Network Laboratory

Ruizhi Liao, Alex Bikfalvi, Jaume Barcelo, Albert Rabassa

Spring 2013

Last updated: May 27, 2013

Contents

Acknowledgements

The assignments presented in this book are the ones that have been prepared over the years in the Network Laboratory course by different instructors, including Anna Escudero, Anna Sfairopoulou and Eduard Bonada.

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 [1].*
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.

Repeat the previous capture using IPv6, by performing ping to the local-link IPv6 address of a neighbor or attempting an IPv6 ping to an existing destination. You may use one of the following commands:

```
ping6 -I <interface> <address>
```

or:

```
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 network layer 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
```

We recommend *Internet Explorer* to interact with the AP web interface. 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[1].

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 `ethtool` 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.

On a Linux machine, you can check your eth interface configration:

```
ethtool eth0
```

and change the configration:

```
sudo ethtool -s eth0 speed 10 duplex half
```

After testing, remember to change the configration back:

```
sudo ethtool -s eth0 speed 1000 duplex full
```

Questions

Is the maximum transmission speed reached? Why?

[1]

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 wireless distribution system (WDS). WDS can also be used to extend the coverage of a WLAN with access points that don't have a wired connection. IEEE 802.11 headers can accommodate up to 4 addresses to differentiate between final addresses and per-hop addresses[2].

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.

[2] This is explained in the theory session

- 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. Your instructor will give your the IP addresses of the lab switches, which shall be similar to the ones from the table below. During this assignment, each group of students will be assigned to a switch. Before you begin, you must connect the Ethernet cable of your computers to the switch assigned to your group, in the manner indicated by your instructor.

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 IP addresses of the other two computers must belong to the range of the VLAN that you are going to use: 192.168.10.*XX* or 192.168.20.*XX*.

Student Group	Switch	IP Address
Group 1	Switch B	192.168.1.102
Group 2	Switch C	192.168.1.103
Group 3	Switch D	192.168.1.104
Group 4	Switch E	192.168.1.105
Group 5	Switch F	192.168.1.106

Table 4.1: *The IP addresses of the lab switches (subject to change, according to the instructions received during the lab).*

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

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 4.2. 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:

```
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 create it 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:

```
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.

	Same switch	Different switch
Same VLAN	OK/KO	OK/KO
Different VLAN	OK/KO	OK/KO

Table 4.3: *Connectivity tests*

```
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?

Find which are the commands that are needed to show the running configurations, and then 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 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, 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 4.3.

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 (optional).

Compare the results that you obtain now with the results obtained in the static assignment of VLANs. Fill in the connectivity table 4.3 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 5.1.

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 5.1.

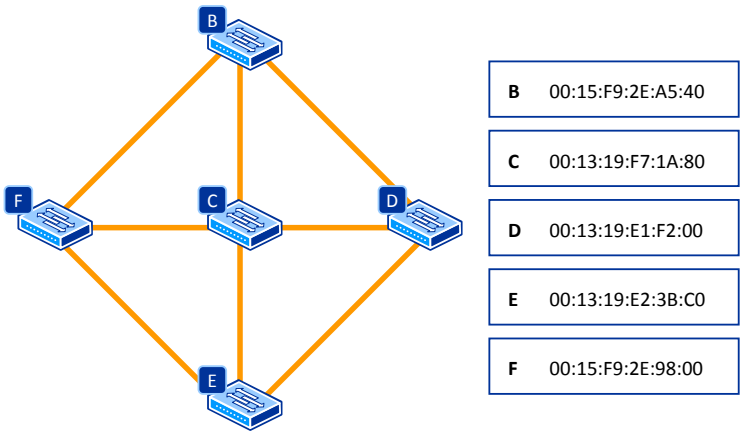

Figure 5.1: *The network topology used for the STP practical exercise.*

Switch ID	MAC	Port	Role	State
Switch B	00:15:F9:2E:A5:40			
Switch C	00:13:19:F7:1A:80			
Switch D	00:13:19:E1:F2:00			
Switch E	00:13:19:E2:3B:C0			
Switch F	00:15:F9:2E:98:00			

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>
```

Observe all the fields and make sure you understand them.

Question
What can you see?
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 5.1 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 5.1 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 administration 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?

Chapter 6

Routing

6.1 Home Preparation

RIP and OSPF are two of the most widely used routing protocols. Find information about these two protocols and compare them. Describe what is the format of a routing table and explain how each of the protocols work.

Read the following quick guide:
www.jaumebarcelo.info/teaching/lxs/routing/GUIA_RAPIDA_CISCO_2010.pdf
Then, download the router user manuals:
www.jaumebarcelo.info/teaching/lxs/routing/manuals_routers.rar

6.2 First Session

In this first session each group will work with a router. The goals of this session are:

- Getting familiar with the configuration method.
- Configuring the Ethernet interfaces.
- Observe the RIP protocol in action.
- Save the configuration in an external TFTP server.

