

FACULTAD DE CIENCIAS
UNIVERSIDAD DE CANTABRIA



Proyecto Fin de Carrera

Desarrollo de un Sistema de Control de Accesos a Red para los Laboratorios de la Facultad de Ciencias

(Development of a Network Access Control Application for the
Computer Classrooms of the Faculty of Sciences)

Para acceder al Título de
INGENIERO EN INFORMÁTICA

Autor: Manuel Pando Muñoz
Julio 2011



El Dr. Ing. Don Pablo Sánchez Barreiro, Ayudante Doctor del Área de Lenguajes y Sistemas Informáticos de la Facultad de Ciencias de la Universidad de Cantabria,

Certifica que D. Manuel Pando Muñoz, alumno de Ingeniería Informática, ha realizado en el Departamento de Matemáticas, Estadística y Computación de la Universidad de Cantabria, bajo mi dirección, el Proyecto Fin de Carrera titulado:

Desarrollo de un Sistema de Control de Accesos a Red para los Laboratorios de la Facultad de Ciencias

Revisado el presente trabajo, estimo que puede ser presentado al tribunal que ha de juzgarlo, y autorizamos la presentación de este Proyecto Fin de Carrera en la Universidad de Cantabria.

Santander, Junio de 2011

Fdo.: Pablo Sánchez Barreiro
Ayudante Doctor del Área de Lenguajes y Sistemas Informáticos.



FACULTAD DE CIENCIAS

INGENIERÍA EN INFORMÁTICA

CALIFICACIÓN DEL PROYECTO FIN DE CARRERA

Realizado por: Manuel Pando Muñoz
Director del PFC: Pablo Sánchez Barreiro
Título: Desarrollo de un Sistema de Control de Accesos a Red para los Laboratorios de la Facultad de Ciencias
Title: Development of a Network Access Control Application for the Computer Classrooms of the Faculty of Sciences
Presentado a examen el día:

para acceder al Título de
INGENIERO EN INFORMÁTICA

Composición del Tribunal:

Presidente (Apellidos, Nombre):
Secretario (Apellidos, Nombre):
Vocal (Apellidos, Nombre):
Vocal (Apellidos, Nombre):
Vocal (Apellidos, Nombre):

Este Tribunal ha resuelto otorgar la calificación de:

Fdo.: El Presidente

Fdo.: El Secretario

Fdo.: Vocal

Fdo.: Vocal

Fdo.: Vocal

Fdo.: El Director del PFC

Agradecimientos

A Pablo Sánchez Barreiro por ofrecerme la posibilidad de realizar este proyecto y resolver las dudas que iban surgiendo.

A los compañeros de clase que han hecho pasar estos cinco años muy rápido.

A mi familia cercana por el apoyo incondicional y los ánimos transmitidos durante toda la vida.

A los amigos íntimos, especialmente a Sergio y a Sergio, sin ellos dos no sería quien soy actualmente, estoy orgulloso de tenerlos como amigos.

Después de cinco años puedo asegurar que esta etapa ha sido una de las más felices de mi vida y me considero afortunado de haberla podido vivir, a todos, muchas gracias.

Resumen

El presente Proyecto de Fin de Carrera, perteneciente a la titulación de Ingeniería en Informática de la Universidad de Cantabria tiene como objetivo implementar un sistema de control de acceso a red durante el transcurso de pruebas evaluables en salas con computadores.

Si partimos de la base de que el deseo de los profesores es conseguir que sus alumnos aprendan y que la meta de las pruebas evaluables es determinar el grado de conocimiento de los alumnos en cierta materia, si el alumno puede consultar contenidos online o comunicarse con otros y la prueba no ha sido diseñada para permitir esto, se puede asegurar que los resultados no serán reales y ciertamente no ayuda al aprendizaje del estudiante.

Por tanto, tener un sistema que asegure el cumplimiento de los términos de la prueba y que además se aproveche de la gran utilidad que tienen las redes de computadores para hacer más cómodas ciertas tareas, parece bastante deseable. La creación de ese sistema es el objetivo de este proyecto.

Como resultado de la realización del proyecto se ha desarrollado un software que consta de una aplicación a ejecutar en el computador utilizado por el docente y otra a ejecutar en el computador de cada alumno que pretende realizar la prueba de modo que, desde la primera, se pueda tener control sobre la segunda.

Ambas aplicaciones han sido desarrolladas en Java, con interfaces gráficas simples para tratar de que el uso de los programas sea lo más intuitivo posible.

Palabras clave: Cortafuegos, Control de acceso red, Distribuido, Linux, Java

Preface

This Master Thesis aims to develop a network access control system for enabling and disabling access to the local network, during the tests conducted with computers in the University of Cantabria.

Teacher's ultimate goal is to promote their student's learning. The goal of test is simply to measure somehow the skills of a student regarding a certain subject. Thus, if the student can find on internet the solution to certain questions he or she should solve by him o herself, or, similarly, if the student can communicate with others students using the network, we cannot ensure the results of the test reflect his or her skills actually . Therefore, we cannot assess properly when the student is truly learning.

So, having a system that ensures compliance with the terms of the test, and can also take advantage of the network to automate and make more comfortable certain tasks, seems quite desirable. The goal of this project is to create such a system.

The result of this project was the development of a distributed software, comprise of two different applications. The first one runs on the teacher's computer. The the second is executed on the computer of every student doing the test. The teacher can control the student's access to the network using his or her application. So, the teacher can grant access to the network to the students, for instance, for distributing automatically some auxiliar material required for the test, as well as deny access to the network.

Both applications have been developed using the Java programming language, with simple graphical interfaces which aims to be as intuitive as possible.

Keywords: Firewall, Network access control, Distributed, Linux, Java

Índice general

1. Introducción	1
1.1. Introducción	1
1.2. Estructura del Documento	1
2. Descripción y Planificación del Proyecto	5
2.1. Descripción Funcional del Sistema	5
2.2. Metodología de Desarrollo	7
2.3. Requisitos de Alto Nivel del Sistema	9
2.4. Iteraciones	10
2.5. Construcción	12
2.6. Sumario	13
3. Antecedentes	15
3.1. Red local	15
3.2. Cortafuegos : Netfilter/iptables	16
3.3. Demonio	16
3.4. MD5	17
3.5. Sumario	17
4. Definición Arquitectónica y Diseño Software	19
4.1. Vista lógica de la arquitectura	19
4.2. Diseño Software	20
4.3. Sumario	23
5. Creación del sistema distribuido base	25
5.1. Incrementos realizados	25
5.1.1. Interfaces gráficas	27
5.1.2. Conexión	27
5.1.3. Envío de ficheros	28
5.2. Pruebas	30
5.3. Sumario	31

6. Comienzo de prueba y denegación de acceso a red	33
6.1. Incrementos realizados	34
6.1.1. Inicio de la prueba	34
6.1.2. Examen temporizado	35
6.1.3. Denegar acceso a red	35
6.2. Pruebas	37
6.3. Sumario	38
7. Despliegue y aceptación	39
7.1. Despliegue	39
7.1.1. Página web	41
7.2. Pruebas	41
7.3. Sumario	44
8. Conclusiones y Trabajos Futuros	45
8.1. Conclusiones	45
8.2. Trabajos futuros	46
A. Contenidos del CD	47
Bibliografía	49

Índice de figuras

2.1. Diferencia entre iteración e incremento.[PK06]	8
2.2. Carga de trabajo en las diferentes fases.[Kru03]	9
2.3. Diagrama de casos de uso del sistema	10
4.1. Diagrama de componentes	19
4.2. Diagrama despliegue del sistema	20
4.3. Diagrama de actividad del sistema	21
4.4. Diagrama de estados de la aplicación del alumno	22
5.1. Casos de uso a implementar	27
5.2. Interfaz de la aplicación profesor	28
5.3. Interfaz de la aplicación alumno	29
5.4. Diagrama de secuencia caso de uso conectar	29
6.1. Aspecto de la GUI del alumno con una prueba temporizada.	36
7.1. Página web del proyecto.	42

Índice de cuadros

2.1. Requisitos de alto nivel del sistema	11
5.1. Requisitos objetivo de la iteración	26
5.2. Requisitos objetivo refinados de la iteración	26
6.1. Objetivos de la iteración	34
6.2. Requisitos ya implementados del sistema	34
6.3. Objetivos refinados de la iteración	35

Capítulo 1

Introducción

Este documento es la memoria de Proyecto de Fin de Carrera en el que se muestra el proceso realizado para construir una aplicación de control de accesos a red durante pruebas evaluables. Tras una breve introducción al problema que se pretende resolver se describe la estructura del documento.

Índice

1.1. Introducción	1
1.2. Estructura del Documento	1

1.1. Introducción

Actualmente cuando se desea que un alumno no tenga acceso a la red durante pruebas evaluables, la solución es desconectar el router o switch del laboratorio, algo que sin duda es efectivo, pero neutraliza un recurso que utilizado correctamente puede ser muy útil, por ejemplo, el tener todos los computadores de una sala interconectados permite que el profesor pueda, con un gasto en tiempo muy reducido, enviar el enunciado de la prueba o ficheros necesarios en general a todos los alumnos. Algo parecido ocurre cuándo se trata de entregar los resultados, si utilizamos el método de desconectar físicamente la red, el profesor ha de utilizar algún tipo de dispositivo de almacenamiento para recoger, individual y secuencialmente los resultados de cada alumno, sin embargo, si se utiliza la red, un alumno decide cuándo enviar los resultados, sin importar si otro está haciendo lo mismo simultáneamente. El ahorro en tiempo es considerable, además se pueden realizar comprobaciones a los ficheros enviados para garantizar que son correctos, ya que es un material bastante sensible, cosa que no es posible si se recogen por medio de dispositivos de almacenamiento.

1.2. Estructura del Documento

A continuación se hace un breve resumen de los contenidos a tratar en capítulos posteriores del documento.

Capítulo 2: Descripción y Planificación del Proyecto

Se describe el ámbito funcional del proyecto y la metodología escogida para su construcción. De acuerdo a ella se realiza una planificación y se enumeran los requisitos de alto nivel que el software a desarrollar ha de cumplir, así como las herramientas a utilizar durante el diseño y desarrollo.

Capítulo 3: Antecedentes

Se explicarán brevemente conceptos básicos que utilizará la solución a crear y su utilidad cuándo esté completado el proyecto.

Capítulo 4: Definición Arquitectónica y Diseño Software

Se explicarán mediante diagramas UML la arquitectura y el diseño propuestos para que la aplicación a desarrollar sea correcta y segura en el cumplimiento de los requisitos, además de para tener una visión global de su funcionamiento.

Capítulo 5: Creación del sistema distribuido base

En este capítulo se describirá el proceso realizado en la primera iteración de la fase de construcción de acuerdo a lo explicado en el capítulo 2 sobre la metodología. En esta primera iteración se crea un sistema distribuido base, dónde el profesor puede enviar ficheros a sus alumnos.

Capítulo 6: Comienzo de prueba y denegación de acceso a red

Se describirá en este capítulo la iteración continuación a la explicada en el capítulo anterior que tiene como principal objetivo el de denegar el acceso a la red una vez que el profesor decide iniciar la prueba.

Veremos cómo gracias a seguir una metodología, el desarrollo se convierte en un proceso repetitivo que si es realizado correctamente disminuirá posibles fallos y por tanto, aumentará la calidad de la solución desarrollada.

Capítulo 7: Despliegue y Aceptación

Se describirá el proceso de despliegue escogido, consistente en el empaquetamiento del software creado para posibilitar una cómoda distribución y de las pruebas realizadas una vez que se ha finalizado el desarrollo del sistema.

Capítulo 8: Conclusiones y Trabajos Futuros

Se finalizará la memoria exponiendo conclusiones y enumerando una lista de posibles líneas de desarrollo futuras.

Capítulo 2

Descripción y Planificación

El presente capítulo describe en líneas generales el ámbito funcional del proyecto, para delimitar su alcance, la metodología a usar durante el desarrollo del sistema y los requisitos de alto nivel del mismo, extraídos del ámbito funcional descrito.

