



**PLIEGO DE PRESCRIPCIONES TÉCNICAS**

PARA LA CONTRATACIÓN DEL SERVICIO DE SOPORTE TÉCNICO Y FUNCIONAL DE LAS AULAS DIGITALES Y SISTEMAS INFORMÁTICOS DE LOS INSTITUTOS DE INNOVACIÓN TECNOLÓGICA Y OTROS CENTROS CON IDENTICAS INFRAESTRUCTURAS DE LA COMUNIDAD DE MADRID

**Índice**

1. INTRODUCCIÓN.....	2
2. OBJETO DEL CONTRATO.....	2
3. ALCANCE Y ESPECIFICACIONES DE LOS SERVICIOS.....	3
3.1. Mantenimiento preventivo y correctivo.....	3
3.2. Gestión de incidencias y peticiones. SOPORTE A USUARIOS .....	4
3.3. Mantenimiento de HARDWARE.....	4
3.4. Mantenimiento de SOFTWARE.....	4
3.5. Mantenimiento de RED.....	5
4. CONDICIONES DE PRESTACIÓN DE LOS SERVICIOS.....	5
4.1. Certificaciones de las empresas licitadoras .....	5
4.2. Requisitos de medios materiales .....	5
4.3. Requisitos de los medios personales. EQUIPO DE TRABAJO.....	6
4.3. Lugar y horario de prestación de los servicios.....	7
4.4. Gestión de incidencias. Tiempos de respuesta.....	7
5. PLANIFICACIÓN, DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS. PLAN DE SERVICIO.....	8
6. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN, .....	9
7. PROPIEDAD INTELECTUAL Y TRANSFERENCIA TECNOLÓGICA.....	9

ANEXO 1: LISTADO DE EQUIPAMIENTO INFORMÁTICO POR CENTROS

ANEXO 2: INFRAESTRUCTURAS DE LOS INSTITUTOS DE INNOVACIÓN TECNOLÓGICA





## 1. INTRODUCCIÓN.

El programa de Institutos de Innovación Tecnológica se puso en marcha en el curso 2010-2011 en quince institutos públicos de la Comunidad de Madrid seleccionados mediante convocatoria pública, con el objeto de impulsar la utilización de las tecnologías de la información y de la comunicación como una herramienta de aprendizaje en la Educación Secundaria Obligatoria.

Los Institutos de Innovación Tecnológica incorporan en sus aulas el uso de las nuevas tecnologías en al menos un tercio del horario global del alumno en un conjunto de materias, haciendo un uso intensivo de infraestructuras TIC.

Todos los Institutos han recibido una dotación específica para hacer frente al proyecto durante los cursos en los que se ha ido implantando. El aula digital como pieza tecnológica fundamental dispone de 30 puestos informáticos (un puesto por alumno), un puesto del profesor con doble monitor y una pizarra digital interactiva, además de un acceso a internet de alta velocidad. Todos los equipos se encuentran conectados a un servidor de centro desde el que se administran y gestionan los usuarios y el almacenamiento, y se controlan de forma remota los equipos de alumnos y profesores.

Al tener una cantidad de terminales elevada, y la posibilidad de que tanto alumnos como profesores vayan cambiando de aula a lo largo del día, se ha implantado la funcionalidad de "Perfiles móviles". Este sistema permite la deslocalización de los usuarios, de tal forma, que desde cualquier terminal pueden trabajar y acceder a sus archivos.

Adicionalmente infraestructuras TIC idénticas a las implantadas en los 15 institutos de innovación tecnológica se han instalado en otros 11 centros, si bien más reducidas.

La Dirección General de Infraestructuras y Servicios, en adelante DGIS, de la Consejería de Educación e Investigación de la Comunidad de Madrid se ha responsabilizado de la instalación y mantenimiento de las referidas infraestructuras, desde su dotación hasta la actualidad. Para dar continuidad a estos servicios, se hace preciso disponer a través de un contrato de servicios de soporte técnico y funcional, de personal capacitado para solventar las posibles incidencias en las referidas infraestructuras, de forma que no se vea afectado el funcionamiento de los centros.

## 2. OBJETO DEL CONTRATO.

La presente contratación tiene como objeto el soporte técnico y funcional de las aulas digitales y sistemas informáticos de los institutos de Innovación Tecnológica y otros centros con idénticas infraestructuras de la Comunidad de Madrid.

En Anexo 1, 'LISTADO DE EQUIPAMIENTO INFORMÁTICO POR CENTROS', se relacionan los centros afectados y el equipamiento instalado en cada uno de ellos.

En Anexo 2, 'INFRAESTRUCTURAS DE LOS INSTITUTOS DE INNOVACIÓN TECNOLÓGICA', se detallan las características del equipamiento instalado y se incluye información específica de procedimientos de instalación, configuración y mantenimiento del equipamiento.





A continuación se especifican los servicios que se incluyen dentro del objeto del presente contrato:

Soporte de gestión y resolución de incidencias, tanto de software como hardware, de los equipos informáticos descritos derivadas de un mal funcionamiento, avería o desconfiguración, incluyendo la sustitución de software, piezas o componentes defectuosos que serán facilitadas por la DGIS o los propios centros.

Se incluye la instalación del software necesario en los equipos informáticos para que puedan instalarse equipos adicionales en la red como impresoras, pizarras digitales y otros dispositivos. Estos equipos adicionales conectados a la red no serán objeto del contrato y su mantenimiento no está incluido en el servicio. El software utilizado será facilitado por la DGIS o por los propios centros, y en ningún caso ocasionará a la empresa gastos adicionales.