Start your computer in Windows. Before disconnecting the computer from the Internet, download the TFTP server from the web site http://tftpd32.jounin.net/, and save it on one of the computers that you will use to connect to the router.

The routers are connected to each other using the Ethernet interfaces and forming the topology from the figure 6.1. Use the console connection to connect to the routers (use either *HyperTerminal* or *putty* to open a serial connection at 9600 bps). The COM port number (e.g. COM1, COM2, etc.) depends on your computer configuration[1]. The escape keystroke to exit the `ping` command in a router is Ctrl-Alt-6.

[1] You can see the name of the local serial ports in the *Device Manager* snap-in. To open the snap-in, click on Start >Run..., type `devmgmt.msc` and click OK. The serial ports are listed under the *Ports* branch.

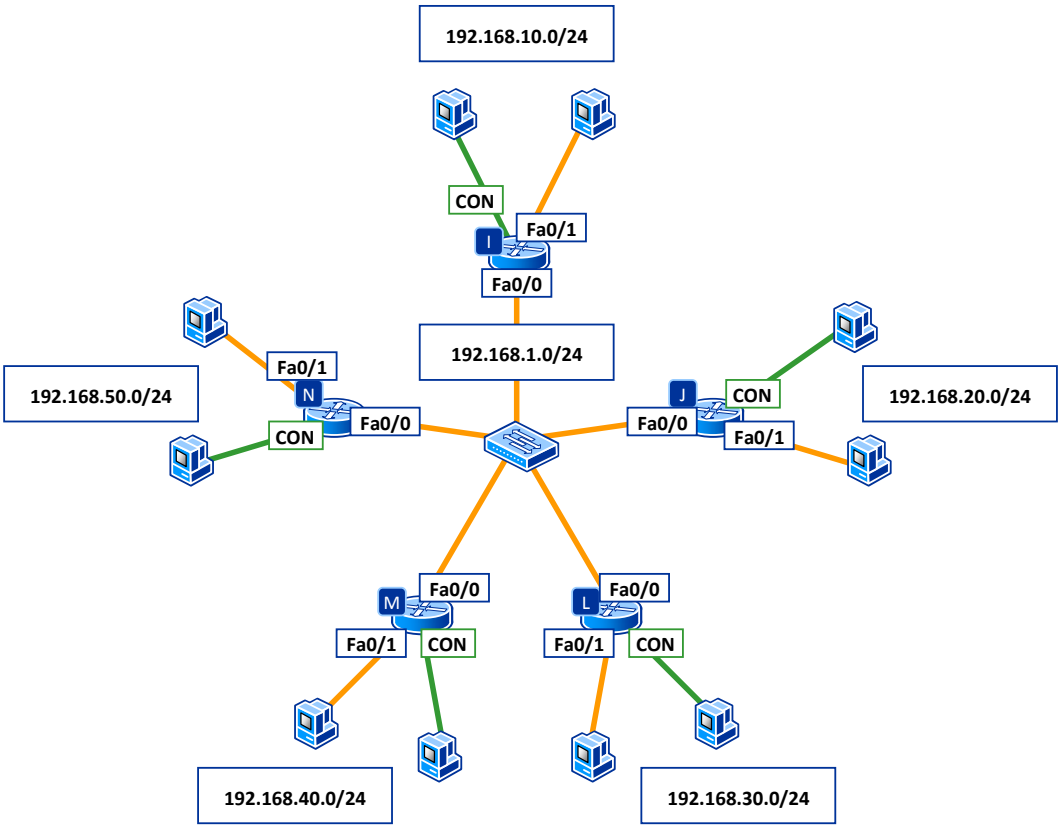

Figure 6.1: *The network topology used for the Ethernet routing exercise.*

6.2.1 Checking the Router Status

Use the console to connect to your router and try the following commands. Prepare a summary of what you can see with each command.

```
show version
show protocols
show interfaces
show processes
show mem
show ip route
show history
```

6.2.2 Create a Running and Startup Configuration

Enter the privileged EXEC mode with the command:

```
Router> enable
```

and password `cisco`, and the the global configuration mode

```
Router# configure terminal
```

Find the commands to:

- show and change the router name;
- debugging mode configuration;

- send pings from the router, and;
- activate fair queueing on the ethernet interfaces (e.g. FastEtherneto/o).

Use the following commands to show and save the current configuration to the startup configuration from the privileged mode.

```
Router# show running-config
Router# copy running-config startup-config
```

6.2.3 IP Addresses Configuration

Go to your physical router equipment and check which interfaces are visible. Use the following command to see what interfaces are available in the router.

```
Router# show interfaces
```

Fill in a table that includes:

- the interface name;
- the interface MTU;
- the interface bandwidth, and;
- the encapsulation protocol.

Enter the Ethernet interface configuration mode with the command:

```
Router(config)# interface <interface name>
```

Then, set the IP address to 192.168.XX.1, where XX is your group ID times 10, i.e. 10, 20, 30, etc. Use a /24 network mask. For the Ethernet interface of your computer use the IP address 192.168.XX.2.