Índice

2.1. Descripción Funcional del Sistema	5
2.2. Metodología de Desarrollo	7
2.3. Requisitos de Alto Nivel del Sistema	9
2.4. Iteraciones	10
2.5. Construcción	12
2.6. Sumario	13

2.1. Descripción Funcional del Sistema

En la siguiente sección se describe el ámbito funcional del sistema software que deseamos construir, es decir, del *DrManhattan*, que es un *Sistema de Control de Accesos a Red para los Laboratorios de la Facultad de Ciencias*.

El objetivo del *DrManhattan* es controlar el acceso a la red local, existente en cada laboratorio de la Facultad de Ciencias de la Universidad de Cantabria, de los computadores conectados a ella. Se desea realizar dicho control sobre todo durante la realización de pruebas evaluables, de cara a evitar que se realicen accesos a contenidos no autorizados (e.g., páginas de internet con posibles soluciones a los problemas planteados, el directorio de trabajo de algún compañero, etc.) durante la realización de dichas pruebas. El sistema que se venía utilizando hasta ahora para evitar el mal uso de la red local consistía simplemente en desconectar la alimentación del concentrador de interconexión, deshabilitando la red. Es decir, se aplicaba el principio de muerto el perro, se acabó la rabia.

No obstante, el tener los diversos computadores interconectados mediante una red local, no sólo tiene inconvenientes, sino que también posee varias ventajas. Por ejemplo, ayuda a facilitar la distribución de material electrónico que resulte necesario para la realización del examen. También puede ser de gran utilidad para recoger los ejercicios realizados por los alumnos de una manera rápida y cómoda, ya que el alumno sólo tendría que enviar el material producido durante la prueba al computador o dirección que le indique el profesor. El método utilizado actualmente para realizar esta tarea consiste en que el profesor acude al computador del alumno cuando este desea entregar los ejercicios realizados y copia tales ejercicios en una memoria USB. Este proceso es lento, tedioso y en muchas ocasiones las memorias USB no son reconocidas por los computadores del laboratorio, lo que exige recurrir a otras técnicas. El tiempo empleado por los docentes para recopilar los ejercicios realizados por los alumnas suele oscilar entre la media hora y la hora completa, mientras que usando la red local dicho proceso podría realizarse en cuestión de minutos (cuando no menos).

Por tanto, el acceso de los computadores a la red local (e internet), se deberá controlar desde un computador distinguido, al que llamaremos *Watchman*, que será normalmente el computador asignado al docente. Dicho computador será el encargado de conceder y denegar el acceso a la red al resto de computadores conectados a la red local.

Se desea que el acceso a la red esté habilitado en las siguientes circunstancias:

1. Al comienzo de la realización de las pruebas, de forma que el docente pueda distribuir material electrónico necesario o de interés para la realización de la prueba (e.g., manuales, el enunciado de la prueba, etc.) entre los diferentes computadores de forma cómoda y eficiente.
2. Cuando el alumno haya finalizado la prueba, de forma que se puedan enviar los resultados a través de la red, evitando el tedioso proceso de tener que recogerlos de forma individual mediante copia en un memoria USB o dispositivo similar. En estos casos, sería además deseable, con objeto de evitar posteriores problemas, que el sistema comprobase la integridad de los archivos recibidos, es decir, que comprobase que no se han sufrido alteración alguna durante la transmisión.

Durante el periodo de tiempo que un alumno esté realizando una prueba, se debe denegar el acceso a la red del computador que esté utilizando para la realización de la prueba.

Por tanto, la secuencia de realización de una prueba evaluable sería tal como sigue:

1. El profesor y los alumnos acceden al aula y encienden sus correspondientes computadores. El acceso a la red está habilitado para todo el mundo.
2. El profesor envía el material necesario para la realización de la prueba a los computadores de los alumnos.
3. A continuación, una vez que un alumno comienza la prueba, se le deniega el acceso a la red al computador que esté utilizando.

4. Si durante la realización de la prueba un alumno considera que ha acabado y está satisfecho con los resultados producidos, indicará al sistema que ha concluido la prueba. Los ficheros producidos como material evaluable se enviarán al *Watchman*. Se comprobará que se han recibido correctamente y no están corruptos, por lo que se pueden abrir y leer sin problema alguno. Obviamente, para el envío de los ficheros de resultados habrá que habilitar de nuevo la red, pero se ha de evitar que el alumno pueda modificar dichos ficheros.
5. Debe existir también la posibilidad de que el docente decida que el tiempo de realización de la prueba ha concluido, por lo que deberá realizarse todo el proceso descrito en el punto anterior, pero para todos los computadores que se encuentren activos en ese momento y siendo el proceso iniciado desde el *Watchman*, en lugar de desde el propio computador del alumno.

Además, se guardarán registros de los eventos ocurridos en cada prueba, con el objetivo de tener información que permita auditar el transcurso de la misma. Dicho registro debe mantener constancia de eventos tales como hora de inicio de la prueba, hora de entrega de cada ejercicio, número de ficheros que se entregan, etc.

Para comodidad del alumno, en las pruebas con hora de finalización predeterminada se mostrará en la interfaz de la aplicación los minutos restantes hasta el final.

La siguiente sección detalla la metodología de desarrollo que usaremos para la construcción de este sistema.

2.2. Metodología de Desarrollo

En esta sección se describe la metodología utilizada para desarrollar el sistema.

Se ha escogido el proceso de desarrollo *iterativo e incremental* que suele ser parte esencial en las metodologías de desarrollo ágiles[Lar03].

La idea principal de este proceso se basa, como su nombre, en iteraciones e incrementos, que no son lo mismo. El software se construye mediante tareas repetitivas, *iteraciones*, en las que se añaden nuevas funcionalidades progresivamente, *incrementos*, para crear una versión del sistema que cumple más requisitos que la anterior. Se realizan tantas iteraciones sean necesarias hasta que todos los requisitos se hayan implementado y, por tanto, el sistema este finalizado.

Es decir, una iteración es un mini-proyecto en el que se obtiene una versión de cada una de las piezas del sistema, sean código o no, y un incremento se puede medir como la diferencia entre una iteración y la anterior. En la figura 2.1 se muestra visualmente esa diferencia.

El proceso se divide en cuatro partes fundamentales:

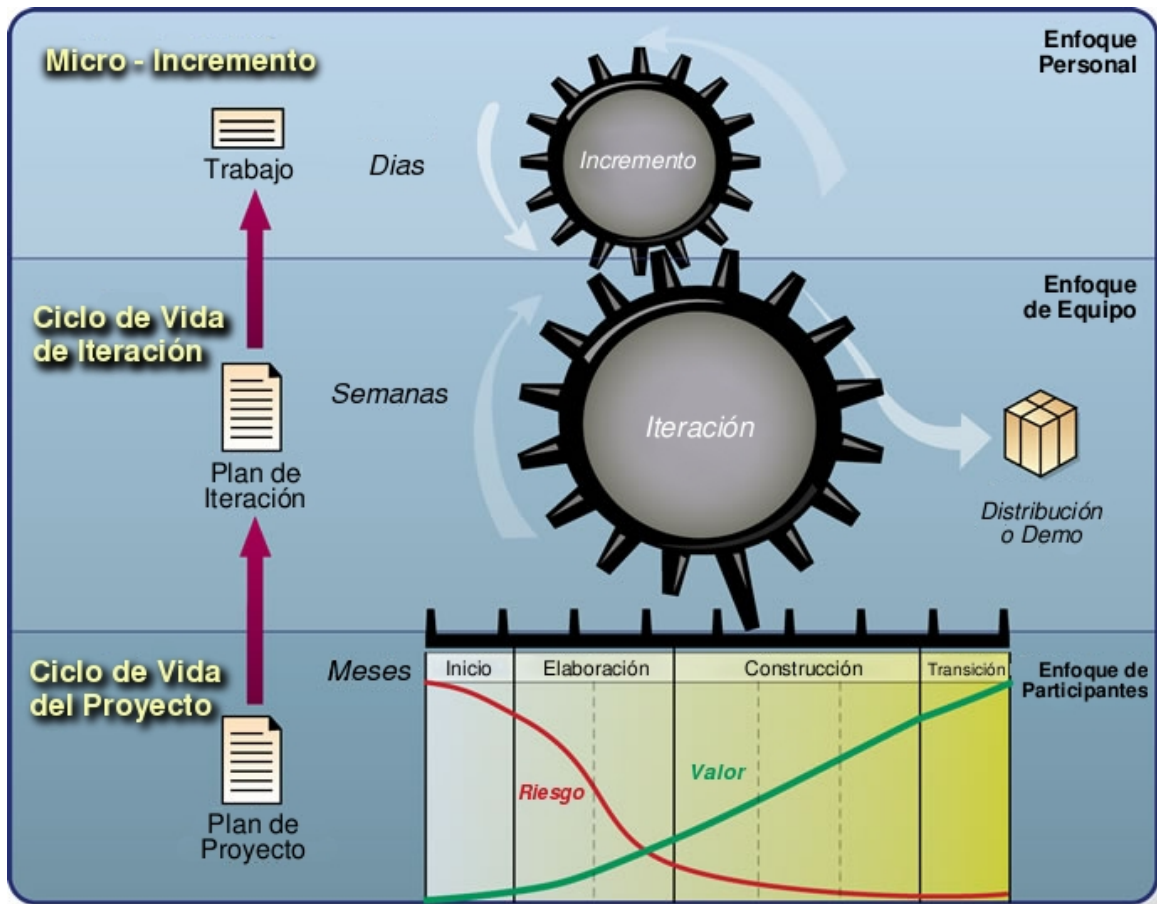


Figura 2.1: Diferencia entre iteración e incremento.[PK06]

1. **Iniciación:** en esta fase se describe el ámbito funcional del sistema, los requisitos de alto nivel y se identifican posibles riesgos. Hay que comprender el sistema y sus límites.
2. **Elaboración:** el objetivo principal de esta fase es el de crear la arquitectura básica, para tener una visión de cómo será el sistema completo y además, proponer soluciones a los riesgos identificados.
3. **Construcción:** cómo su nombre indica, esta es la fase dónde se construye y prueba la aplicación. Se realiza un pequeño proceso en cascada en cada iteración de esta fase.
4. **Transición:** se despliega el sistema y finaliza el proceso.

Cada una de estas fases, como es lógico, puede tener más de una iteración, en función del tamaño del proyecto, con tareas propias de la etapa en que se esté, así por ejemplo, en la etapa de construcción, en cada iteración se escoge un grupo de requisitos de alto nivel, se refinan, y partiendo de la versión del sistema obtenida en la iteración anterior, se diseñan, implementan y prueban esos requisitos, creando la versión que se utilizará en la siguiente

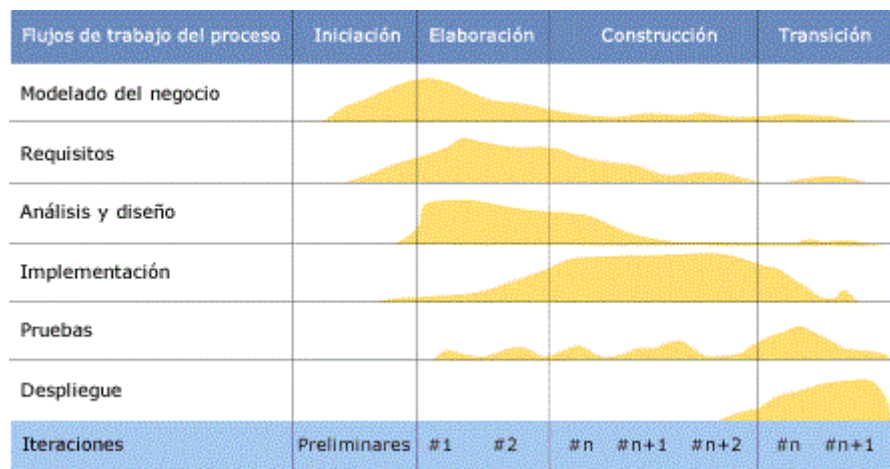


Figura 2.2: Carga de trabajo en las diferentes fases.[Kru03]

iteración. En la figura 2.2 se muestra una aproximación de lo que sería la carga de trabajo que requieren las distintas tareas en función de la etapa en que se encuentre el proyecto.

Al finalizar el proceso obtenemos tanto el código de la aplicación, como modelos y documentación de la misma que se van creando a lo largo de las iteraciones.