### 3. ALCANCE Y ESPECIFICACIONES DE LOS SERVICIOS.

Los servicios se realizarán sobre los equipos instalados y en funcionamiento en los centros en el momento de entrada en vigor del concurso. Los licitadores podrán inspeccionar dicho estado con anterioridad a la finalización del plazo de presentación de ofertas al concurso. Para ello deberán cursar una solicitud a la DGIS, Servicio de Tecnologías de la Información y la Comunicación, C/Santa Hortensia, 30, 2º planta. Madrid, 28002. Teléfono: 917325135-6).

Ante la posible evolución de las infraestructuras, y la incorporación de nuevos equipos informáticos en las actuales instalaciones durante la vigencia del contrato, previo acuerdo de ambas partes, podrá modificarse el inventario objeto del servicio, para lo que deberán actualizarse los anexos I y II, que recogen todas las infraestructuras incluidas inicialmente en el contrato y su ubicación en centros.

Con las actuaciones que se realicen en el marco de este contrato debe asegurarse el mantenimiento integral del referido equipamiento, de forma que se asegure que continúe operativo y en perfecto grado de funcionamiento, para ello se realizarán las siguientes actuaciones:

#### 3.1. Mantenimiento preventivo y correctivo.

Los servicios de mantenimiento preventivo consistirán en la revisión periódica, sin existir incidencias previas, de las infraestructuras informáticas, tanto de hardware como de software. Para ello la empresa adjudicataria dispondrá de los medios necesarios para acceder remotamente a los equipos de los centros a través de programas de conexión remota para monitorizar todos los equipos informáticos y analizar el estado de los mismos, pudiendo verificar el correcto funcionamiento de sus componentes.

Estos programas facilitarán también la prestación de servicios remotos de mantenimiento correctivo sin presencia en los centros cuando sea necesario.

La empresa adjudicataria elaborará un informe, al menos cada dos meses, sobre la situación de las infraestructuras de cada centro, en el que se incluirá información sobre las actuaciones realizadas con carácter preventivo e indicadores sobre el funcionamiento de las mismas.

Se considera mantenimiento correctivo todos los servicios que se realicen a petición de la DGIS o los IIT para solucionar las anomalías o averías (hardware, software) que se presenten en cualquiera de los equipos, en la red de datos o en los demás sistemas objeto del contrato.





## Comunidad de Madrid

Este tipo de mantenimiento se iniciará previa gestión de incidencias que se documentarán y se gestionarán hasta su resolución, quedando documentadas. Las correspondientes actuaciones se desarrollarán remotamente y presencialmente en los propios centros.

### 3.2. Gestión de incidencias y peticiones. SOPORTE A USUARIOS

Los servicios relacionados con el soporte a usuarios incluyen la gestión y resolución de incidencias físicas y lógicas tanto de hardware como de software. Así mismo incluyen la gestión y tratamiento de peticiones procedentes de los usuarios o de la propia DGIS, motivadas por el mantenimiento correctivo o evolutivo de las aplicaciones o sistemas.

La gestión de las peticiones e incidencias se realizará a través de la herramienta de gestión de incidencias corporativa de la DGIS, <http://gestiona.educa.madrid.org/dtic/>, a la que se dará acceso a los responsables de la empresa adjudicataria.

Si analizada la petición o incidencia por el soporte a usuarios se considera que para su resolución se exceden los servicios incluidos en el presente contrato, se procederá a su escalado a los responsables de la DGIS.

El soporte a usuarios también se responsabilizará de la comunicación de cuestiones técnicas a los centros, elaborando la documentación técnica necesaria, relacionadas con actualizaciones y prestación de los servicios.

### 3.3. Mantenimiento de HARDWARE.

La DGIS facilitará un stock de material de los principales componentes instalados en los centros. Cuando se requiera, la empresa adjudicataria verificará su correcto funcionamiento y podrá utilizarlos para la resolución de incidencias.

La empresa adjudicataria se encargará de gestionar el inventario del material de reposición que facilite la DGIS.

De forma preventiva se realizarán revisiones periódicas detalladas del correcto funcionamiento de los equipos a nivel de hardware y de sus componentes. Incluirá la revisión de los servidores de centro, equipos informáticos (islas) y equipos de acceso de usuarios.

El mantenimiento correctivo incluirá todas las actuaciones necesarias para la resolución de incidencias que puedan surgir, para lo que la DGIS o los propios centros facilitarán las piezas o componentes necesarios en su caso, correspondiendo a la empresa adjudicataria todos los trabajos de manipulación, sustitución y configuración de los equipos hasta que se verifique su completa operatividad en su ubicación.

### 3.4. Mantenimiento de SOFTWARE.

De forma preventiva se comprobará el correcto funcionamiento del software instalado, en servidores y equipos de isla, incluyéndose la revisión de los parámetros críticos de los equipos y de la red.

Especialmente se comprobará el funcionamiento de herramientas del servidor, actualizaciones, sistema antivirus, copias de seguridad y servicios relacionados con la administración de usuarios, grupos de trabajo, permisos y accesos.







## Comunidad de Madrid

El mantenimiento correctivo incluirá la reinstalación de software en el caso de anomalías en el funcionamiento y la recuperación de datos de copias de seguridad en caso de pérdidas de los mismos, así como la reconfiguración del software ya instalado.