Question

What is the command that you have used?

Use the command:

```
Router# show interfaces
```

to verify the IP address assignment, and enable the interface with the command:

```
Router(config-if)# no shutdown
```

Verify the line status and the interface status using the command:

```
Router# show protocols
```

Use the commands:

```
Router# show cdp neighbors
```

and:

```
Router# show cdp neighbors detail
```

to see the neighboring Cisco devices. Write down the information received from the different interfaces.

- the neighbor identifier;
- the IP address, and;
- the port.

Use the `ping` command to test the connectivity to the other routers in the lab and write down the round-trip times and other results that you may consider relevant.

From your computer, use the `telnet` command to connect to your router.

Question
Is it possible to remotely configure a router?
Is login and password required?
Does a console user notice that there is an ongoing telnet connection?
Use telnet to change a parameter of the router (e.g., the name) and verify the changes both using the console and the telnet connection. What happens?
Do messages appear on the console when changes are done over Telnet? What information is included in these messages?

Logout the Telnet session to the Cisco router.

6.2.4 IP Routing Configuration

In this exercise, we shall enable the RIP protocol and check the status of the routing table as well as the RIP transactions of each router.

Check whether IP routing is enabled using the command:

```
Router# show protocols
```

Question
What is the status of IP routing?

Enter the global configuration mode and enter the submenu `router`.

Question
What is the purpose of this submenu?

Use the `?` command to list available routing protocols and write down the results. Enter into the configuration of RIP.

```
Router(config)# router rip
```

Use the command:

```
Router(config-router)# network <your network>
```

to associate your network to the RIP routing process. Assume that we are working with *C* class IP addresses. Therefore, the last byte of the network address must be 0. Verify that the RIP protocol is now enabled and that your network has been recognized by the router using the command:

```
Router# show ip protocol
```

Observe the relevant parameters and answer the following questions:

Question
What is the use of the timers?
What are their values?
Are they too small, or too large?
What happens if we change the values?

Verify the status of the routing table with the command:

```
Router# show ip route
```

Question
What is the meaning of each of the fields in the table?
How can we check which are the networks to which RIP protocols is associated?
If there is no information, why?

Work together with another group to do this part. If there is no other group ready, skip this exercise and come back to it when another group reaches this point.

Add an static route to the other group's network. Use the following command from the configuration mode.

```
Router(config)# ip route
```

Explain what happens when you use `traceroute` to the other groups router (both interfaces). Repeat the experiment after deleting the static route in one of the routers. Explains what happens and why.

The command:

```
Router# debug ip rip
```

shows the RIP messages that are sent and received by the router.

Question
What are the source and destination of these packets?
What information do we obtain?

6.2.5 Saving the Router Configuration in a TFTP Server

A convenient way to store a router's configuration is using TFTP. We need to install the TFTP server in a computer with connectivity (layer 3 connectivity) to the router. Install the server and configure in which folder you want to save the router's configuration.

In the router, execute the command:

```
Router# copy running-config tftp
```

and follow the instructions to enter the TFT server address (this is one of your computers) and the filename that you want to use. In the computer, open the configuration file using a text editor.

Question
What can you observe?

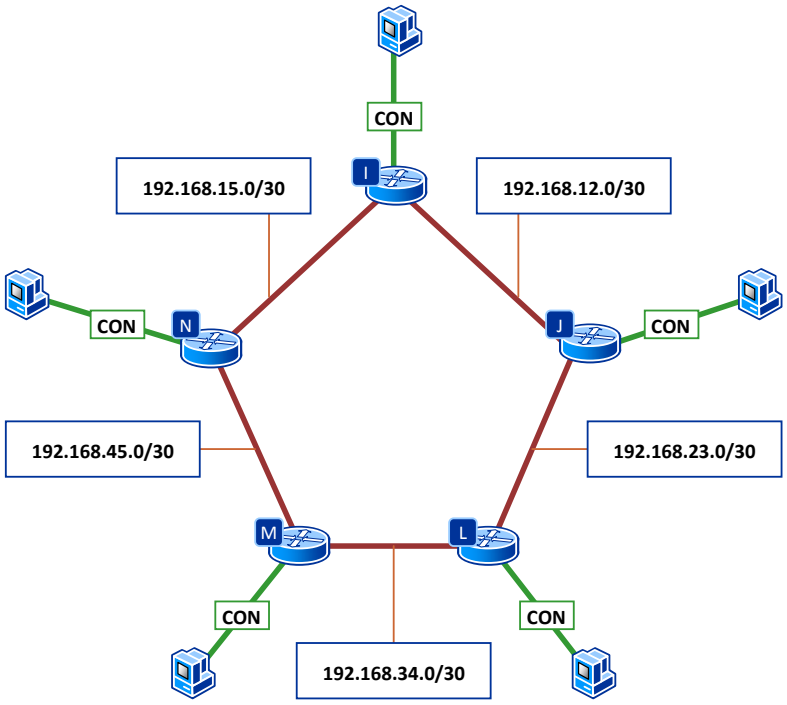

Figure 6.2: *The network topology used for the WAN routing exercise.*

To copy the configuration in the TFTP server to the router, there are two different options. Either use the command:

```
Router# copy tftp running-config
```

on the server or simply copy and paste on the configuration terminal.