Las principales razones por las que se ha escogido este tipo de proceso y no otro son:

- ◆ Poca incertidumbre a la hora de diseñar y planificar, ya que al realizarse en cada iteración y no del sistema completo, se tiene mayor comprensión de los riesgos y de las tareas a realizar.
- ◆ Se adapta bien a cambios de requisitos.
- ◆ Si se priorizan los requisitos para implementarlos en las primeras iteraciones de la construcción, se obtiene una aplicación con funcionalidades clave en la que el cliente puede decidir si está o no correcto.
- ◆ Al trabajar con un subconjunto de requisitos en cada iteración la complejidad se reduce, lo que facilita que se reduzca también el número de errores producidos.

De la primera fase, *iniciación*, la descripción funcional detallando el alcance del sistema está descrita en la sección 2.1, a continuación se muestra un diagrama de casos de uso, basado en esa descripción y en la siguiente sección se describen los requisitos de alto nivel extraídos.

2.3. Requisitos de Alto Nivel del Sistema

Esta sección describe el segundo paso en nuestro proceso de desarrollo, de acuerdo a la metodología descrita en la sección anterior, que es la identificación de los requisitos de alto

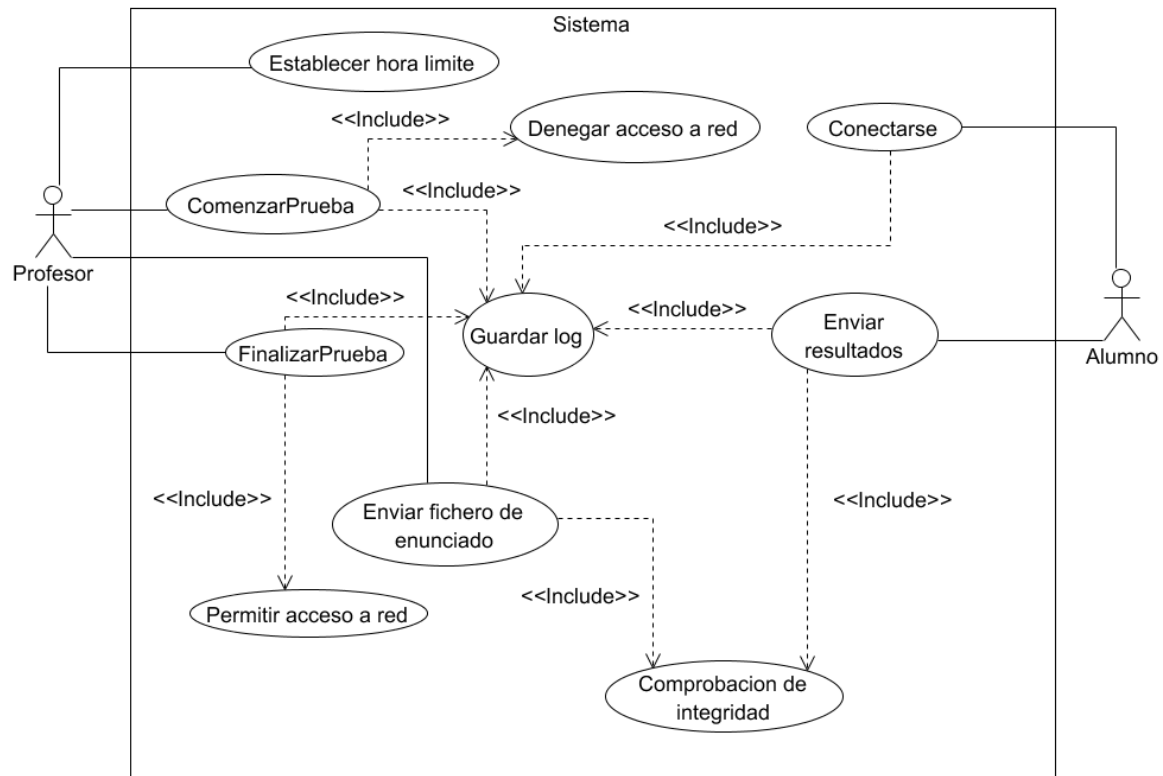


Figura 2.3: Diagrama de casos de uso del sistema

nivel que ha de satisfacer nuestro sistema software, de acuerdo a la descripción del ámbito funcional proporcionada en la Sección 2.1.

En concreto, se han identificado los requisitos de alto nivel para nuestro sistema expuestos en la tabla 2.1.

2.4. Iteraciones

En esta sección se describen las iteraciones previstas para el desarrollo de la aplicación.

▪ Iteración 1: Crear un sistema distribuido[AST06].

- Requisitos implementados: R06, R07
- Descripción: En la primera iteración la aplicación del alumno se podrá conectar al watchman para esperar el inicio de la prueba, envío de ficheros etc... y el profesor es capaz de enviar el enunciado.

▪ Iteración 2: Denegar acceso a red una vez comenzada la prueba.

Identificador	Descripción
R01	Un computador de la red debe poder ser designado como <i>Watchman</i> .
R02	Todos los computadores que no sean <i>Watchman</i> serán computadores normales, y podrán ser utilizados para la realización de las pruebas evaluables.
R03	El profesor debe ser capaz desde el <i>Watchman</i> de indicar el inicio de la prueba.
R04	El profesor debe ser capaz desde el <i>Watchman</i> de indicar el fin de la prueba.
R05	El profesor ha de ser capaz desde el <i>Watchman</i> de establecer una hora límite para la duración de la prueba.
R06	El profesor debe ser capaz desde el <i>Watchman</i> de enviar el fichero de enunciado al resto de computadores.
R07	El alumno desde su computador debe ser capaz de conectarse al <i>Watchman</i> .
R08	El alumno desde su computador debe ser capaz de enviar sus resultados al profesor.
R09	El alumno desde su computador debe ser capaz de indicar que da por finalizada la prueba.
R10	El alumno desde su computador debe tener la posibilidad de ver el tiempo restante el pruebas de duración prefijada.
R11	La aplicación del alumno ha de ser capaz de denegar el acceso a la red al empezar la prueba.
R12	La aplicación del alumno ha de ser capaz de permitir el acceso a la red al finalizar la prueba.
R13	La aplicación ha de ser capaz de comprobar que los archivos se han enviado correctamente.
R14	La aplicación del profesor ha de ser capaz de guardar registros de actividad.

Cuadro 2.1: Requisitos de alto nivel del sistema

- Requisitos implementados: R03, R05, R10, R11
- Descripción: En la segunda iteración el profesor puede establecer una hora límite e indicar el inicio de la prueba. La aplicación del alumno es capaz de denegar el acceso a la red cuando se inicia la prueba y en caso de que la duración este prefijada, consultar el tiempo restante

■ Iteración 3: Habilitar red y enviar resultados

- Requisitos implementados: R04, R08, R09, R12
- Descripción: En la tercera iteración se permite al profesor finalizar la prueba de modo general. Del mismo modo, cada alumno puede finalizar la prueba por su

cuenta y enviar su archivo de resultados al computador del profesor. La aplicación del alumno, cuando este finaliza la prueba, habilita el acceso a la red.

■ **Iteración 4: Comprobación de integridad**

- Requisitos implementados: R13
- Descripción: En la cuarta iteración se implementa el sistema de comprobación de integridad de los ficheros transmitidos por red para garantizar la correcta recepción de los mismos.

■ **Iteración 5: Sistema de logs**

- Requisitos implementados: R14
- Descripción: Definir los mensajes necesarios para cuando en la aplicación ocurre algo que se desee guardar.

En cuanto a los requisitos R01 y R02 están implementados en arquitectura del sistema, no son funcionalidades.

2.5. Construcción

Para el diseño se utiliza el programa Visual Paradigm, versión 8.1 y para la construcción del sistema se ha utilizará el entorno de desarrollo Eclipse 3.5.2[Bur05], en su versión para el lenguaje Java[KA05]. Eclipse es un IDE de código abierto, multiplataforma, en el que se pueden instalar multitud de plug-ins para aumentar sus funcionalidades. Concretamente, para la realización de este proyecto se han usado el Google Web Toolkit en su versión para eclipse 3.5, que facilita mucho la creación de interfaces gráficas de modo visual, y Subclipse, para simplificar el trabajo con el repositorio Subversion[CMP08].

Google Code es un servicio de alojamiento de proyectos ofrecido por Google, que permite alojar código de Subversion de modo que se puede crear fácilmente un sistema de control de cambios, muy útil si se quiere regresar a un estado anterior del programa, recuperar algún objeto borrado, etc.

Las razones principales para trabajar con estas y no otras herramientas son que, todas ellas tienen licencias que permiten usarlas gratuitamente y que ya se tenía cierta experiencia en su uso.

El sistema operativo escogido ha sido Ubuntu 10.10[BH11] de 32 bits y la versión de kernel 2.6.35.

2.6. Sumario

Durante este capítulo se han descrito el ámbito funcional del sistema, para detallar las funcionalidades que ha de cubrir la solución a desarrollar, la metodología a seguir durante el análisis, diseño, desarrollo y despliegue del proyecto, metodología ágil basada en iteraciones e incrementos. De acuerdo a esta metodología se extrajeron los requisitos de alto nivel y se planificaron las iteraciones a realizar en la fase de desarrollo. Para finalizar se expusieron las principales herramientas que se usarán. En el siguiente capítulo se describirán brevemente algunos de los conceptos tecnológicos de los que hará uso el proyecto.

Capítulo 3

Antecedentes

El siguiente capítulo describe brevemente las tecnologías sobre las que se fundamenta el presente proyecto. Más concretamente, se explica el funcionamiento de las redes locales, del framework Netfilter para el filtrado de paquetes, de los demonios en los sistemas Linux[Bar04] y del algoritmo MD5, cuatro aspectos fuertemente relacionados con el proyecto.

La aplicación a desarrollar está pensado que se utilice en los laboratorios de la Facultad de Ciencias de la Universidad de Cantabria, en estos laboratorios los computadores están conectado mediante una *red local* y utilizan sistemas Linux. Para gestionar los permisos de acceso a la red se va a utilizar un *demonio* que interactúe con *Netfilter* por medio de iptables. Para detectar si hay algún problema en la transferencia de los ficheros por la red se utilizará MD5.

Índice

3.1. Red local	15
3.2. Cortafuegos : Netfilter/iptables	16
3.3. Demonio	16
3.4. MD5	17
3.5. Sumario	17

3.1. Red local

Una *Red local* o LAN[Sta04], siglas en inglés de Local Area Network, es un conjunto de computadoras conectadas entre sí en un área relativamente pequeña, como los laboratorios de la Facultad.

Cada uno de estos equipos interconectados en la red se conoce como nodo. Estos nodos son capaces de enviar, recibir y procesar comandos con el fin de transportar datos, así como compartir información y recursos a través de la red.

El funcionamiento de la red está estandarizado siendo el protocolo TCP/IP [Koz05] el más extendido, gracias a esto cualquier equipo que cumple el estándar podrá comunicarse con otros que también lo cumplan, sin importar fabricante o tecnología interna.

3.2. Cortafuegos : Netfilter/iptables

Netfilter es un framework que permite filtrar de paquetes, traducción de direcciones y puertos de red y varias funcionalidades más para el manejo de paquetes. Es parte del núcleo de Linux desde la versión 2.4 del mismo, sustituyendo a ipchains, bastante limitado en comparación con Netfilter.

Para interactuar con Netfilter una de las aplicaciones más usadas es *iptables*[Pur04], siendo necesarios permisos de administrador para ello.

Ejemplo de uso de iptables:

```
# iptables -A INPUT -s 195.65.34.234 -j ACCEPT
```

El parámetro -A indica que se va a añadir una regla, el objetivo de la mismo es aceptar todos los paquetes entrantes provenientes del host indicado¹. Del mismo modo, si lo que queremos es no aceptar las peticiones se cambiaría ACCEPT por DROP y si nos queremos referir a los paquetes salientes OUTPUT por INPUT.

Para cambiar el tratamiento por defecto de un tipo de paquete se puede usar:

```
# iptables -P INPUT DROP
```

Con esta orden conseguimos que por defecto, todos los paquetes entrantes (INPUT) sean rechazados (DROP). Se pueden variar los términos del mismo modo que el ejemplo anterior.