La empresa adjudicataria realizará la actualización de los sistemas operativos y de las diferentes aplicaciones instaladas en cada equipo cuando sea requerido. Asimismo realizará la instalación de software adicional, facilitado por la DGIS o por los propios centros, que se requiera para que nuevos periféricos puedan funcionar.

### 3.5. Mantenimiento de RED.

La empresa adjudicataria se responsabilizará preventivamente del análisis y monitorización de los parámetros básicos de la red de las distintas instalaciones, de forma que se garantice su adecuado funcionamiento, asegurando la correcta configuración y optimización de las comunicaciones entre los sistemas conectados en red

El mantenimiento correctivo incluirá las actuaciones de reconfiguración del hardware y software de red después de actuaciones en el sistema o de incidencias.

La empresa adjudicataria no se responsabilizará de la sustitución de cableado defectuoso ni de la sustitución de elementos de red.

## 4. CONDICIONES DE PRESTACIÓN DE LOS SERVICIOS.

### 4.1. Certificaciones de las empresas licitadoras

Por razón de la naturaleza del contrato las empresas licitadoras deben estar en posesión de las acreditaciones establecidas en el Pliego de Cláusulas Administrativas Particulares, en adelante PCAP.

### 4.2. Requisitos de medios materiales

La empresa prestataria del servicio habrá de aportar como mínimo los siguientes recursos materiales:

- Los equipos informáticos necesarios para acceder en remoto a los ordenadores (servidores y puestos de aula de los centros). Estos equipos deberán tener capacidad suficiente para realizar conexiones a internet (varias conexiones simultáneas), software para realizar el control remoto de equipos y funcionalidades relacionadas con este control.
- Equipo portátil que soporte la instalación de un sistema MAX (Madrid\_linux), en la última versión publicada.
- Material fungible.
- Teléfono móvil y facilidades de desplazamiento a los centros educativos en los que están instaladas las infraestructuras.
- Identificativos el personal que presta el servicio.

El equipo de trabajo utilizará asimismo el equipamiento que facilite la DGIS para la conexión remota con los centros a través de redes propias institucionales.





La empresa adjudicataria deberá utilizar los componentes suministrados por la DGIS o por los propios centros para el mantenimiento y resolución de las incidencias de las infraestructuras.

### 4.3. Requisitos de los medios personales. EQUIPO DE TRABAJO.

La empresa adjudicataria destinará a la ejecución del contrato al menos a dos personas:

- Jefe de Proyecto: Que ejercerá funciones de coordinación del servicio y tendrá dedicación parcial.
- Técnico: Con dedicación exclusiva al proyecto.

Además del referido equipo de trabajo estable, se valorará que las empresas pongan a disposición del proyecto otro personal técnico que pueda realizar, cuando sea necesario, tareas requeridas para la resolución de incidencias de forma que no se sobrepasen los tiempos establecidos para la resolución de las mismas. En este sentido la empresa podrá utilizar otros técnicos para tareas como la sustitución de piezas o la configuración de equipos en los propios centros, siendo necesario que las empresas licitadoras justifiquen esta posibilidad. A tal efecto las empresas licitadoras podrán proponer y justificar la incorporación de personal adicional mediante una bolsa de horas, para el período de vigencia del contrato, sobre la que se irán contabilizando las correspondientes actuaciones.

El número de horas propuesto por la empresa será objeto de valoración según lo establecido en el PCAP.

La DGIS podrá exigir el cumplimiento y ejecución total de la bolsa de horas adicionales propuestas por la empresa adjudicataria en actuaciones específicas relacionadas con el objeto del contrato.

El personal adscrito al proyecto deberá contar con las titulaciones exigidas en el PCPA.

La experiencia laboral del técnico adscrito al proyecto en los sistemas y tecnologías implantados en los centros e infraestructuras objeto del contrato, se especifica en el PCPA.

En ningún caso existirá relación contractual entre ninguno de los componentes del equipo de trabajo y la DGIS, siendo la relación entre la empresa adjudicataria y la DGIS.

Las empresas licitadoras deberán establecer el procedimiento de sustitución de cualquiera de los técnicos, tanto del jefe de proyecto como del técnico in situ, por bajas de forma que el servicio no quede interrumpido. Las vacaciones de estos técnicos serán consensuadas con la DGIS de forma que no afecte a la necesaria continuidad del servicio.

El jefe de proyecto, designado por la empresa adjudicataria, deberá pertenecer a la plantilla de la misma y ejercerá las funciones de supervisión y gestión de los medios personales y materiales aportados.

A este Coordinador corresponderá también en exclusiva la impartición directa de las órdenes e instrucciones de trabajo a los trabajadores de la empresa adjudicataria.

De igual modo el Coordinador del Servicio designado por la empresa será el canal único de relación con la Consejería de Educación e Investigación para tratar los diferentes aspectos relacionados con la prestación del servicio.

Corresponde a la empresa adjudicataria ejercer la dirección de los medios personales propuestos y asegurar el cumplimiento del servicio, así como asumir las obligaciones inherentes respecto a sus trabajadores, como son, entre otras:





## Comunidad de Madrid

- El pago de los salarios.
- La concesión de permisos, licencias y vacaciones.
- Sustituciones.
- Cumplimiento de las obligaciones en materia de prevención de riesgos laborales.
- Imposición de sanciones disciplinarias.
- Asunción de las correspondientes obligaciones en materia de Seguridad Social.

La incorporación del equipo de trabajo que prestará sus servicios de forma continuada a lo largo de toda la vigencia del concurso se realizará inmediatamente después de la firma del contrato (al siguiente día laboral).