6.3 Router Interconnection

In this session, we shall use the WAN (serial) interfaces of the routers. The figure 6.2 illustrates the topology of the network. In the previous session we used the Ethernet interfaces to connect the routers, and in this session we will use the serial interfaces.

6.3.1 Shutdown the Ethernet Interfaces

Make sure that there is no cable connected to the Ethernet interface, and that there is a cable connecting the serial interfaces. Delete the IP address of the Ethernet interface:

```
Router(config-if)# no ip address
```

and administratively shutdown the interface:

```
Router(config-if)# shutdown
```

Verify that the changes have been applied using:

```
Router# show running-config
```

6.3.2 Configuration of the WAN Serial Interface

From the privileged EXEC mode of your router, enter the global configuration mode. Enter into the configuration of the WAN serial interface and configure the IP.

To choose the IP, use the following algorithm. Assume the your group id is X and your neighbor's group ID is Y. If $X < Y$, then your IP is 192.168.XY.1. Otherwise, it is 192.168.YX.2. Use a /30 network mask.

The serial interfaces are interconnected by cables that, in the middle, have male/female connector. The router in the female connector side sets the communication rate. You can find which is the female router issuing the command:

```
Router# show controller
```

The DTE interface uses the male connector, and the DCE interface uses the female connector. Alternatively, you may also look at the number on the cable, where 1428 is male and 1429 is female.

Use the command:

```
Router(config-if)# clock rate 128000
```

or the closest available rate.

Verify the configuration and use the command:

```
Router(config-if)# no shutdown
```

on both connected routers to enable the communication. Then use the command:

```
Router# show protocols
```

to verify the state of the line.

Now we will gather information about neighboring devices using the command:

```
Router# show cdp neighbors
```

or

```
Router# show cdp neighbors detail
```

and we will elaborate a table indicating, for each neighbor, the following information:

- the neighbor identifier;
- the neighbor IP address, and;
- the port.

Make sure that routing is enabled using the following commands:

```
Router(config)# ip routing
Router(config)# router rip
Router(config-router)# network 192.168.XX.0
```

and look at the routing tables using the command

```
Router# show ip route
```

Compare the routing tables to the ones obtained in the previous session and highlight the differences. Use the `ping` to the other devices in the network.

Question
Which ones are reachable?
Which ones are not?
Why?
Are there differences in the round-trip-time compared to the measures taken in the previous session?
Why?

6.3.3 Network Topology

Prepare a sketch of the network topology that we have used in this session and compare it to the topology of the previous session.

Question
What are the differences?
What are the advantages?
And disadvantages?

6.4 Configuration of an L2-L3 Network

This third session extends the previous one by including switches to the network topology, as shown in the figure 6.3. The topology consists of a ring of routers connected in a ring using the serial interfaces. Each router is connected using the ethernet interface to a local area network with two or more computers. The devices used in this assignment are:

- computers;
- up to six Cisco routers with an ethernet interface and two serial interfaces;
- up to three Cisco switches, and;
- direct and cross-over RJ-45 cables.

Each group has to configure its router and its VLAN. It is assumed that the previous session has been successfully completed and the connectivity tests were satisfactory.

6.4.1 VLAN Configuration

We connect using Telnet to our switch and enter the privileged EXEC mode. Create a VLAN with a number equal to ten times your group number (e.g. VLAN 20 for group 2). Assign a port connected to the router and one or two other ports connected to computers. Remember to keep the port of the computer you are using for managing the switch in VLAN 1.

Use an IP equal to 192.168.1.XX where XX is the group multiplied by ten for the computer in VLAN 1. Use an IP 192.168.VLAN.YY for the other VLAN. YY is going to be 1 for the router and 2 for the computer. You can use YY equal to 3 if you have another computer.

Test the connectivity between your different computers and with computers of other groups. Write down when a `ping` command is successful and when it is not successful, and provide an explanation.