Si tenemos iptables con la configuración por defecto, se aceptan todos los paquetes entrantes y salientes, no hay ninguna restricción.

3.3. Demonio

Un *demonio* (del inglés, *daemon*[Sta06]) es un tipo de proceso que posee la siguientes características:

1. Se ejecuta en segundo plano,
2. Generalmente se inicia en tiempo de arranque,

¹en vez de la IP podemos poner su FQDN (*Fully Qualified Domain Name*) si lo deseáramos

3. No usa los sistemas de entrada/salida estándar,
4. Mantienen la información que necesitan en ficheros especiales bien identificados.

Normalmente están cargados en memoria esperando una señal para ser ejecutados, por lo que su gasto de recursos no suele ser significativo.

Un ejemplo claro de demonio es *httpd*, que se ejecuta en los servidores web. El nombre viene de *HTTP Daemon* y es utilizado para aceptar peticiones, una vez que las acepta, crea otros procesos se encargan de atenderlas.

En el proyecto se implementa un demonio para interactuar con Netfilter, que como hemos visto en la sección anterior, requiere privilegios de administrador para ello, por eso se ha decidido utilizar un demonio y no realizarlo desde la aplicación principal. Es más sencillo configurar un programa simple como el demonio, que acepta peticiones y actuar en consecuencia de las órdenes recibidas, para iniciarse en tiempo de arranque con privilegios de administrador, que no ser necesarios permisos especiales para ejecutar la aplicación del alumno.

3.4. MD5

MD5[Den07] son las siglas de Message-Digest Algorithm 5, algoritmo resumen del mensaje, que genera un número, conocido como firma, de 128 bits a partir del contenido de ese mensaje, de tal modo que, si por cualquier razón, el contenido cambia, el número resultante de aplicar el algoritmo al nuevo contenido cambiará también.

Es utilizado, por ejemplo, para realizar firmas a los paquetes que nos descargamos de los repositorios para instalar aplicaciones en Linux, de este modo, si vemos que la firma MD5 del fichero que hemos descargado, no concuerda con el que debería, puede ser que se haya corrompido en el proceso de descarga, o que lo descargado no sea lo que aparenta.

En la aplicación es utilizado para comprobar la integridad de los archivos enviados por la red, se genera el MD5 en el computador local del fichero a transferir, se transfieren el fichero y el resultado del MD5, al recibir, se reconstruye el fichero y se genera un nuevo MD5 a partir de él, si coinciden, tenemos la garantía de que se ha transferido correctamente.

3.5. Sumario

Durante este capítulo se han descrito conceptos necesarios sobre los que este proyecto fundamenta sus funcionalidades más importantes como son la combinación de demonio y cortafuegos, para controlar el acceso a la red, o el algoritmo MD5, para las comprobaciones de integridad de los ficheros. En el siguiente capítulo se describirá la arquitectura de la aplicación a desarrollar.

Capítulo 4

Arquitectura y diseño

En el presente capítulo se presentan, mediante diagramas UML[MB04, GB04], la arquitectura del sistema[Cop10], los módulos de los que está compuesto, las comunicaciones existentes entre ellos, y el funcionamiento del mismo, es decir, se crea el marco de referencia que servirá de base para la construcción de la aplicación.

Índice

4.1. Vista lógica de la arquitectura	19
4.2. Diseño Software	20
4.3. Sumario	23

4.1. Vista lógica de la arquitectura

En esta sección se describe la vista lógica de la arquitectura mediante un diagrama de componentes en la imagen 4.1.

Los dos componentes principales *DrManhattanProfesor* y *DrManhattanAlumno* ofrecen cada uno interfaces de comunicación usadas por el otro. *DrManhattanAlumno* también se

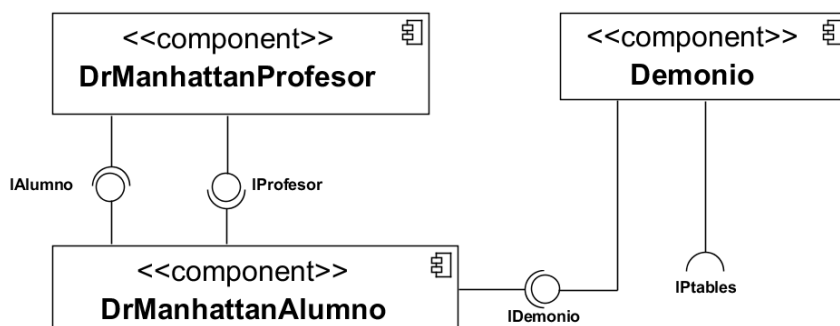


Figura 4.1: Diagrama de componentes

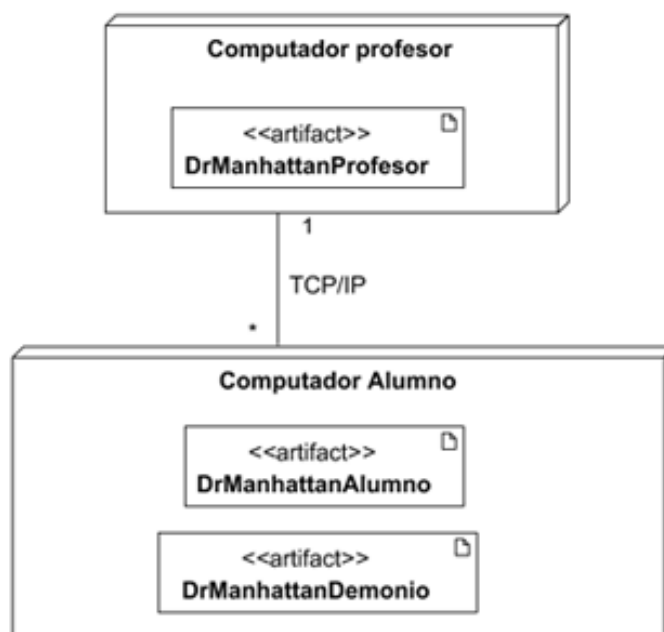


Figura 4.2: Diagrama despliegue del sistema

comunica con una tercera parte del sistema, el *Demonio*, que como vemos en la figura 4.2 forma parte de la aplicación del alumno. Este *Demonio* es el encargado de comunicarse con *iptables* cuándo hay que cambiar la política de acceso a la red.

En la imagen 4.2 vemos la vista de despliegue del sistema. Tenemos dos tipos de computadores, en los que se ejecuta la aplicación del profesor, y en los que se ejecuta la del alumno.

Sólo se permite la existencia de una aplicación en el computador del profesor, a la que se conectan mediante TCP/IP un número indefinido de aplicaciones alumno, lógico, ya que en una prueba de una asignatura suelen ser varios los alumnos realizándola.

En la figura 4.3 se muestran las posibles interacciones que tanto el alumno como el profesor realizan con sus respectivas aplicaciones durante el transcurso normal de una prueba, se siguen los pasos descritos en la sección 2.1.

4.2. Diseño Software

En esta sección se muestra en la figura 4.4 un diagrama de estados para clarificar la aplicación del alumno.

Esa figura representa el protocolo a implementar que ha de garantizar la principal funcionalidad de la aplicación, denegar el acceso a la red en los computadores de los alumnos

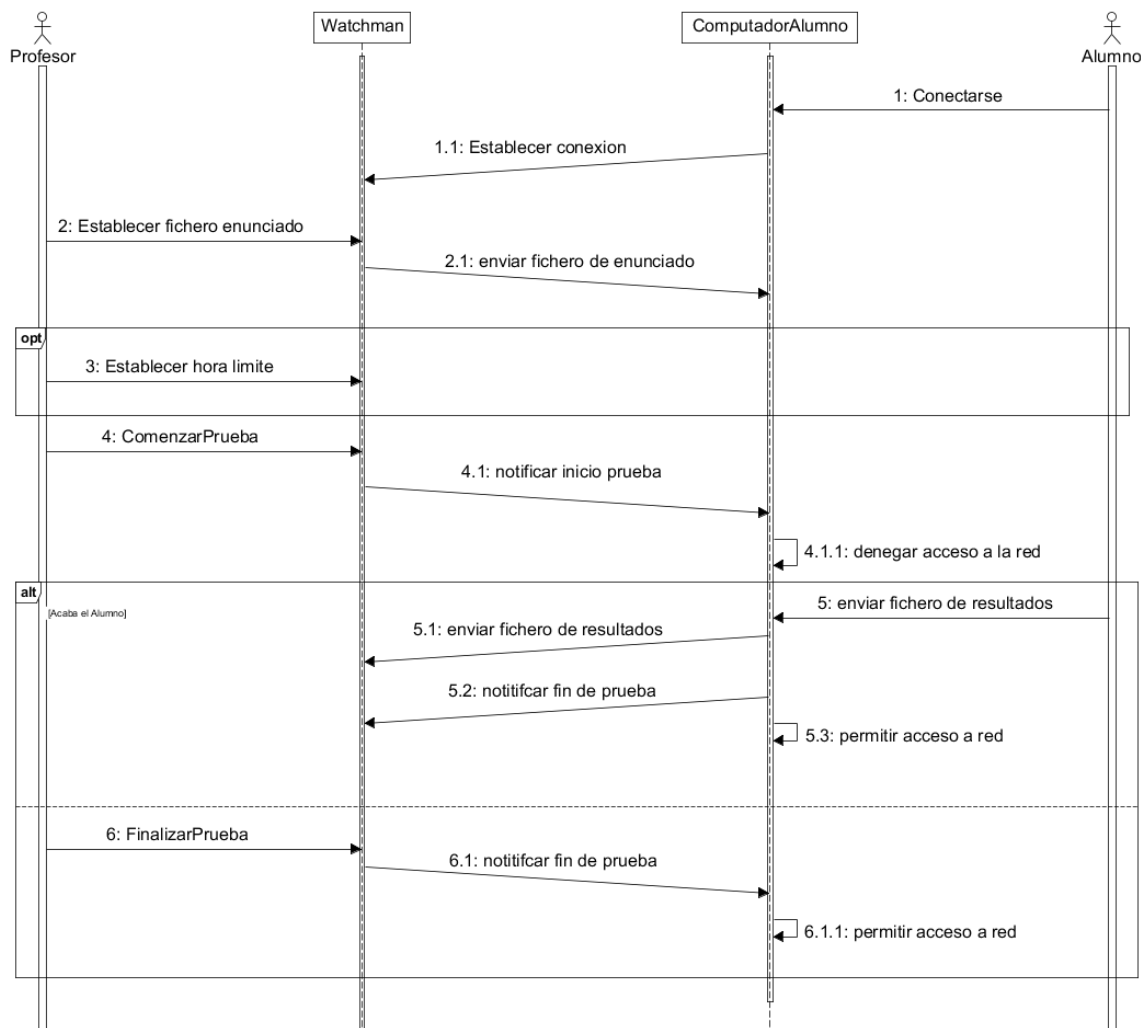


Figura 4.3: Diagrama de actividad del sistema

que están realizando la prueba, mientras esta esté en marcha, sin necesidad de apagar el router o switch del laboratorio.

El acto desactivar la red se consigue por medio de iptables, sección 3.2, cambiando la política de los paquetes salientes una vez que empieza la prueba y hasta que acaba.

Por defecto iptables permite todo el tráfico que entre y salga del equipo, modificando las reglas para que deseché cualquier paquete destinado a cualquier equipo, conseguimos que no se pueda realizar ninguna petición a ningún nodo de la red, y, por tanto, tampoco recibiremos el contenido de la posible respuesta, el equipo del alumno queda aislado del resto.