El equipo humano que se incorporará tras la formalización del concurso deberá estar formado por las personas relacionadas en la oferta adjudicataria y consecuentemente valoradas. Podrán realizarse cambios de las personas que integran el equipo de trabajo si se dan las siguientes condiciones:

- Justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio.
- Presentación de posibles candidatos con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir.
- Aceptación de los candidatos por parte de la DGIS.

El equipo humano lo elegirá siempre la empresa, siempre que los técnicos presentados cumplan los requisitos exigidos y sean validados por la DGIS.

La DGIS se reserva la facultad de proponer cambios en el equipo de trabajo para mejorar el servicio y efectuar entrevistas personales o pruebas de cualificación técnica al personal asignado.

### 4.3. Lugar y horario de prestación de los servicios.

El horario para la prestación del servicio se establece en 40 horas semanales.

Los servicios se centralizarán en la sede de la DGIS, Calle Santa Hortensia, 30. 2ª planta, y de forma puntual será necesario el desplazamiento hasta los centros detallados en el Anexo I, dando servicio presencial diario de 8 horas (días laborales). Preferentemente se actuará en horario de 9:00 a 14:00 horas y de 15:00 a 18:00 horas, pudiendo modificarse estos períodos en función de requerimientos del servicio. Los servicios no se darán durante el mes de agosto, debiendo realizarse durante el resto de meses.

Se considera horario de servicio a la franja horaria diaria en la que la empresa está en disposición, tanto de recibir una comunicación de incidencia como de visitar y acometer la resolución de la misma independientemente del personal desplazado en el organismo.

Los servicios objeto del presente contrato se efectuarán obligatoriamente en las propias dependencias de la DGIS, debido a que los técnicos de la empresa adjudicataria deberán trabajar conjuntamente con los responsables y técnicos de la DGIS y acceder a la intranet y entornos de prueba que se replican en dichas dependencias.

La DGIS pondrá a disposición del equipo de trabajo, para la ejecución del contrato, un espacio definido para la ubicación de los medios materiales y personales necesarios para la prestación del servicio.

### 4.4. Gestión de incidencias. Tiempos de respuesta.

En función de la naturaleza de los equipos a mantener, así como de la magnitud de la incidencia, se establecen las siguientes criticidades:





## Comunidad de Madrid

- Criticidad alta, para equipos servidores y funcionalidades de red que afecten al servidor.
- Criticidad media, para equipos de isla que dan servicio a varios puestos de trabajo.
- Criticidad baja, para puestos de trabajo de usuario final (terminales).

El adjudicatario estará obligado a respetar un tiempo de respuesta y de resolución máximo para cada tipo de incidencia, según se refleja en la siguiente tabla:

CRITICIDAD INCIDENCIA	TIEMPO DE RESPUESTA	TIEMPO DE RESOLUCIÓN
Alta	2 horas	12 horas
Media	4 horas	36 horas
Baja	8 horas	60 horas

Se entiende por tiempo de respuesta el plazo transcurrido desde la comunicación de una incidencia por parte del centro o de la DGIS, hasta el momento en que el adjudicatario se pone a disposición del usuario en las instalaciones donde esté ubicado el equipo, personándose en las mismas para resolverla o por control remoto cuando pueda resolverse así la incidencia.

Se entiende por tiempo de resolución el plazo transcurrido desde que se efectúa la respuesta y se inicia la gestión de la incidencia hasta la aceptación por parte del centro, de la resolución de la incidencia. Es de aplicación en el caso de que la misma pueda resolverse con material o componentes en stock puesto a disposición del proyecto cuyo inventario es gestionado por la propia empresa en el marco del contrato o mediante actuaciones en el software que puedan ejecutarse a cargo de las licencias disponibles.

En el caso de que el material necesario para la resolución de la incidencia no esté disponible el tiempo de resolución se contabilizará desde el momento en que la empresa disponga del material necesario para la resolución hasta la aceptación por parte del centro de la resolución de la incidencia.

Los tiempos se contabilizarán dentro del horario de servicio establecido.

La empresa adjudicataria deberá realizar las labores de mantenimiento y las reparaciones en los centros sin que interfieran en el funcionamiento educativo de los mismos, acordando con los centros las franjas horarias más adecuadas para realizar estas actuaciones.

## 5. PLANIFICACIÓN, DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS. PLAN DE SERVICIO.

Corresponde a la DGIS la supervisión y dirección de los trabajos así como proponer las modificaciones que convenga introducir para la correcta consecución de los objetivos establecidos en el contrato.

El jefe de proyecto designado por el adjudicatario será el interlocutor único con las personas responsables nombradas por la DGIS. El jefe de proyecto se reunirá periódicamente con los responsables de la DGIS y analizarán tanto el servicio de mantenimiento y soporte realizado, como la evolución de los sistemas y necesidades.

Para ello y con al menos dos días de antelación a la fecha propuesta de reunión remitirá el informe de seguimiento correspondiente. El informe del servicio contemplará, al menos, los siguientes aspectos: seguimiento del servicio, coordinación de las acciones en curso,





## Comunidad de Madrid

incidencias significativas ocurridas y gestión dada, análisis de problemas y recomendaciones para la mejora del servicio, estrategias o cualquier mejora que se considere oportuna.