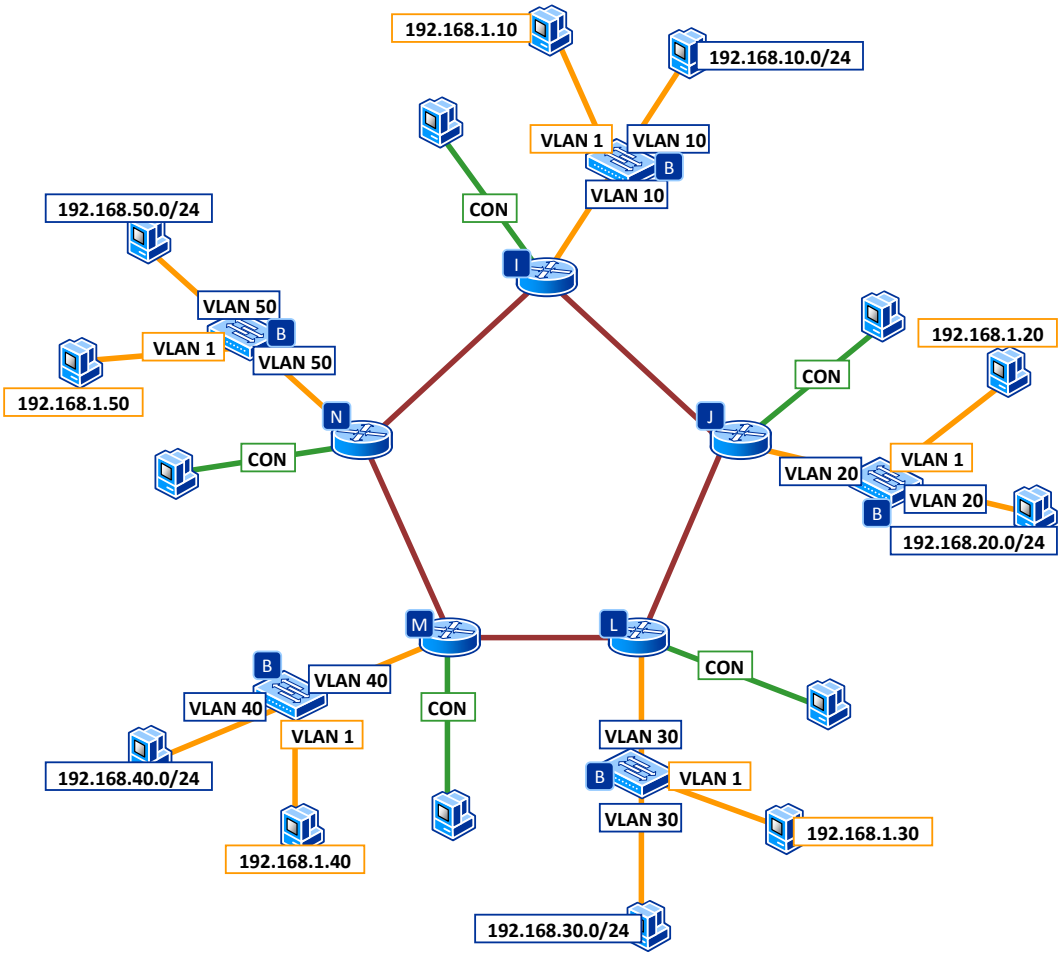

Figure 6.3: *The network topology used for the L2-L3 network.*

6.4.2 Configuring the Router LAN Interface

In the router console enter the privileged EXEC mode and use the command:

```
Router# show interfaces
```

to see the interfaces which are available in the router. We enter the global configuration mode and in in the configuration of the LAN (Ethernet) interface. We configure the IP for this interface. Then we enable the interface with the command:

```
Router(config-if)# no shutdown
```

and check the link status LED. We can also check the status of the line and the interface using the command:

```
Router# show protocols
```

Then we enable the routing. From the global configuration menu we enter the router menu and we use the command:

```
Router(config-router)# network 192.168.VLAN.0
```

to associate our network to the routing process. We will assume that we are using class C networks. Then we use the command:

```
Router# show routes
```

to see the routing tables.

6.4.3 Connectivity Test

We add our router's IP as as the default gateway for the computers connected to the router. We perform ping tests from the router to the other devices of the network. Finally, we fill in a table with the following information:

- the destination IP address;
- the packet loss, and;
- the average delay.

Now we repeat the tests from the computer. If we are on a Linux box, we may also try the `tracepath` and `mtr` commands. We will include the configuration of the switch and the router in the lab assignment report.

Chapter 7

Firewall

The goals of this assignment are the following.

- Familiarizing ourselves with firewalls.
- Correctly configuring the different options.
- Configuring a local area network, establishing different security polices using filtering and traffic monitoring.
- Solve a case study about connecting a Small/Medium Enterprise (SME) network to the Internet using a firewall.

7.1 Home Preparation

The Cisco firewall can be configured using a Java program which is called *Adaptive Security Device Manager* (ASDM). This tool makes it possible to interact with the firewall using a graphical user interface (GUI) on a computer with the Windows operating system.

Read more from the following document: `www.jaumebarcelo.info/teaching/lxs/ipsec/ASA_Getting_Started.pdf` Read also all the assignment and prepare a solution for the *case study*.

You can download a copy of the Cisco ASDM software from the following link. `https://www.dropbox.com/s/5yjqflzvgrlere0/asa.zip`

In the beginning, we can familiarize ourselves with the Adaptive Security Device Manager (ASDM) software using a demo version. The software requires the Java Runtime Environment (JRE) version 1.6.18. After installing and launching the program, select the Run in Demo Mode checkbox and choose the desired demo version. The version we use during this practice is 5.2.