A la hora de volver a permitir el acceso a la red, basta con modificar la política para el

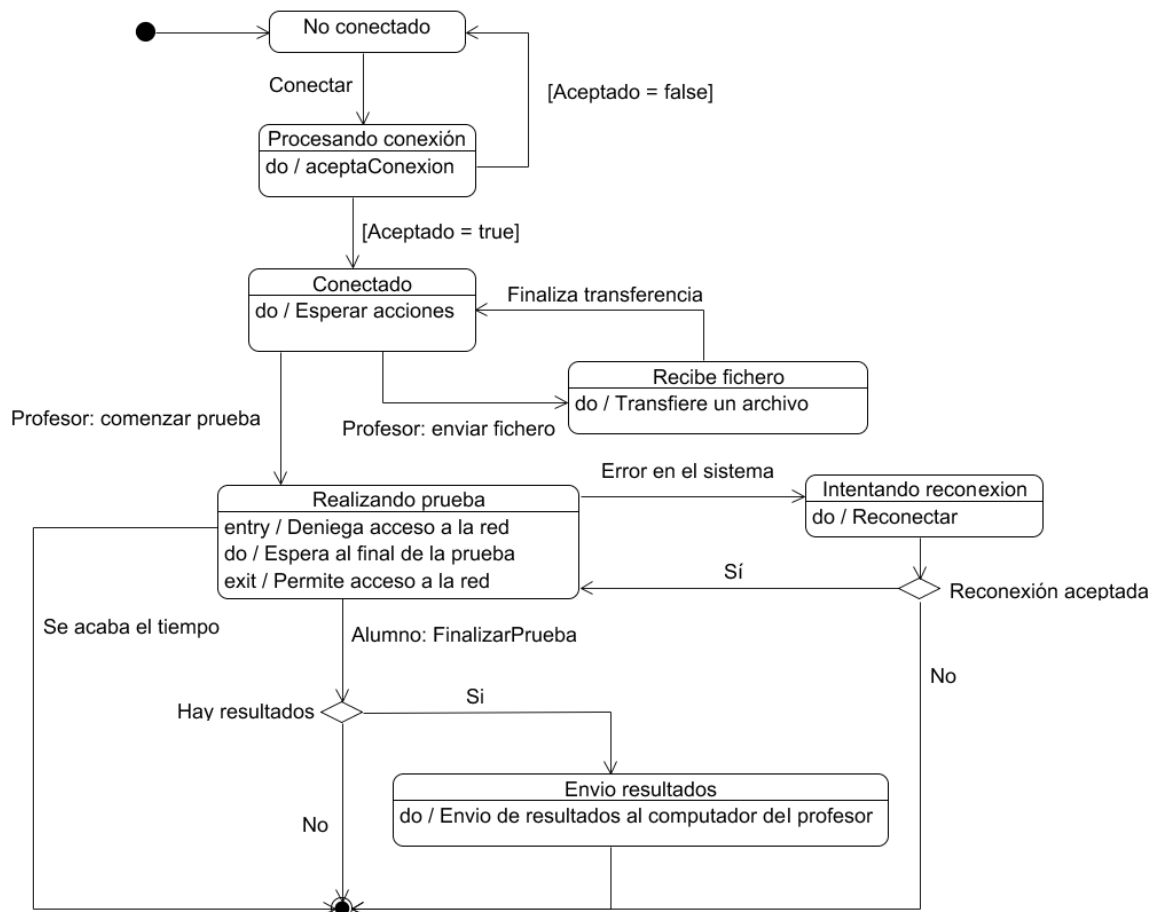


Figura 4.4: Diagrama de estados de la aplicación del alumno

tratamiento de los paquetes salientes y restaurarla al estado anterior. Un alumno corriente no puede realizar esta operación ya que son necesarios privilegios de administrador para ello, entonces, una vez que la aplicación desactiva la red, un alumno no puede interactuar con iptables para activarla de nuevo.

Vemos en la imagen que el único modo de finalizar la prueba es partiendo de una prueba ya iniciada, lógicamente, es decir, desde el estado “Realizando prueba”. Nada más entrar en este estado se desactiva el acceso a la red, por tanto, si se pretende finalizar la prueba, se ha tenido que realizar la misma sin acceso a la red. Además el acto de enviar los resultados se implementa de modo que no se pueda modificar el fichero una vez habilitada la red pero antes de transferirlo definitivamente.

Para entrar en el estado “Realizando prueba”, se pueden seguir dos caminos. El normal implica conectar la aplicación del alumno con la aplicación del profesor, cosa que únicamen-

te se puede hacer antes de que dé comienzo la prueba, por consiguiente, tampoco se puede realizar la prueba con acceso a la red y al finalizarla, conectarse y enviar los resultados, la aplicación no aceptaría la conexión.

El otro camino involucra a una funcionalidad que tiene el sistema que consiste en permitir reconexiones de alumnos que estuviesen realizando la prueba y por el motivo que sea, un error en el sistema, por ejemplo, hayan tenido que reiniciar el computador, cuándo la aplicación del alumno vuelva a ejecutarse, al inicio de la sesión automáticamente, se reconectará con la aplicación del profesor. En la imagen se observa que sólo se puede reconectar si previamente se estaba realizando la prueba y al reconectar volveríamos automáticamente a ese estado, en el que la red se desactiva al entrar, es decir, que aunque se reinicie el computador del alumno durante el transcurso de la prueba no se conseguiría acceso a la red.

4.3. Sumario

En este capítulo se ha presentado, mediante diagramas UML, la base arquitectónica en la que se basará todo el desarrollo de la aplicación y el protocolo a implementar para intentar garantizar la integridad de la prueba. En el siguiente capítulo se describe una de las iteraciones realizadas a lo largo del desarrollo del software.

Capítulo 5

Creación del sistema distribuido base

En el siguiente capítulo se describe lo realizado en la primera iteración de la fase de construcción.

La base de la que se parte son los resultados de las iteraciones anteriores, correspondientes a las fases de iniciación y elaboración, es decir, los requisitos del sistema y su arquitectura.

De acuerdo con lo planificado en la sección 2.4, el objetivo de esta iteración es el de crear la base del sistema distribuido, implementando los requisitos de la tabla 5.1 que son el subconjunto de los casos de uso mostrados en la figura 5.4.

El primer paso en una iteración de la fase de construcción de acuerdo a la metodología es refinar los requisitos de alto nivel a implementar, con lo que obtenemos la tabla 5.2

Índice

5.1. Incrementos realizados	25
5.1.1. Interfaces gráficas	27
5.1.2. Conexión	27
5.1.3. Envío de ficheros	28
5.2. Pruebas	30
5.3. Sumario	31

5.1. Incrementos realizados

En las siguientes secciones se describen los incrementos realizados para la implementación.

Identificador	Descripción
R01	Un computador de la red debe poder ser designado como <i>Watchman</i> .
R02	Todos los computadores que no sean <i>Watchman</i> serán computadores normales, y podrán ser utilizados para la realización de las pruebas evaluables.
R06	El profesor debe ser capaz desde el <i>Watchman</i> de enviar el fichero de enunciado al resto de computadores.
R07	El alumno desde su computador debe ser capaz de conectarse al <i>Watchman</i> .
R13	La aplicación ha de ser capaz de comprobar que los archivos se han enviado correctamente.

Cuadro 5.1: Requisitos objetivo de la iteración

Identificador	Descripción
R01	Un computador de la red debe poder ser designado como <i>Watchman</i> .
R02	Todos los computadores que no sean <i>Watchman</i> serán computadores normales, y podrán ser utilizados para la realización de las pruebas evaluables.
R06	El profesor debe ser capaz desde el <i>Watchman</i> de enviar el fichero de enunciado al resto de computadores.
R06.1	El profesor escogerá el fichero a enviar con un diálogo desde la aplicación.
R06.2	Solamente es posible transferir un fichero a la vez.
R07	El alumno desde su computador debe ser capaz de conectarse al <i>Watchman</i> .
R07.1	La identificación del equipo necesaria para la conexión del <i>Watchman</i> se realizará por medio de la IP.
R07.2	El <i>Watchman</i> debe soportar conexiones simultáneas.
R07.3	Para una correcta conexión son necesarios datos del alumno, nombre y apellidos.
R07.4	Para una correcta conexión es necesario que el alumno indique en que directorio desea recibir el enunciado en caso de que lo haya.
R07.4.1	El alumno ha de tener permisos de escritura en el directorio que seleccione.
R13	La aplicación ha de ser capaz de comprobar que los archivos se han enviado correctamente.
R13.1	Para la comprobación de integridad de los archivos se usarán firmas MD5.

Cuadro 5.2: Requisitos objetivo refinados de la iteración

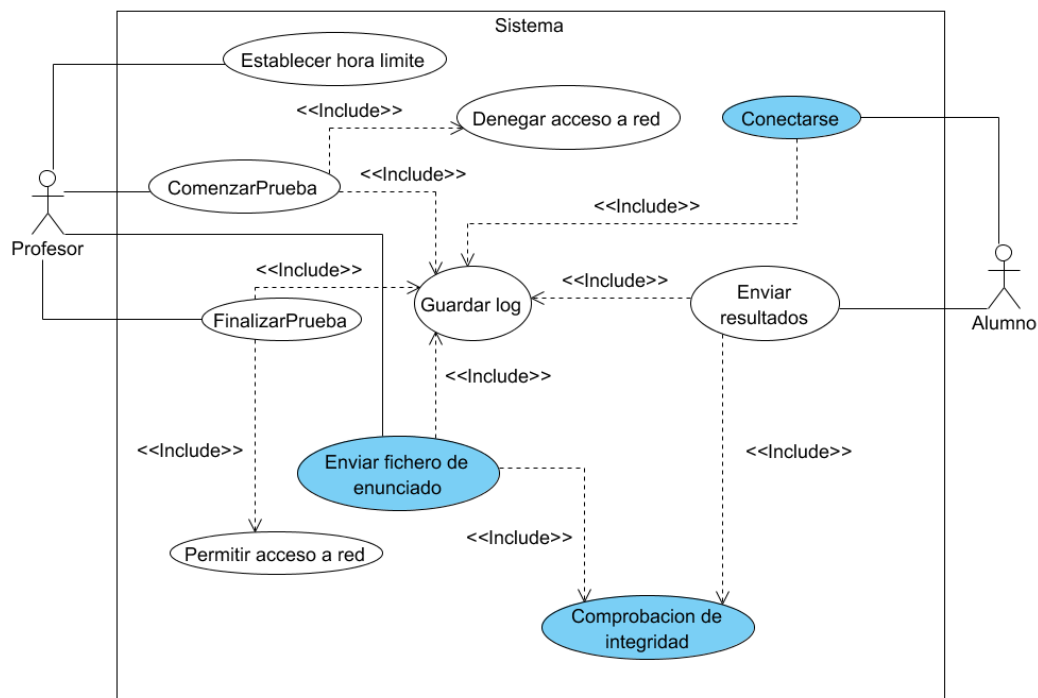


Figura 5.1: Casos de uso a implementar

5.1.1. Interfaces gráficas

Los requisitos R01 y R02 no reflejan funcionalidades que ha de tener el sistema, sino que tratan sobre la arquitectura del mismo. Como se ha comentado es un software distribuido, así que tenemos dos aplicaciones distintas. Las interfaces diseñadas para estas aplicaciones se muestran en la imagen 5.2 la que utilizará el profesor y en la 5.3 la que utilizará el alumno.

5.1.2. Conexión

En esta sección se comenta el proceso para implementar el requisito R07 “El alumno desde su computador debe ser capaz de conectarse al *Watchman*” el caso de uso “Conectarse” representado en el diagrama de secuencia de la imagen 5.4. El resto de diagramas de cada caso de uso se encuentran en el CD, en la carpeta UML.

En este incremento la aplicación del alumno debe, dada la IP del equipo dónde se está ejecutando el computador del profesor, establecer una conexión con él. Este es un punto básico del sistema, si no se es capaz de establecer correctamente una conexión, las dos aplicaciones no podrán comunicarse y no funcionará nada.