Todas las cuestiones necesarias para la prestación de los servicios requeridos serán facilitadas por la empresa adjudicataria garantizándose el cumplimiento de los requisitos establecidos, configurándose al efecto un documento denominado 'Plan de Servicio' que deberá incluir los siguientes puntos:

- Descripción y planificación del servicio ofertado.
- Mantenimiento preventivo: planificación, metodología y procedimientos con indicación de dedicación presencial.
- Mantenimiento correctivo: planificación, metodología y procedimientos especificando tiempos de respuesta y resolución.
- Mantenimiento de hardware, software y red de datos. Planificación, metodología y procedimientos
- Atención a usuarios.
- Organización de servicios y actuaciones en centros.
- Organización de recursos humanos y técnicos adscritos al servicio.

Una vez iniciado el contrato se actualizará el 'Plan de Servicio', con información de los trabajos realizados referente a las operaciones e incidencias tratadas y las modificaciones en los procedimientos que sean necesarias.

La proposición técnica de los licitadores interesados en el presente deberá incluir una propuesta de 'Plan de Servicio' que se deberá adecuar a la estructura establecida en este apartado. Esta propuesta será evaluada y valorada para la adjudicación del contrato.

## 6. SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN,

El adjudicatario quedará obligado al cumplimiento de lo que dispone el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

El adjudicatario queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato, información o documentación que se pueda conocer con ocasión del cumplimiento del contrato, especialmente las de carácter personal, que no podrá copiar o utilizar con una finalidad diferente a la que figura en este pliego, ni tampoco ceder a otros ni tan solo a efectos de conservación sin la autorización escrita de la DGIS.

El adjudicatario se compromete a no utilizar la información y datos proporcionados por la Administración u obtenidos en la ejecución del contrato, para fines ajenos al mismo y no previstos en el presente Pliego.

El incumplimiento por parte de la empresa de estos términos generará la resolución del contrato y la pérdida de la garantía definitiva, todo ello sin perjuicio de la responsabilidad civil o penal que procediera.

## 7. PROPIEDAD INTELECTUAL Y TRANSFERENCIA TECNOLÓGICA.

Toda la documentación generada durante la ejecución del contrato será de propiedad exclusiva de la administración, sin que el adjudicatario pueda conservarla, ni obtener copia





## Comunidad de Madrid

de la misma o facilitarla a terceros sin la expresa autorización de este centro directivo, que la daría en su caso previa petición formal del adjudicatario con expresión del fin.

El adjudicatario aceptará expresamente que los derechos de explotación de los sistemas y desarrollos realizados en el marco del presente contrato corresponden únicamente a la administración, que podrá utilizarlos y cederlos sin ninguna limitación.

Durante la ejecución de los trabajos objeto del contrato el adjudicatario se compromete a facilitar en todo momento, a las personas designadas por la DGIS para estos efectos, la información y documentación que soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollen los trabajos así como de las tecnologías, métodos y herramientas utilizadas. Para realizar esta tarea será imprescindible la elaboración de una memoria explicativa del funcionamiento del servicio durante el contrato.

El JEFE DE SERVICIO DE TECNOLOGÍAS  
DE LA INFORMACIÓN Y LA COMUNICACIÓN

Fdo.: José Quirino Vargas Ibáñez





## ANEXO 1

### LISTADO DE EQUIPAMIENTO INFORMÁTICO POR CENTROS

		DOTACIONES				Total		Total	Total
	Centro	DOT 1	DOT 2	DOT 3	DOT 4	Aulas	Servidores	PC-ISLA Ó PROFESOR	Terminales (NL300-MCT)
IIT(Institutos de Innovación tecnológica)	ALPEDRETE	2	1	2	3	8N	1	32+2U	240N+10U
	CALDERÓN DE LA BARCA	3	2	3	3	11N	1	44+2U	330N+10U
	CARDENAL CISNEROS	3	1	2	4	10N	1	40+2U	300N+10U
	GALILEO GALILEI	3	4	3	3	13N	1	52+2U	390N+10U
	GRAN CAPITÁN	3	3	2	3	11N	1	44+2U	330N+10U
	ISAAC PERAL	4	2	3	3	12N	1	48+2U	360N+10U
	LAS ROZAS I	2	2	2	3	9N	1	36+2U	270N+10U
	LEONARDO DA VINCI	3	2	4	3	12N	1	48+2U	360N+10U
	MARÍA MOLINER	2	2	2	2	8N	1	32	240N
	MIGUEL DE CERVANTES	4	3	4	4	15N	1	60+2U	450N+10U
	PRÍNCIPE FELIPE	4	4	4	4	16N	1	64+2U	480N+10U
	ROSA CHACEL	3	2	4	3	12N	1	48+2U	360N+10U
	SALVADOR DALÍ	3	2	4	3	12N	1	48+2U	360N+10U
	SAN ISIDRO	3	3	2	2	10N	1	40+2U	300N+10U
	SATAFI	3	2	3	4	12N	1	48+2U	360N+10U
NO IIT	SAN MATEO	1	1	2	0	2U+2N	1v.o	8+14U	60N+65U
	CARMEN MARTIN GAITE	1	0	0	0	1U	1v.o	6+2	30+10
	CARPE DIEM	2	0	0	0	2U	1v.o	12+2	60+10
	FRANCISCO AYALA	1	0	1	0	2U	1v.o	12	60
	TIRSO DE MOLINA	1	0	0	0	1U	1v.o	6	30





		DOTACIONES				Total		Total	Total
	Centro	DOT 1	DOT 2	DOT 3	DOT 4	Aulas	Servidores	PC-ISLA Ó PROFESOR	Terminales (NL300-MCT)
Sin servidor	ARCIPRESTE DE HITA	0	0	1	0	1N		4	30
	HOTEL ESCUELA	0	0	0	2	2N		4+5	34+36
	JUAN DE LA CIERVA(Tablets)	0	0	0	1	1N		4	30
	MUNDIAL86(piscina)	0	0	0	1	1N		4	30
	CEIPS Maria Moliner(Villanueva de la Cañada)	0	0	1	0	1N		4	30
	CEIP Angel Gonzalez(Leganés)	0	0	1	0	1N		4	30
	<b>TOTALES SOLO IIT</b>	45	35	44	46	171		712	5270
	<b>TOTALES</b>	50	36	50	46	188		803	5815

### Descripción de la información de la tabla.

Ejemplo con cabecera, línea de ejemplo y descripción.