7.2 Configuring the working place

For this practical exercise, each group needs 3 computers and a Cisco ASA 5505 firewall. Connect one of the computers to switch B via the patch panel. Before disconnecting this computer from the Internet,

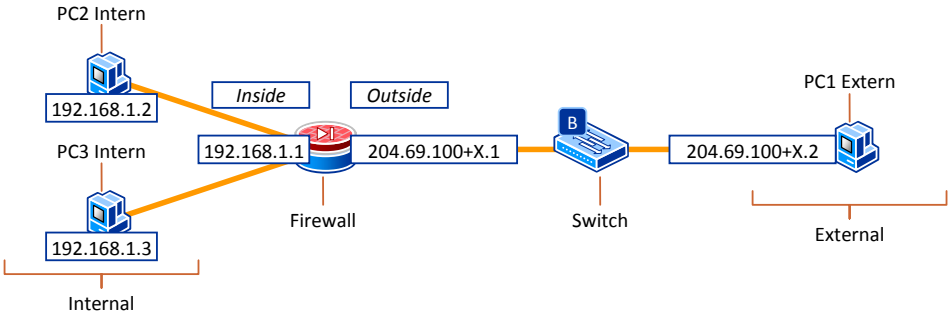

Figure 7.1: *The network topology for the firewall lab assignment.*

download an FTP server such as *Filezilla*. Connect the other two computers to the two internal ports of the firewall (ports 2 and 3).

Connect the firewall to the switch B via the patch panel. Configure the IP address on the external interface (*outside*) of the firewall according to the figure 7.1, where *X* is the number of your group. Configure the default gateway of the three computers with the IP address of the corresponding firewall interface, internal (*inside*) for the internal computers and external (*outside*) for the external computers.

We shall use the FTP to verify that our network configuration works. Identify the transport layer protocol and the port number for FTP.

7.3 Adaptive Security Device Manager (ASDM)

We will find the *ASMD launcher* on the desktop. The default username and password are blank. The default IP address of the firewall is 192.168.1.1 .

The CISCO ASA firewalls assign a *security level* to the interfaces. A security level of 100 means the interface is 100% trusted. A security level of 0 means that the interface is not trusted at all. We shall check the interfaces available and their security level. Discuss the appropriateness of this configuration.

We try to ping between the two computers connected to the internal interfaces.

Question
Does it work? Why?

7.4 Default Configuration of the ASA 5505

The Cisco ASA use the same OS that the other devices used in the previous assignments, the Cisco IOS. Open the Options >Preferences menu and check the Preview commands before sending them to the device option. This will show us the equivalent commands that would be used on the console to change the configuration.

Explain which is the default configuration of the firewall. Observe and explain the different aspects that can be configured using the icons on the left hand side of the screen.

Questions
What is the default configuration of Ethernet 0/0 (outside)?
Why do you thing that the router ships with this configuration?

Now, we will change the IP address of the Ethernet 0/0 (*outside*) interface to 204.69.100+X.1. Remember that the X is the group number, and use a /24 network mask. Now we connect the external computer (via

switch B) to the *outside* interface. We configure the IP of the external computer to an address of the outside range and we set the firewall's outside address as the computer's default gateway.

Questions
Can you ping from the outside PC to an inside PC? Why?
What is the difference compared to the previous case?

Look at the Syslog from the Home screen to answer this questions.

7.5 Firewall

An alternative configuration option is Telnet. We can enable the Telnet options from the ASDM configuration page using Properties >Device Access >Telnet. We have to make sure that we have applied the changes. Now we connect to the device using a Telnet client and `cisco` (small letters) as a password.

We try the

```
# who
```

command to see who is connected to the firewall.

```
# show run
```

to see the running configuration. Find information about Telnet and DHCP and explain it. We also try the commands

```
# show interface
```

and

```
# show traffic
```

and explain the information that they provide.

Discuss the security implications of connecting using Telnet of the console.

7.6 The Hosts/Networks Table

In the Network Objects/Groups tab (from the Configuration >Global Objects page) we can view, edit, add and delete hosts and networks lists defined for every interface. The hosts and networks are organized according to the interface they are connected to (inside/outside). It is recommended to name all the hosts we are managing.

We add the two internal computers by selecting Add >Network Object.... The network mask is 255.255.255.255, as it is a single host. Add also a corresponding object for the external computer. We apply to save the changes.

7.7 Access Rules

The access rules make it possible to establish security policies as a list of rules. The tables to specify how a computer interacts with another by allowing and denying specific services and protocols. We try to connect from the inside computer to the outside computer and explain the behavior and the default Access Rules (from the Configuration >Security Polivy page) table for the inside interface.

The rules are examined sequentially until one of the applies. If the first rule applies, the second is not checked. If the first rule does not apply, then the second is checked. The process is repeated until one of the rules applies.

Question
The last rule is *any to any deny*. Why?

The first rule allows traffic from any IP source to any IP destination if the destination interface has a lower security level. If this rule does not apply, the second rule is examined. The second rule always applies and discards the packet.

