate a particular client, in which case the client will automatically re-connect to the repeater.

To verify that the client connects successfully to the other AP, repeat the round-trip time and bandwidth tests that you have performed before. Do the tests while connected to both *AP-root* and *AP-repeater*. Repeat the ping tests while a file is being transferred.

| Question |
| --- |
| Can you observe any difference? |

Chapter 4

# Virtual Local Area Networks (VLANs)

## 4.1 Switch User Manual

You can download the switch user manual from here:
http://www.jaumebarcelo.info/teaching/lxs/wlan/manual_vlan.pdf

## 4.2 Introduction

In this lab assignment, we shall configure a Cisco switch to create different VLANs. The IP addresses of the lab switches are 192.168.1.110, 192.168.1.111 and 192.168.1.112. A sketch on the blackboard/whiteboard specifies the switch to which your PC is connected. Each VLAN has a unique identifier that takes values between 0 and 4094. In this lab assignment we shall use the identifiers 10 and 20.

Each group will use three computers. With one computer you shall manage the switch, and this compute requires an IP address in the same subnetwork as the address of the switch. Your instructor will give your further 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

All Cisco switches used during this lab, use an operating system called the Cisco *Internetwork Operating System*, or *IOS*. The IOS features a command-line interface (CLI), which is accessible using a serial cable or a LAN Telnet connection.

We shall use the IOS command-line interface in four modes of operation, which are described in the table **??**. As shown in the table, you can identify the current mode of operation according to the CLI prompt. The *user EXEC* mode offers limited information about the switch. The *privileged EXEC* mode allows us to access detailed information. The *global configuration* mode enables us to configure the general aspects of the switch, whereas we can use the *interface configuration* mode 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. After entering a specific mode, it is possible to leave to the previous one using the command:

| Command Mode | CLI Prompt | Access |
|---|---|---|
| User EXEC | `Switch>` | By default, when connecting to the switch for the first time, you are in this mode. |
| Privileged EXEC | `Switch#` | From the User EXEC mode, enter the `enable` command. |
| Global Configuration | `Switch(config)#` | From the Privileged EXEC mode, enter the `configure terminal` command. |
| Interface Configuration | `Switch(config-if)#` | From the Global Configuration mode, enter the `interface <if-name>`, where `if-name` is the name of the interface that we want to configure, such as `FastEthernet0/4` or `Fa0/4`. |

Table 4.1: *Command modes of the Cisco IOS command-line interface*

```
exit
```

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 information about how to use the command and the required parameters. For example, the command:

```
ip address ?
```

would give you information about the parameters you could use after address.

Enter the *privileged EXEC* mode and use the command:

```
Switch# show running-config
```

to see the current configuration of the switch.

| 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:

```
Switch# show vlan
```

or

```
Switch# show vlan id <id>
```

to collect more information.

| Questions |
|---|
| 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 *global configuration* mode and try to delete the default VLAN.

```
Switch(config)# no vlan 1
```

**Question**

What happens?

Use the `?` command to find which commands can be used in this mode. Create a new VLAN with the command:

```
Switch(config)# vlan <id>
```

The type of the VLAN is Ethernet and the `id` must be set according to the sketch you find on the blackboard/whiteboard. Include the exact command that you used and the reply message of the router in your report.

Verify the new configuration using the following command:

```
Switch# show vlan
```

in the privileged EXEC mode.

**Question**

What is the default name of the new VLAN?

Delete the VLAN that you have just created using the command:

```
Switch(config)# no vlan <id>
```

and verify that it has been deleted and created again. What???

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:

```
Switch# show vlan brief
```

In the *global configuration* mode, use the command:

```
Switch(config)# vlan <id>
```

to configure the VLAN that you have created. In the *VLAN configuration* mode use the `name` command to change the name of the VLAN. The VLAN configuration mode is not included in the operation modes table.

```
Switch(config-vlan)# name <vlan-name>
```

Name your VLAN `vlanXX-GroupX-switchX`, and verify the changes. Include in your report the exact commands that you used and the output of the switch.

**Question**

Which other parameters can be changed in the VLAN configuration mode?

In the *privileged EXEC* mode, take a look at the running configuration and compare it with the start-up configuration.

**Question**

Are they equal?

| | Same switch | Different switch |
|---|---|---|
| Same VLAN | OK/KO | OK/KO |
| Different VLAN | OK/KO | OK/KO |

Table 4.2: *Connectivity tests*

Find which is the command that is needed to copy the running configuration to the start-up configuration. The students also need to find the command to show the start-up config for the previous point. 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 creating one or more VLANs, during the next step we assign ports to the VLANs. The simplest assignment is the *static* assignment.

First, enter the *global configuration* mode. Find out which are the ports that you want to modify (for example, 0/1, 0/2, etc.). Modify only the configuration of the ports that are assigned to the other two computers from your group. 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. Here, check the options of the `switchport` command and use the switch user manual if you require extra information. After making the changes (what changes – specify?) return to the *privileged* mode. Verify the changes that you have made comparing the running configuration to the start-up configuration. Save your changes.