Para que se pueda establecer la conexión se utilizan las clases “ServerSocket” y “Socket”,

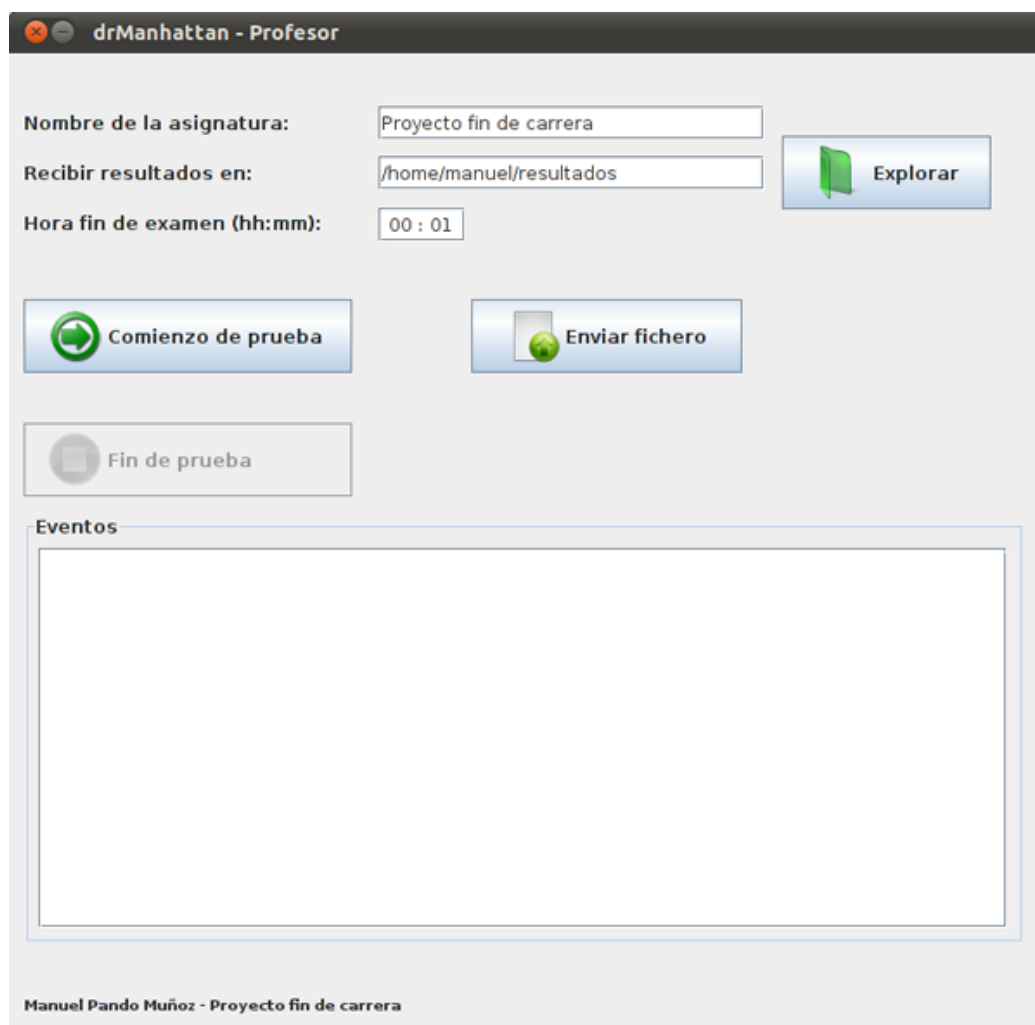


Figura 5.2: Interfaz de la aplicación profesor

de la librería “java.net”[PC98, Pit10]. Con la primera conseguimos que la aplicación del profesor espere nuevas conexiones de alumnos y con la segunda creamos realmente la conexión desde la aplicación del alumno, partiendo de la IP proporcionada. Cada vez que se crea una conexión nueva se almacena en una lista. Además, como no se quiere bloquear la interfaz gráfica[Dev99] del profesor mientras los alumnos se conectan, esto se realiza en un hilo de ejecución[Oak04] aparte.

5.1.3. Envío de ficheros

Una vez que los alumnos están conectados correctamente el profesor puede enviarles un enunciado o ficheros necesarios para la realización de la prueba y el sistema ha de poder detectar errores en la transferencia de dichos ficheros. Como ya hemos comentado, la aplica-

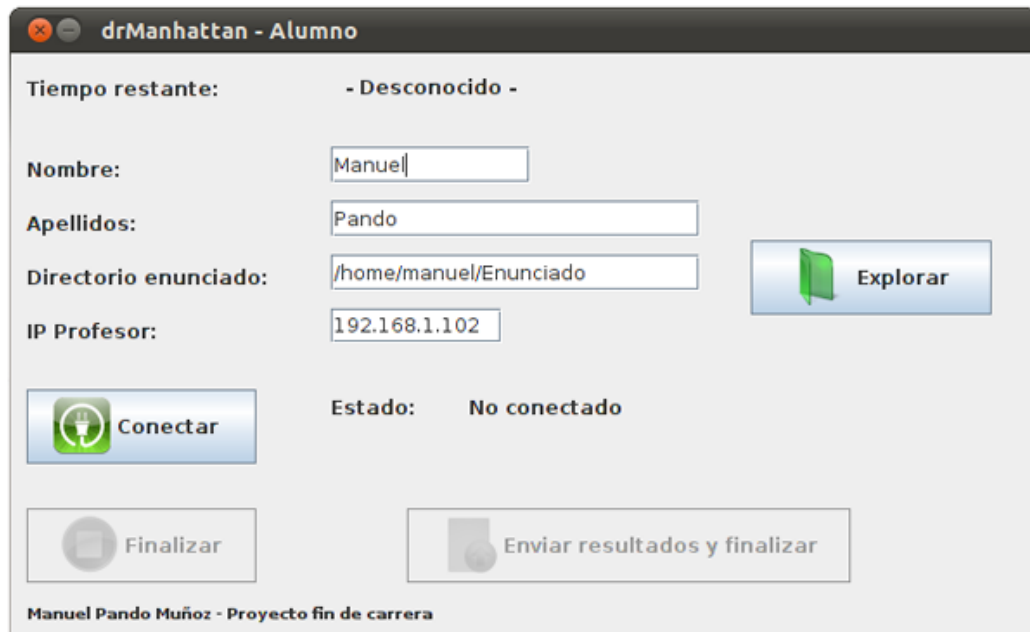


Figura 5.3: Interfaz de la aplicación alumno

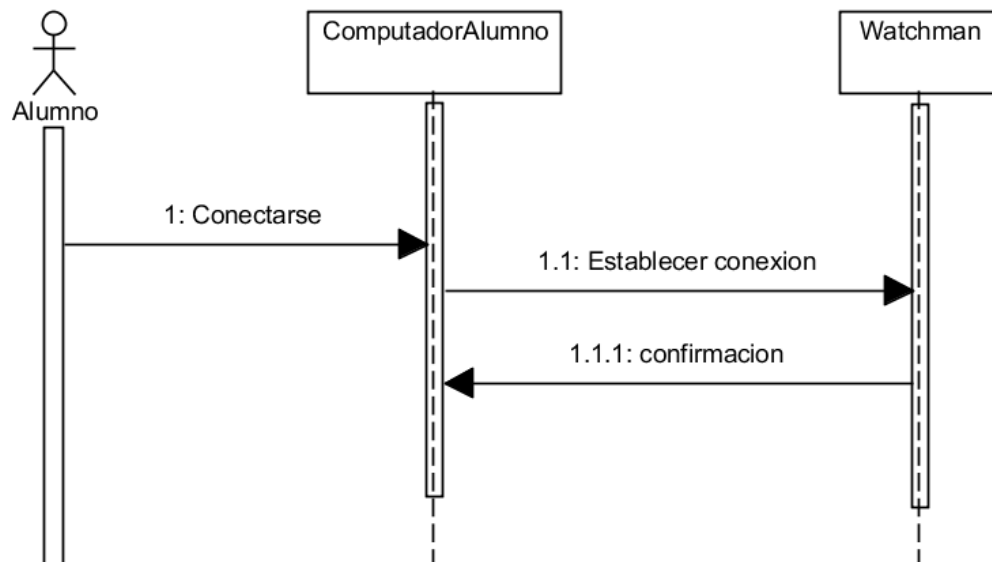


Figura 5.4: Diagrama de secuencia caso de uso conectar

ción del profesor mantiene una lista con la conexiones creadas de modo que leer un fichero y enviarlo por cada conexión de la lista es un proceso trivial.

5.2. Pruebas

Después de finalizar la codificación de las funcionalidades descritas en las secciones anteriores es el turno para las pruebas.

Debido a la naturaleza del sistema, automatizar pruebas con una herramienta estilo *JUnit* se antoja difícil, ya que funciona a base de eventos[Mü10] y es distribuido, por eso, para probar la aplicación se utilizan secuencias de acciones con el fin de desencadenar los eventos requeridos en cada funcionalidad. En esta iteración se realizan las siguientes:

- **R07** El alumno desde su computador debe ser capaz de conectarse al *Watchman*.
 - Prueba: Intentar conectarse a un equipo en el que no se ejecuta la aplicación del profesor.
 - Objetivo: La aplicación responde correctamente ante direcciones erróneas.
 - Prueba: Conectarse al equipo en el que se está ejecutando la aplicación del profesor.
 - Objetivo: La aplicación conecta correctamente.
 - Prueba: Conectar varios alumnos al profesor.
 - Objetivo: La aplicación del profesor soporta correctamente varios alumnos conectados.
- **R06** - El profesor debe ser capaz desde el *Watchman* de enviar el fichero de enunciado al resto de computadores.
- **R13** La aplicación ha de ser capaz de comprobar que los archivos se han enviado correctamente.
 - Prueba: Intentar enviar un fichero sin alumnos conectados.
 - Objetivo: La aplicación no produce errores porque no haya alumnos conectados.
 - Prueba: Enviar un fichero a varios alumnos conectados.
 - Objetivo: Cada alumno recibe correctamente una copia del fichero original.

- Prueba: Enviar un fichero a varios alumnos conectados y forzar una comprobación de integridad errónea.
- Objetivo: Cada alumno es alertado de que ha habido problemas en la transferencia del fichero.

5.3. Sumario

En este capítulo se ha descrito el proceso realizado a lo largo de la primera iteración de la fase de desarrollo consistente en refinamiento de requisitos, diseño de los casos de uso a implementar, incrementos implementados y pruebas realizadas. En el siguiente capítulo se describe la segunda iteración de la fase de construcción que tiene su base en lo generado en la iteración descrita a lo largo de este capítulo.

Capítulo 6

Comienzo de prueba y denegación de acceso a red

En el siguiente capítulo se describe lo realizado en la segunda iteración de construcción. Se parte de lo obtenido en las iteraciones previas, que esta expuesto a lo largo de los capítulos precedentes.

En cuanto al estado de la aplicación, en la primera iteración de construcción, descrita en el capítulo 5, se ha desarrollado un sistema distribuido, en el que el alumno puede conectarse con la aplicación del profesor y recibir ficheros enviados desde ella.

El objetivo de esta iteración es que el profesor pueda establecer el inicio y de la prueba, poder prefijar una hora de finalización de la misma y que la aplicación del alumno sea capaz de denegar el acceso a la red mientras dure la prueba.

En la tabla 6.1 se pueden ver los requisitos de alto nivel a implementar durante esta iteración, en la 6.3 ya refinados y en la 6.2 la base, o lo que es lo mismo, lo implementado en la iteración anterior. La lista global de requisitos se encuentra en la tabla 2.1.

Índice

6.1. Incrementos realizados	34
6.1.1. Inicio de la prueba	34
6.1.2. Examen temporizado	35
6.1.3. Denegar acceso a red	35
6.2. Pruebas	37
6.3. Sumario	38

Identificador	Descripción
R03	El profesor debe ser capaz desde el <i>Watchman</i> de indicar el inicio de la prueba.
R05	El profesor ha de ser capaz desde el <i>Watchman</i> de establecer una hora límite para la duración de la prueba.
R10	El alumno desde su computador debe tener la posibilidad de ver el tiempo restante el pruebas de duración prefijada.
R11	La aplicación del alumno ha de ser capaz de denegar el acceso a la red al empezar la prueba.

Cuadro 6.1: Objetivos de la iteración

Identificador	Descripción
R01	Un computador de la red debe poder ser designado como <i>Watchman</i> .
R02	Todos los computadores que no sean <i>Watchman</i> serán computadores normales, y podrán ser utilizados para la realización de las pruebas evaluables.
R06	El profesor debe ser capaz desde el <i>Watchman</i> de enviar el fichero de enunciado al resto de computadores.
R07	El alumno desde su computador debe ser capaz de conectarse al <i>Watchman</i> .
R13	La aplicación ha de ser capaz de comprobar que los archivos se han enviado correctamente.

Cuadro 6.2: Requisitos ya implementados del sistema

6.1. Incrementos realizados

En las siguientes secciones se describen los incrementos realizados dentro de esta iteración, generalmente coincide el número de incrementos en cada iteración con el número de requisitos a implementar.