We shall observe and explain the rules for the traffic arriving to the external interfaces. To understand the rules, we will pay attention to the graphical diagrams offered by the software.‘

We shall install and configure the FTP server to the external computer. Remember that it is needed to add a folder.

Question
Is it possible to access the FTP server from the internal computers?

Use the rules to deny the access to the FTP server to one of the internal computers and allow access to the other. Observe the log messages to verify that access is being denied. Each time that you change the configuration and try to access to the ftp server, clean the browser cache.

7.8 Translation Rules

The ASA 5505 supports both network address translation (NAT) which is a one-to-one address translation (one inside to one outside) and port address translation (PAT) which is a many-to-one address translation. Look at the default configuration for the translation rules.

Questions
How does this configuration affect outgoing traffic?
What is the IP address used after the packets traverse the firewall?

7.9 Monitoring

We can use the ASDM for network monitoring. It allows to select the message supervising level. Check the Telnet connections and connected users using the options of the menu on the left. There is also a tool to generate graphs such as traffic, memory and CPU. Look at some of the graphs and enumerate them.

7.10 Case Study

An enterprize has a C class network 204.69.100+X.0 and wants securely connect their internal network to an external network. The address of the outside firewall interface is 204.69.100+X.1.

In the internal network there is an FTP server with address 192.168.1.4 that needs to be accessed from the outside network using the address 204.69.100+X.4.

The other requirements are that internal users must be able to ping external devices, but not the other way around.

We shall configure the firewall to satisfy the above requirements. Explain the changes that we have made and the tests performed to verify the correctness of the configuration.

Chapter 8

Final Project

In this project we will configure a network combining the different technologies that we have learned along the course. We will extend the topology in the routing assignment with wireless connectivity (WLAN) and security (Firewalls,IPSec) and traffic monitoring (Wireshark).

8.1 Topology

The topology that we will construct is presented in Fig. 8.1. As in the routing assignments, each group will configure a part of the topology. In this assignment, each group will take care of a router, a firewall, a switch, an access point and the necessary PCs. This topology interconnects secured networks (behind a firewall) with another network that offers access to the Internet. Each secured network needs at least a PC and an FTP server.

8.2 Equipment and addresses

The assignment of equipment and addresses to the groups is detailed in Table 8.1. The switches are shared and the table specifies the ports for each group. The IP addresses for WiFi devices, Ethernet devices, the FW interior interface and the public addresses are also included.

Note that the in the interior networks we use a 23 bits netmask. This means that both WiFi stations and Ethernet stations are in fact in the same subnet.

For the serial links with public addresses between routers

8.3 Security guidelines

We will imagine that each team is configuring a company site. There will be two companies and three sites per company. The security guidelines are as follows:

- The internal PCs should be able to connect to the internal FTP server.
- The PCs of other sites of the same company should be able to connect to our FTP server.