Se utiliza terminología específica descrita y detallada en Anexo 2.

DOTACIONES				Total		Total	Total
DOT 1	DOT 2	DOT 3	DOT 4	Aulas	Servidores	PC-ISLA Ó PROFESOR	Terminales (NL300-MCT)
2	1	2	3	8N + 2U	1	32+2U	240N+10U
<p>Número de aulas instaladas en cada dotación. (4 dotaciones)</p> <p>Interpretación de datos del ejemplo:</p> <p>En la primera dotación se instalaron 2 aulas, en la segunda 1, en la tercera 2 y en la cuarta 3.</p>				<p>Total de aulas instaladas</p> <p>N = Aula o equipo de terminales Ncomputing.</p> <p>U = Aula o equipo de terminales USB</p> <p>8N: 8 aulas con terminales Ncomputing L300</p> <p>2U: Dos islas con terminales Multipoint USB MCT</p>	<p>Número de servidores de centro</p> <p>v.o.: Versión inicial (funcionalidad restringida).</p>	<p>Total 32+2=34 PC.</p> <p>32 conectados a terminales Ncomputing y 2 conectados a Multipoint USB</p>	<p>240 Ncomputing</p> <p>10: USB Multipoint.</p>

## ANEXO 2

# INFRAESTRUCTURAS DE LOS INSTITUTOS DE INNOVACIÓN TECNOLÓGICA



## I. Tabla de contenido

A.	AULAS DIGITALES.....	5
1.	Introducción .....	5
2.	Composición de un aula .....	7
3.	Tolerancia a Fallos .....	9
4.	Requisitos para montar un aula .....	10
5.	Configuraciones de red .....	11
a)	Configurar la red en Windows.....	13
b)	Configurar la red en MAX.....	15
6.	Configuración de Vspace (software de Ncomputing) .....	16
7.	Instalación de los terminales.....	18
8.	Configuración de los terminales.....	19
9.	Configuración para el puesto del profesor .....	24
B.	PUESTOS CON TERMINALES USB (MULTIPOINT) .....	27
1.	Hardware Multipoint, conexiones del MWS300.....	27
2.	Conexión de una isla Multipoint .....	28
a)	Conexionado de la red.....	29
b)	Montaje de equipos Multipoint Aislados .....	29
c)	Requisitos para montar un sistema Multipoint.....	29
3.	Proceso de arranque de un equipo .....	30
4.	Perfiles de usuario.....	33
a)	¿Que es el perfil del usuario? .....	33
b)	¿Que significa que sea móvil?.....	33
c)	Borrado de perfil en Windows .....	33
5.	Políticas o directivas de grupo .....	34
a)	¿Qué son las políticas de grupo?.....	34
C.	PROCEDIMIENTO DE ACTUALIZACION DEL DRIVER MCT .....	35
D.	PROCEDIMIENTO PARA UNIR UN EQUIPO AL DOMINIO .....	37
1.	Windows.....	37
2.	MAX.....	37
3.	En general.....	37
4.	Cómo unir un equipo al dominio .....	38
1)	Procedimiento para MAX.....	38
2)	Procedimiento para Windows: .....	43
3)	ANEXO 1. Cómo conectarse por escritorio remoto a otro equipo.....	53
4)	ANEXO 2. Cómo sacar un equipo del dominio.....	57
E.	MANUAL DEL SERVIDOR DE CENTRO .....	58
1.	CARACTERÍSTICAS DEL SERVIDOR DE CENTRO.....	58
2.	CONFIGURACIÓN DE LA BIOS .....	58
3.	INSTALACIÓN DESDE MAQUETA(USB) .....	59
a)	Iniciar System RescueCD .....	59
b)	Restaurar servidor.....	59
c)	Generar nueva imagen .....	59
d)	Chequeo de Memoria .....	60
e)	Cargar /boot/grub/grub.cfg del servidor .....	60