6.1.1. Inicio de la prueba

En esta sección se comenta cómo se consigue que el profesor pueda notificar a los alumnos el inicio de la prueba. Como ya hemos comentado, partimos de la iteración anterior en la cual los alumnos eran capaces de conectar a la aplicación del profesor. En la aplicación del alumno, cuando se crea una conexión, se inicia a su vez un hilo de ejecución que se mantiene a la espera de recibir distintas órdenes provenientes del computador del profesor. De este modo se hace muy simple mantener desde la aplicación del profesor una lista de las conexiones abiertas con cada alumno y, al presionar el botón de iniciar la prueba, recorrer esa lista enviando la orden por cada conexión, de modo similar a como se transfiere un fichero,

Identificador	Descripción
R03	El profesor debe ser capaz desde el <i>Watchman</i> de indicar el inicio de la prueba.
R03.1	Para que comience la prueba es necesario el nombre de la asignatura, el directorio dónde recibir resultados y una hora de finalización.
R03.1.1	Se han de tener privilegios de escritura en el directorio seleccionado.
R03.2	Se ha de pedir confirmación antes de comenzar realmente.
R05	El profesor ha de ser capaz desde el <i>Watchman</i> de establecer una hora límite para la duración de la prueba.
R05.1	Si la hora de finalización es inferior a la del momento en que comienza la prueba, no se tendrá en cuenta.
R10	El alumno desde su computador debe tener la posibilidad de ver el tiempo restante el pruebas de duración prefijada.
R10.1	Se implementará con un hilo propio para no bloquear la interfaz.
R11	La aplicación del alumno ha de ser capaz de denegar el acceso a la red al empezar la prueba.
R11.1	Se utilizará iptables como medio para impedir el acceso a la red.
R11.2	Se utilizará un demonio para la interacción privilegiada con iptables.

Cuadro 6.3: Objetivos refinados de la iteración

sección 5.1.3. Cuando cada una de las aplicaciones del alumno recibe esa orden, actúa en consecuencia.

6.1.2. Examen temporizado

El profesor puede establecer una hora límite, llegada la cual, la prueba terminará automáticamente. Cuando el profesor define este límite en su aplicación y decide comenzar la prueba, se envía también si hay una hora de fin y, en caso afirmativo, cual es junto con la orden de comenzar la prueba. De este modo la aplicación del alumno puede mostrar una cuenta atrás con los minutos restantes para la finalización, para facilitar la referencia temporal tal como se muestra en la imagen 6.1.

6.1.3. Denegar acceso a red

Cómo ya hemos visto en las secciones anteriores, una vez que la aplicación del alumno recibe la orden de comenzar la prueba, se ha de denegar el acceso a la red. Para ello se utiliza iptables, por medio de un demonio.

El demonio creado es muy simple, se ejecuta en segundo plano esperando a que la aplicación del alumno conecte, y en función de lo requerido en ese momento, permitir o no el acceso a la red interactuando con iptables. Este demonio se inicia en tiempo de arranque y con los permisos necesarios para poder usar el cortafuegos.

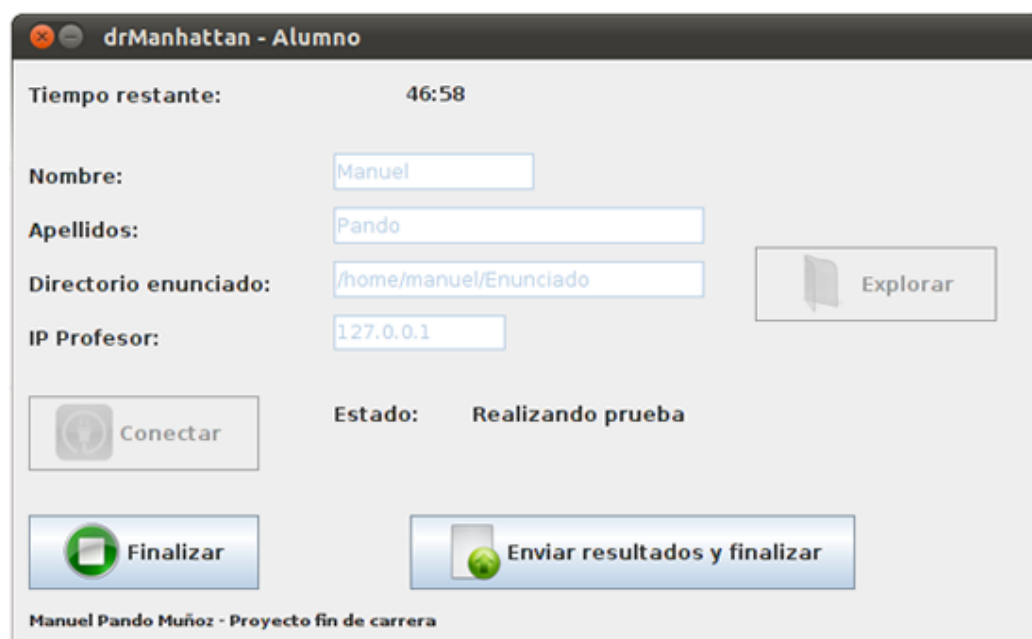


Figura 6.1: Aspecto de la GUI del alumno con una prueba temporizada.

Las órdenes concretas que ejecuta el demonio son, cuándo se desea denegar la red:

```
iptables -P OUTPUT DROP
iptables -A OUTPUT -s 127.0.0.1 -j ACCEPT
```

Con la primera de ellas se cambia la política del tratamiento a los paquetes salientes del equipo, de modo que los deseche, dicho de otro modo, no se permiten las comunicaciones salientes con otros computadores, de esta forma se evita que se hagan peticiones, por ejemplo, a un servidor web[Yea96].

La segunda es para permitir los paquetes salientes dirigidos al propio equipo local. Esto es necesario para la comunicación entre la aplicación del alumno y el demonio, que como se ha visto en la sección 4.1 se ejecutan en el mismo computador.

Puede parecer que el equipo queda totalmente aislado, incluso del computador del profesor, pero esto no es así, puesto que ya hay una conexión establecida y dado que la aplicación del alumno espera órdenes de la aplicación del profesor, puede seguir funcionando perfectamente, puesto que los paquetes de entrada sí que están permitidos, lo que estas instrucciones imposibilitan es la creación de nuevas conexiones y el envío de mensajes a cualquier computador que no sea el propio.

6.2. Pruebas

En esta sección se describen las pruebas realizadas en la iteración con el objetivo de determinar si el funcionamiento de lo construido es correcto.

- **R03** - El profesor debe ser capaz desde el *Watchman* de indicar el inicio de la prueba.
 - Prueba: Pulsar el botón para iniciar la prueba con alumnos conectados.
 - Objetivo: A los alumnos conectados les llega la señal, no admite nuevas conexiones.
 - Prueba: Pulsar el botón para iniciar la prueba sin alumnos conectados.
 - Objetivo: Se inicia la prueba, no admite nuevas conexiones.
- **R05** - El profesor ha de ser capaz desde el *Watchman* de establecer una hora límite para la duración de la prueba.
- **R10** - El alumno desde su computador debe tener la posibilidad de ver el tiempo restante el pruebas de duración prefijada.
 - Prueba: Establecer como límite temporal horas futuras y comenzar la prueba.
 - Objetivo: La aplicación del alumno muestra el tiempo restante correcto. No se admiten nuevas conexiones.
 - Prueba Establecer como límite temporal horas pasadas.
 - Objetivo: Se inicia la prueba, la aplicación del alumno no muestra límite temporal. No se admiten nuevas conexiones.
 - Prueba: Establecer como límite temporal horas incorrectas y comenzar la prueba.
 - Objetivo: La aplicación del alumno detecta las horas erróneas y no comienza la prueba.
- **R11** - La aplicación del alumno ha de ser capaz de denegar el acceso a la red al empezar la prueba.
 - Prueba: Después de que de inicio una prueba, en el computador del alumno, intentar abrir páginas web en el navegador, pings a equipos.
 - Objetivo: La aplicación del alumno desactiva el acceso a la red.

Como se puede comprobar tras la lectura de los dos capítulos dedicados a describir una iteración, la construcción en esta metodología es un proceso repetitivo y todas las iteraciones son muy similares.

6.3. Sumario

En este capítulo, como en el anterior, se muestra el proceso a seguir de acuerdo a la metodología escogida, demostrando que es un proceso repetitivo. En el siguiente capítulo se describirán las acciones de despliegue y aceptación realizadas.

Capítulo 7

Despliegue y aceptación

En el siguiente capítulo se presentan lo realizado en torno al despliegue y la aceptación una vez la aplicación ha sido desarrollada.

Índice

7.1. Despliegue	39
7.1.1. Página web	41
7.2. Pruebas	41
7.3. Sumario	44

7.1. Despliegue

Para que la aplicación pueda ser usada de un modo cómodo fuera del ambiente de desarrollo se hace necesaria la creación de instaladores. Esto se puede hacer, por ejemplo, con el comando *dpkg* en sistemas Linux derivados de Debian[Kra05], ya que con él se crean archivos .deb. En nuestro caso se han de crear dos instaladores, uno para la aplicación del profesor, y otro para la aplicación de los alumnos.

En el sistema de archivos, cada carpeta tiene su utilidad, de modo que si, por ejemplo, queremos conocer los logs generados por alguna aplicación sabemos que hemos de buscar en */var/log/*, */etc/* para los aspectos de configuraciones, etc.

Esto es interesante conocerlo para que los archivos que coloque nuestro instalador en el sistema, estén correctamente ubicados, y que se puedan localizar fácilmente, en caso de querer modificarlos o eliminarlos.

Por ejemplo, la aplicación del alumno, creará en los siguientes directorios, los siguientes ficheros:

- */etc/rc2.d:*

- *S88drManhattanDaemon*

Este fichero contiene un script muy simple que se encarga de iniciar en segundo plano el demonio. Los ficheros en este directorio se ejecutan cuando se entra al segundo nivel de ejecución, en el arranque del sistema.

■ **/usr/bin:**

- *drManhattanAlumno.jar*
- *drManhattanAlumno.sh*
- *drManhattanDaemon.jar*

En este directorio se encuentran los ejecutables de las aplicaciones que pueden utilizar todos los usuarios.

■ **/usr/share/applications:**

- *drManhattanAlumno.desktop*

En nuestro caso se ha utilizado un sistema Ubuntu con el entorno de escritorio GNOME, en ese directorio se guardan las entradas de cada aplicación que se puede ejecutar en GNOME, en archivos de texto dónde se especifica la ruta del ejecutable, el icono del programa, su versión, comentarios, etc.

■ **/usr/share/drManhattanAlumno/iconos:**

- *icono.png*
- *envioFichero.png*
- *explorar.png*
- *fin.png*

Contiene los datos que no dependen de la arquitectura del sistema, imágenes, sonidos, etc.

■ **/usr/share/menu:**

- *drManhattanAlumno*

Cada archivo localizado en este directorio contiene la información necesaria para que GNOME pueda crear una entrada en el menú despegable de aplicaciones.

■ **/usr/share/doc/drManhattan-Alumno:**

- *copyright*
- *manual.pdf*

Este directorio contiene documentos relacionados con la aplicación, en este caso los términos de la licencia y el manual de usuario.

Una vez que están definidos los archivos y el directorio dónde los ha de colocar el instalador, creamos una carpeta a modo de raíz en la que simulamos el árbol de directorios anterior. Por ejemplo, creamos la carpeta `/home/usuario/deb`, y dentro de ella creamos `/home/usuario/deb/etc/rc2.d/`, `/home/usuario/deb/usr/bin/`, etc y los archivos correspondientes.

Dentro de la carpeta raíz se ha de crear además de lo anterior, un directorio llamado “DEBIAN” con tres ficheros, “control”, “postinst” y “postrm”. En el primero se especifican las características del paquete y los otros dos se ejecutan justo después de instalar el paquete y justo después de desinstalarlo, respectivamente, en nuestro caso actualizan los menús desplegables para que aparezca o desaparezca la aplicación.