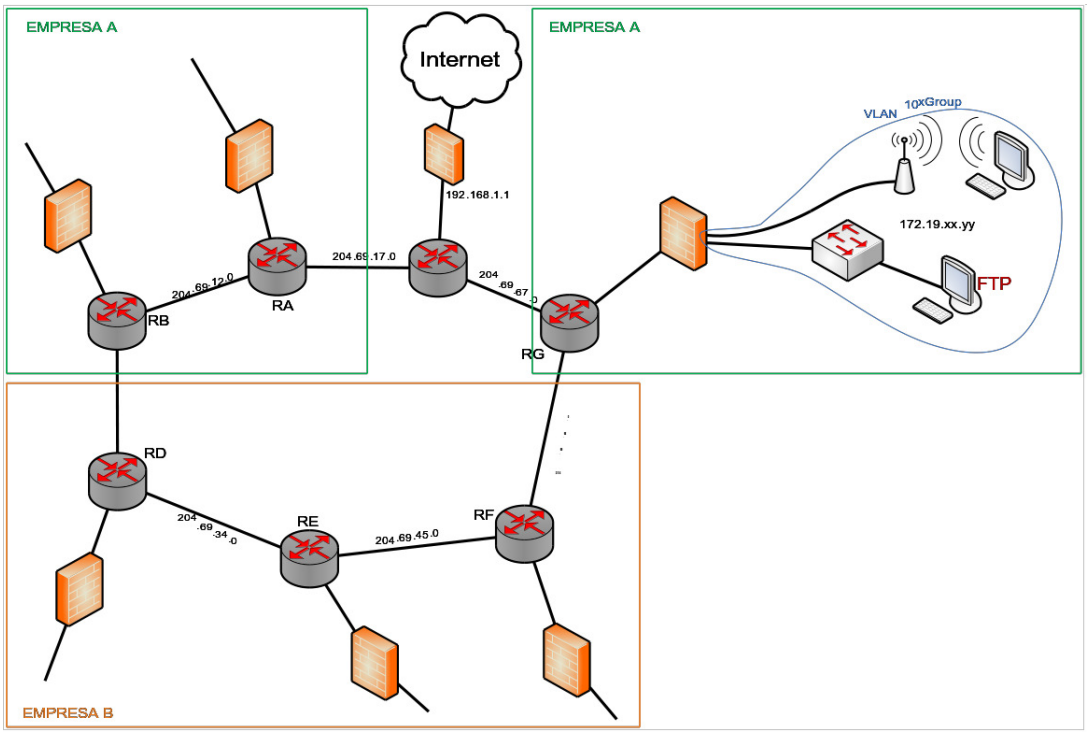

Figure 8.1: *Topology of the final assignment*

Group	Router	Switch	Ports	IPs WiFi	IPs Eth	FWin	IPs public
1	A	B	1-6	.80.1X/23	.81.1X/23	.80.1/23	201.69.10.0/24
2	B	B	7-12	.82.1X/23	.83.1X/23	.82.1/23	201.69.20.0/24
3	D	C	1-6	.84.1X/23	.85.1X/23	.84.1/23	201.69.30.0/24
4	E	C	7-12	.86.1X/23	.87.1X/23	.86.1/23	201.69.40.0/24
5	F	D	1-6	.88.1X/23	.89.1X/23	.88.1/23	201.69.50.0/24
6	G	D	7-12	.90.1X/23	.91.1X/23	.90.1/23	201.69.60.0/24

Table 8.1: *Equipment and addresses*

- The PCs of sites of the other company should not be able to connect to our FTP server.
- Our PCs should be able to ping outer hosts.
- It should not be possible for outer PCs to ping our hosts.
- PCs should have Internet connectivity.

8.4 Device configuration

We have to configure the devices in our site:

- Switch: Creating the VLANs and assigning ports.
- Router: Serial and ethernet interfaces. Routing protocol.
- AP: Basic configuration.
- Firewall: NAT translation, filtering rules, inside and outside interface.

To configure the switch, you need to be connected to VLAN1. To configure the router, you can use the console connection. To configure the FW and the AP, you can directly connect to them.

8.5 Home preparation

Find which ranges of IP are private addresses. Find information about Classless Inter-Domain Routing and what is the difference between /23 and /24.

Questions
Do the addresses assigned to WiFi and ethernet devices belong to the same subnet? Why?
What is the explanation for the IP address for the internal interface of the FW?

Fill in Fig. 8.1 with the configuration information (port, switch, IPs, NAT, firewall rules, etc.)

8.6 Steps and checkpoints for device configuration

- Step: Study the configuration.
- Checkpoint: Complete the configuration information on the figure.
- Step: Configure the switches (VLANs and ports).
- Checkpoint: VLANs created and ports assigned.
- Step: Configure the FW interfaces.
- Checkpoint: Ping the FW from the PC.
- Step: Configure the router (interfaces, RIP, routes, etc.)
- Checkpoint: ping from the router to the firewall, ping between routers, routing table, ping between firewalls.
- Configure the FW rules and NAT.

More details in Section 8.9

8.7 Lab report

The lab report should include both the devices configuration and the validation tests. As a minimum, it should contain:

- Complete network figure with all the IPs, VLANs, ports, etc.
- Configuration
  - Routing tables.
  - NAT and filtering rules configuration.
  - Use the appendixes for snapshots.
- Tables with results of the validation tests (connectivity, delay, throughput, etc.)

8.8 Optional assignments

Configure the firewall to prevent that wireless stations connect to the FTP server. Create a VPN between the sites of the company.

8.9 Final tips

The IPs of the switches are:

- A: 192.168.1.111
- C: 192.168.1.112
- D: 192.168.1.113

The DNS of the upf is 193.145.56.11

8.9.1 Firewall configuration

j

- Connect the PC to the FW (inside)
- Enable https access to the network 172.19.XX.0
- Change the inside interface address to 172.19.XX.XX/23 . We will lose connectivity.
- Change the IP of the PC to 172.19.XX.XX/23. Default gateway is the inside interface of the FW. Restart ASDM.
- Change the external IP of the firewall to 204.69.XX.XX/24
- Add a static default route at the outside interface of the FW. 0.0.0.0-0.0.0.0 with the router interface as a gateway.

8.9.2 Router configuration

- Configure the IP of the ethernet interface.
- Configure the IP of the serial interfaces. 204.69.XX.XX/24 clockrate 200.000
- Add RIP to the routers. Add all networks. Check routing table.
- Configure Internet access. Add an static route to the gateway of the lab. ip route 0.0.0.0 0.0.0.0 192.168.1.1

8.9.3 Access point configuration

- Change the IP of the AP and set the FW as the default gateway. Use the console to change the IP address of the interface bvi1.
- Make sure that HTTP access is enabled.
- Connect the AP to the firewall.
- Use a PC with wired connection and the browser to connect to the AP. Configure the gateway. Configure also the wireless network (SSID, broadcast, radio interface up).
- Add a DHCP server to the FW to serve address to wireless PCs. Properties → DHCP → DHCP Server → Configure IP range and DNS.

Bibliography

[1] D. Plummer. Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware. RFC 826 (Standard), November 1982. Updated by RFCs 5227, 5494.