Use the `ping` command to test the connectivity between the two auxiliary computers. Try the connectivity between the configuration computer (the one that you use to connect to the switch CLI) to the auxiliary computers. Finally, try the connectivity between the computers of your group and computers of other groups in your class. Explain the results and the conclusions of the experiments, and complete the table **??**.

| Questions |
|---|
| 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/whiteboard. In the *privileged EXEC* mode use the command:

```
Switch(config)# show interfaces <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 command:

```
Switch(config)# show vlan
```

to check the status of the ports.

| Question |
| --- |
| Where can you find the trunk ports? |

## 4.6 Setup the VLANs Carried by a Trunk Port

By default, a trunk port carries traffic of all VLANs. However, it is possible to configure which VLANs are allowed in a given trunk port. To accomplish this, from the *privileged EXEC* mode, check which are the VLANs in the trunk port of your switch.

| Question |
| --- |
| Which command do you use? |

In the *global configuration* mode, enter into the configuration of the trunk port.

| Question |
| --- |
| Which command do you use? |

Now we are going to configure the trunk port to allow the traffic of our VLAN. Check the options of the command:

```
Switch(config-if)# switchport trunk allowed vlan [remove | add] <vlan-list>
```

The parameter `vlan-list` is a list of VLAN identifiers (or names) separated by a hyphen (`-`) when specifying a VLAN range, or a comma (`,`) when specifying a set of VLANs.

Exit the configuration mode and return to the *privileged EXEC* mode. Use the commands:

```
Switch# show interface interface-id status
```

or

```
Switch# show interface status
```

to see the configuration of one or all the interfaces.

| Question |
| --- |
| What are the results? |

Try also the command:

```
Switch# show interfaces trunk
```

and write down the results.

## 4.7 Connectivity Test

Verify whether the following connections are possible and explain why.

- Ping a computer of the same VLAN, connected to a different switch.
- Ping the switch of a different VLAN.
- Perform additional tests. Examples???

Compare the results that you obtain now with the results obtained in the static assignment of VLANs. Fill in the connectivity table **??** again.

| Questions |
| --- |
| Are there any differences? Why? |

Change the IP address of one of your auxiliary computers to an address belonging to the range of the other VLAN. Perform the connectivity tests again.

| Question |
| --- |
| 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 of the switches (for example, to 666) and leave no ports assigned to that VLAN, except for administration.

## 4.11 Speed and Duplexing (Optional)

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

## 4.12 Administrative Shutdown of an Interface (Optional)

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

Chapter 5

# Spanning Tree Protocol (STP)

## 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 (STP). 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 and to remember which are the basic commands to interact with the switch.

## 5.3 Theoretical Construction of the Tree

The switches are connected as illustrated in the figure **??**.

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

Fill in the table **??**.

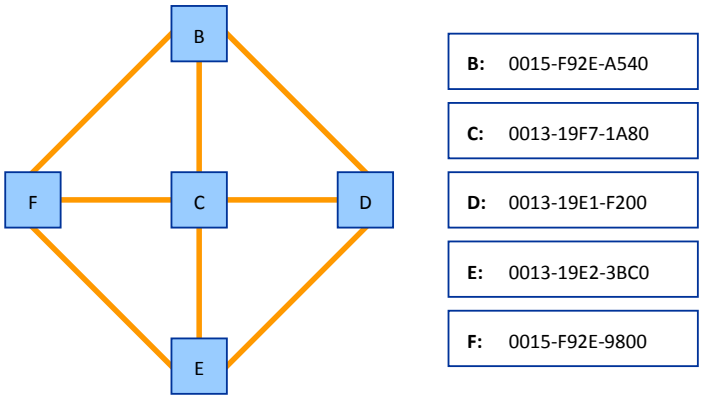


Figure 5.1: *The network topology used for the STP practical exercise.*

| Switch ID | MAC | Port | Role | State |
|---|---|---|---|---|
| Switch B | | | | |
| | | | | |
| | | | | |
| ⋮ | | | | |

Table 5.1: *The spanning tree.*

## 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 simultaneous Telnet connections, one for each of the switch.

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:

```
Switch# show spanning-tree vlan <id>
```

| Question |
|---|
| 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 the table **??** and compare practical results to the theoretical computation.

## 5.5 Changing the STP Configuration

Now that you are familiar with the STP parameters, you will make some changes that will result in the computation of a new tree. In the *global configuration* mode use the command:

```
Switch(config)# spanning-tree vlan <id>
```

or, alternatively, you may use:

```
Switch(config)# interface vlan <id>
Switch(config)# 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 behavior 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 the 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 the computer connected to the VLAN 1 (the computer used for the administartion of the switch) and capture the traffic for several seconds using *Wireshark*. Observed the received STP frames and identify the different fields in 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.

| Question |
| --- |
| Why are you receiving these frames at your computer? |