Una vez que tenemos todo creado, cambiamos los permisos del directorio raíz y subdirectorios así:

```
chown root.root -R /home/usuario/deb/
```

Después de esto, la orden para empaquetarlo en un fichero `.deb` es:

```
dpkg -b /home/usuario/deb /home/usuario/paquete.deb
```

Para instalar, teniendo permisos de administrador:

```
dpkg -i /home/usuario/paquete.deb
```

7.1.1. Página web

Para dotar de una mayor visibilidad al proyecto se ha construido una web sencilla, alojada en <http://www.alumnos.unican.es/mpm14/> en la que se puede encontrar información, documentación y el código fuente del proyecto. Se han creado además un video tutorial, disponible en la propia web, para poder visualizar el funcionamiento de la aplicación.

7.2. Pruebas

Como se comentó en la sección 5.2 en la que se explicaban las pruebas realizadas durante una iteración, las pruebas han sido combinaciones de acciones, tanto de modo local mientras se desarrollaba, como en los laboratorios de la Facultad con el objetivo de imprimir mayor realismo, tanto en el entorno de ejecución, como en la carga de las aplicaciones.

- Prueba: Intentar conectar a una IP en la que no se está ejecutando la aplicación del profesor.
- Objetivo: La aplicación informa del error y permite volver a introducir los datos de conexión.



Figura 7.1: Página web del proyecto.

- Prueba: Sin alumnos conectados, enviar fichero de enunciado.
- Objetivo: La aplicación del profesor no produce errores y permite seguir ejecutándose.
- Prueba: Con un alumno conectado, enviar ficheros de enunciado.
- Objetivo: El alumno recibe correctamente el fichero.
- Prueba: Con varios alumnos conectados, enviar ficheros de enunciado.
- Objetivo: Todos los alumnos reciben correctamente los ficheros.
- Prueba: Iniciar prueba sin alumnos conectados.

- Objetivo: La prueba queda iniciada, no se admiten nuevas conexiones.
- Prueba: Iniciar prueba con varios alumnos conectados.
- Objetivo: Desde los computadores de los alumnos no se puede acceder a la red. No se admiten nuevas conexiones.
- Prueba: Introducir hora errónea e iniciar prueba.
- Objetivo: La aplicación informa del error y la prueba no se inicia.
- Prueba: Iniciar prueba temporizada y esperar a que acabe el tiempo.
- Objetivo: Cuando finaliza el tiempo los alumnos recuperan acceso a la red pero no pueden enviar resultados.
- Prueba: Iniciar prueba temporizada y finalizar manualmente.
- Objetivo: Al finalizar manualmente, cada alumno que esté realizando la prueba recibe un aviso de que ha finalizado. No se pueden enviar ficheros de resultado y se devuelve el acceso a la red.
- Prueba: Iniciar prueba normal y finalizar todos los alumnos sin resultados.
- Objetivo: Cada alumno deja de poder acceder a la red al iniciar la prueba, cuando finalizan se les devuelve correctamente el acceso. En la aplicación del profesor se muestran los logs correctos.
- Prueba: Iniciar prueba normal y finalizar alumnos sin resultados y alumnos con ellos.
- Objetivo: El árbol de directorios se crea correctamente para almacenar los resultados. Los archivos son transferidos correctamente.
- Prueba: Iniciar prueba normal y finalizar mientras hay alumnos realizando la prueba.
- Objetivo: Cada alumno que esté realizando la prueba recibe un aviso de que ha finalizado. No se pueden enviar ficheros de resultado y se devuelve el acceso a la red.
- Prueba: Iniciar prueba normal y reiniciar el computador de un alumno para intentar reconectar sin acabar la prueba.

- Objetivo: Al reiniciar un computador con el que se estaba realizando una prueba, la aplicación del alumno reconoce el estado previo y deniega el acceso a la red.
- Prueba: Iniciar prueba normal, reiniciar el computador de un alumno, finalizar la prueba e intentar reconectar.
- Objetivo: Al reiniciar un computador con el que se estaba realizando una prueba, la aplicación del alumno reconoce el estado previo, intenta reconectarse pero como ya ha finalizado muestra mensaje de error. La red no se desactiva.
- Prueba: Iniciar prueba temporizada y reiniciar el computador de un alumno para reconectar antes de que se acabe la prueba.
- Objetivo: Al reiniciar, reconecta correctamente y el tiempo restante es correcto.
- Prueba: Iniciar prueba temporizada y reiniciar el computador de un alumno para reconectar después de que se acabe la prueba.
- Objetivo: Al intentar reconectar no puedo puesto que ya ha finalizado y muestra un error.

Esta lista contiene las pruebas de integración y validación realizadas, esto es, cuándo se prueba el funcionamiento del sistema completo para comprobar que cumple los requisitos establecidos en la tabla 2.1.

7.3. Sumario

En este capítulo se han presentado el despliegue de la aplicación, consistente en la creación de paquetes instaladores y la creación de una página web para otorgar una mayor visibilidad al proyecto y las pruebas de integración y aceptación realizadas para comprobar el cumplimiento de los requisitos. En el siguiente capítulo concluye el documento exponiendo conclusiones y presentando unas posibles líneas de desarrollo futuro.

Capítulo 8

Conclusiones y Trabajos Futuros

Para concluir la memoria se presentan a continuación las conclusiones y trabajos futuros posibles como continuación a este proyecto.

Índice

8.1. Conclusiones	45
8.2. Trabajos futuros	46

8.1. Conclusiones

Como se comentaba al principio de este documento el objetivo del proyecto era el de crear una aplicación que facilitase la realización de pruebas evaluables a los docentes, automatizando ciertas tareas que si no han de realizarse manualmente, como la recogida de resultados, con el gasto de tiempo que ello conlleva, además de tener que ser realizado secuencialmente.

Para conseguir esto, se ha pasado por una fase de investigación, para tener conocimientos suficientes del problema a solucionar, las diferentes opciones posibles para ello y poder así tomar decisiones razonadas. Esto se transformó en una planificación y un diseño del proyecto, que se ha ido exponiendo a lo largo del documento.

La solución obtenida es una aplicación que permite, enviar archivos desde el computador del profesor a los alumnos, deshabilitar el acceso a la red durante el transcurso de la prueba, haciendo uso de iptables, software muy utilizado y probado, y recoger automáticamente los resultados, comprobando la integridad de los ficheros, como principales funciones a través de interfaces visuales intuitivas y amigables.

Unas de las lecciones que considero más importantes aprendidas a lo largo del desarrollo de este proyecto de fin de carrera, es la importancia de tener unos requisitos claros y definidos antes de planificar el diseño y construcción de la aplicación y tener un análisis y un diseño

correcto y claro antes de codificar realmente el software y cómo el cambio en requisitos en fases avanzadas del proyecto puede suponer muchas horas de trabajo extra, en comparación con las primeras fases.

Merece la pena “perder” el tiempo revisando los requisitos y sus posibles incongruencias antes de empezar con la codificación.

Durante la realización de las pruebas descritas en la sección 7.2 se encontraba presente el administrador de sistemas de la Facultad, que propuso la funcionalidad de recuperar el estado frente a reinicios del sistema, parecía algo interesante añadirlo a la aplicación, así que se hizo. Esto realmente no significa un cambio en uno de los requisitos, sino la adición de uno nuevo, y gracias a la metodología usada para la construcción, que es flexible y prevé posibles cambios en los requisitos, el tiempo extra de codificación y diseño no fue mucho, comparado con lo que podría haber sido de utilizar una metodología en cascada.

En la siguiente sección se detallan posibles mejoras o adaptaciones a realizar en la aplicación para aumentar su funcionalidad, usabilidad y atractivo en general.

8.2. Trabajos futuros

Como continuación de este proyecto, en lo referido a su principal función, el mantenimiento de la integridad de las pruebas evaluables, o en el aumento de la comodidad a los docentes, pueden añadirse las siguientes líneas de desarrollo:

- **Deshabilitar USB:** Los dispositivos USB son otro posible aspecto que podría enturbiar los resultados de una prueba, teniendo en cuenta que cada día son más pequeños.
- **Acceso restringido:** En algunos momentos puede ser deseable que los alumnos accedan a ciertos contenidos en la red, apuntes de la asignatura en una plataforma como Moodle, por ejemplo, pero no al resto de internet, que el docente pudiese especificar qué contenidos son accesibles y durante cuánto tiempo sin duda puede resultar interesante.
- **Multiplataforma:** El proyecto ha sido construido íntegramente con el lenguaje de programación Java, pero el hecho de utilizar un cortafuegos propio del sistema Linux hace que no sea multiplataforma. Modificar esa parte del código y adaptarla para otros sistemas, haría que se pudiese utilizar independientemente de la plataforma, algo que es siempre atractivo.
- **Integración con otras aplicaciones:** Todos sabemos que en lo referente a la seguridad informática no se puede garantizar que una aplicación sea a prueba de todo, la integración con otros sistemas, de análisis de tráfico por ejemplo, proporcionarían un aumento de la confianza en el proyecto.

Apéndice A

Contenidos del CD

El CD tiene la siguiente estructura:

- **Fuentes:** Contiene el código fuente de la solución desarrollada.
- **Instaladores:** Contiene dos paquetes instaladores para sistemas Debian.
- **Manual:** Contiene el manual de usuario de la solución.
- **Memoria:** Contiene la memoria en formato electrónico.
- **UML:** Contiene un archivo con diagramas UML de la aplicación.

Bibliografía

- [AST06] Maarten Van Steen Andrew S. Tanenbaum. *Distributed Systems: Principles and Paradigms*. Prentice Hall, 2006.
- [Bar04] Daniel J. Barrett. *Linux Pocket Guide*. O'Reilly, 2004.
- [BH11] Amber Graner Benjamin Hill, Matthew Helmke. *Official Ubuntu Book*. Prentice Hall, 2011.
- [Bur05] Ed Burnette. *Eclipse IDE Pocket Guide*. O'Reilly, 2005.
- [CMP08] Brian W. Fitzpatrick C. Michael Pilato, Ben Collins-Sussman. *Version Control with Subversion*. O'Reilly, 2008.
- [Cop10] James O. Coplien. *Lean Architecture: for Agile Software Development*. Wiley, 2010.
- [Den07] Tom St. Denis. *Cryptography for Developers*. Syngress, 2007.
- [Dev99] Java Gui Development. *Java Gui Development*. Sams, 1999.
- [GB04] James Rumbaugh Grady Booch, Ivar Jacobson. *Unified Modeling Language Reference Manual*. Addison-Wesley Professional, 2004.
- [KA05] David Holmes Ken Arnold, James Gosling. *Java Programming Language*. Prentice Hall, 2005.
- [Koz05] Charles M. Kozierok. *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference*. No Starch Press, 2005.
- [Kra05] Martin F. Krafft. *The Debian System: Concepts and Techniques*. No Starch Press, 2005.
- [Kru03] Philippe Kruchten. *The Rational Unified Process: An Introduction*. Addison-Wesley Professional, 2003.
- [Lar03] Craig Larman. *Agile and Iterative Development: A Manager's Guide*. Addison-Wesley Professional, 2003.

-
- [MB04] James Rumbaugh Michael Blaha. *Object-Oriented Modeling and Design with UML*. Prentice Hall, 2004.
- [Mü10] Gero Mühl. *Distributed Event-Based Systems*. Springer, 2010.
- [Oak04] Scott Oaks. *Java Threads*. O'Reilly Media, 2004.
- [PC98] Douglas Kramer Patrick Chan, Rosanna Lee. *The Java Class Libraries, Volume 1: java.io, java.lang, java.math, java.net, java.text, java.util*. Addison-Wesley Professional, 1998.
- [Pit10] Esmond Pitt. *Fundamental Networking in Java*. Springer, 2010.
- [PK06] Bruce MacIsaac Per Kroll. *Agility and Discipline Made Easy: Practices from OpenUP and RUP*. Addison-Wesley Professional, 2006.
- [Pur04] Gregor N. Purdy. *Linux iptables Pocket Reference*. O'Reilly, 2004.
- [Sta04] William Stallings. *Comunicaciones y redes de computadores*. Pearson, 2004.
- [Sta06] William Stallings. *Sistemas Operativos*. Pearson, 2006.
- [Yea96] Nancy J. Yeager. *Web Server Technology*. Morgan Kaufmann, 1996.