f) MaX-Servidor, con Linux 2.6.32-33-server .....	60
4. CONFIGURACIONES DESPUÉS DE REMAQUETAR .....	60
5. INSTALACIÓN DESDE CERO .....	63
6. ACTIVAR EL PANEL DE MAX-CONTROL .....	83
7. PARTICIONES Y RAID .....	83
8. ACCESO AL PANEL DE ADMINISTRACIÓN WEB .....	88
9. ESTADO DE LOS MÓDULOS .....	90
10. CONFIGURACIÓN GENERAL .....	91
11. CONFIGURACIÓN DE RED .....	92
12. CONFIGURACIÓN DE DNS .....	94
13. CONFIGURACIÓN DE LA PUERTA DE ENLACE .....	95
14. CORTAFUEGOS .....	96
15. CONFIGURACIÓN DEL SERVICIO DHCP .....	99
16. CONFIGURACIÓN DEL SERVICIO DNS .....	100
17. CONFIGURACIÓN DEL SERVICIO NTP .....	101
18. USUARIOS Y GRUPOS .....	102
1. Usuarios .....	102
2. Grupos .....	103
19. CONFIGURACIÓN DE LA VPN .....	106
20. COMPROBACIONES DE LA VPN .....	108
21. CONECTARSE A LA VPN DESDE MAX .....	111
22. CONECTARSE A LA VPN DESDE WINDOWS .....	114
23. CREAR UN BACKUP DEL LDAP .....	118
24. RESTAURAR EL BACKUP DEL LDAP .....	118
25. CAMBIAR UN DISCO AVERIADO .....	119
a) Cambio del disco .....	122
26. EL DIRECTORIO /HOME/SAMBA/NETLOGON .....	124
27. COMO ACTUALIZAR EL FICHERO "CONFIGURACION_FIREFOX.ZIP" .....	125
28. CREAR COPIA DE SEGURIDAD DE /HOME/SAMBA / CON 'TAR ' .....	126
29. RESTAURAR COPIA DE SEGURIDAD DE /HOME/SAMBA CON 'TAR ' .....	126
30. APAGADO / REINICIO DEL SERVIDOR .....	128
31. CONFIGURAR EL BOTÓN DE ENCENDIDO/APAGADO .....	128
32. RESOLUCIÓN DE PROBLEMAS .....	129
a) Reparar ficheros de cuotas .....	129
33. CAMBIO DE UNA INTERFAZ DE RED .....	132
34. ALGUNA DE LAS INTERFACES DE RED NO RESPONDE .....	134
35. COMANDOS DE INTERÉS .....	134
a) Abrir una consola(cmd) de Windows desde el servidor de centro .....	134
b) Averiguar las conexiones activas de SAMBA .....	134
c) Reiniciar un equipo en Windows desde el servidor de centro .....	134
F. PROCEDIMIENTO: CONFIGURACIÓN EQUIPO DE ALUMNO CON TERMINALES USB .....	136
1. CÓMO ACTUALIZAR LA BIOS .....	146
2. CONFIGURACIÓN DE LA BIOS .....	146
3. POSIBLES INCIDENCIAS Y SOLUCIÓN A LAS MISMAS .....	146
a) Terminales en negro .....	146
b) Estaciones que no se asignan .....	148



c) Isla en negro .....	150
d) Cable USB en mal estado .....	151



## A. AULAS DIGITALES

### 1. Introducción

El objetivo de este tipo de aulas es reducir al mínimo el número de ordenadores PC tradicionales para sustituirlos por terminales ligeros cuyas ventajas son: dispositivos mucho más compactos, consumo menor de potencia y por tanto de emisión de calor y son más baratos. Su tamaño es tan pequeño que se pueden incluso acoplar a la parte trasera de los monitores.

Los terminales ligeros no tienen potencia de cálculo para ser autónomos, es decir, no pueden ejecutar un Sistema Operativo de escritorio como Windows o Linux, sólo se componen de un hardware mínimo para abrir una **sesión remota** en los equipos PC que son los que verdaderamente tienen instalado el Sistema Operativo y actúan como servidores de sesiones. En los IIT (Institutos de Innovación Tecnológica) se instalan tres PCs para dar servicio a 30 terminales (10 por PC). La potencia de los PCs que se instala es suficiente para que un PC de servicio a 10 terminales con sobrada fluidez haciendo un uso habitual de ofimática y navegación pero realmente no existe un límite en el número de terminales más que el de las limitaciones del propio hardware del equipo.



*Imagen 1: Instalación de un terminal en la parte trasera de un monitor*

Los terminales utilizan una red Ethernet para la comunicación con los PCs. La conexión física se realiza mediante un conector RJ45 a una velocidad de enlace de 100Mbps, ancho de banda suficiente para enviar la información de vídeo y otros eventos como la posición del ratón y pulsaciones de teclas. La ventaja de utilizar una red Ethernet es que los PCs servidores no tienen porqué estar próximos a los puestos de alumno, ni siquiera en la misma sala. En los IIT los servidores de cada aula se ubican en el rincón de la mesa del profesor.



*Imagen 2: Conexiones de un terminal NComputing L300*

Los PCs que ahora actúan como servidores de escritorio remoto, necesitan un sistema



servidor como Windows 2008 Server R2 o Linux (MAX 9.5 en nuestro caso) Dicho sistema permite que varios usuarios distintos tengan abierta sesión remota (desde el terminal) usando gráficos, sonido y dispositivos conectados por USB.

Este sistema permite abrir una sesión gráfica con el equipo remoto y da al usuario la misma sensación tal como si lo hiciera localmente pero tiene algunas limitaciones respecto al sistema tradicional de un PC por puesto. En general se tienen las restricciones habituales de una conexión por escritorio remoto como que el usuario no pueda cambiar la resolución de su pantalla pero además se enumeran los siguientes inconvenientes que se deberían tener muy en cuenta si se plantea montar un aula de este tipo:

- El reconocimiento de dispositivos conectados por USB al terminal ligero es limitado, no se recomienda por ejemplo conectar pizarras digitales ya que no tienen buen soporte. Por eso no recomendamos el uso para el puesto del profesor.
- El uso de Arduino o dispositivos similares es factible pero se vuelve complejo ya que un usuario en su sesión puede ver las placas Arduino de las demás sesiones(en nuestro caso hasta 10) y tiene que discernir qué placa es la suya.
- Algunas aplicaciones que funcionan bien en las versiones de escritorio de Windows pueden no hacerlo en Windows Server o no ser compatibles por estar ejecutándose en un entorno multiusuario al tener que abrir una misma instancia de la aplicación en el mismo equipo. Cada vez es menos usual que una aplicación falle por este motivo ya que cada vez tienen más en cuenta estos entornos de trabajo donde se virtualizan o se comparten los recursos, pero conviene asegurarse antes de la compatibilidad de las aplicaciones que se tenga previsto utilizar.
- Las aplicaciones que necesitan acceso exclusivo al hardware del equipo siendo el caso más típico la tarjeta gráfica, no funcionarán o como mucho sólo se podrá abrir una sola instancia de aplicación. Hay ciertas aplicaciones de vídeo que al hacer uso exclusivo de la gráfica, esta queda bloqueada para su uso en las sesiones de otros usuarios.





## 2. Composición de un aula

La imagen 3 muestra la arquitectura típica de un aula de terminales tal y como se monta en los IIT. Exceptuando el servidor de centro, todos los demás elementos están ubicados dentro del aula:

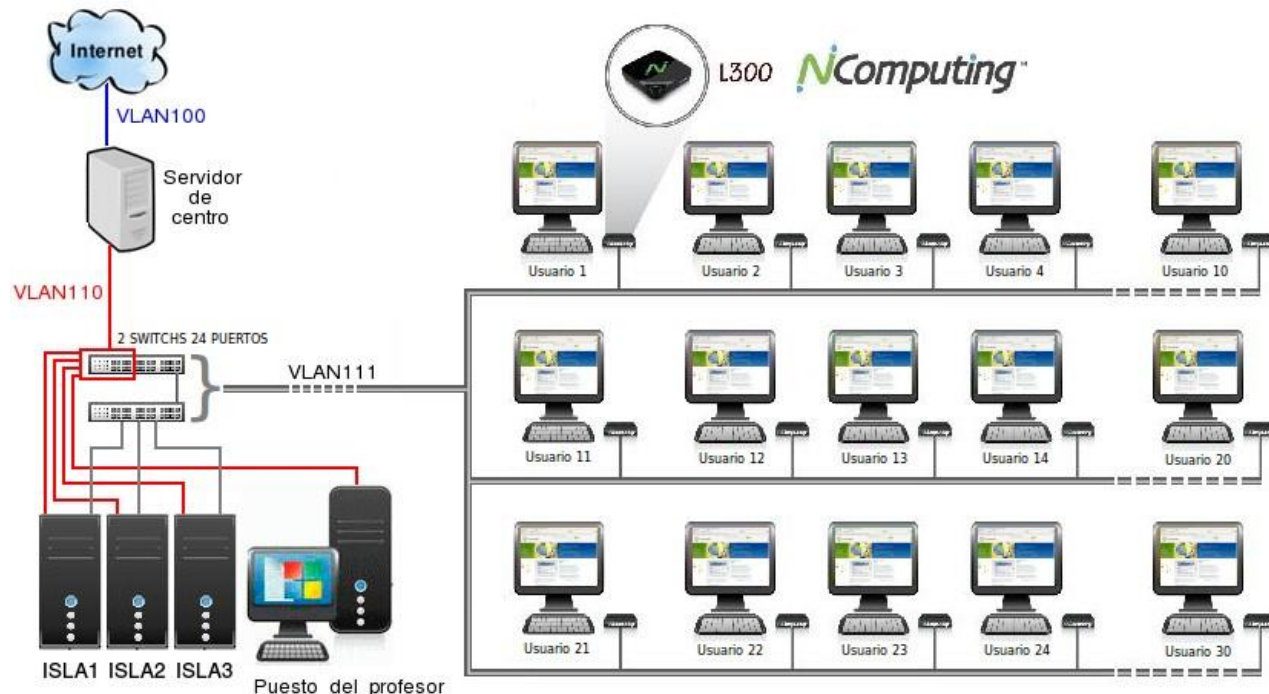


Imagen 3: Arquitectura de un aula de terminales

En el aula se instalan dos switches de 24 puertos (también sería factible uno de 48) para dar servicio a todas las conexiones de red necesarias, que son: 30 terminales, un equipo de profesor, tres equipos servidores (6 conexiones ya que cada servidor usa dos tarjetas de red) y opcionalmente una impresora de red y varios puntos adicionales para por ejemplo la conexión de un portátil o punto Wifi.

A los equipos servidores de sesiones se les denomina coloquialmente “ISLAS”. Estos equipos una vez configurados no llevan conectado ni monitor, ni teclado, ni ratón ya que no se trabaja con ellos directamente y se accede a ellos por conexión de red cuando hace falta realizar alguna tarea administrativa.

El tráfico de red entre los terminales y las ISLAS puede ser considerable sobre todo si tenemos en cuenta la instalación de varias aulas. Por ello para optimizar el número de colisiones de red es conveniente aislar la red de terminales de la red de acceso a Internet (la VLAN110 en los IIT). Para ello lo único necesario es que los equipos de ISLA dispongan de una tarjeta de red adicional y al menos uno de los switches del aula tiene que ser gestionable para poder crear una VLAN adicional y aislar así la red de los terminales.

En la figura 3 se puede observar esta división del switch siendo los trazos en rojo la VLAN110. Los trazos en gris formarían la red de terminales NComputing generalmente llamada VLAN111. La característica de la red de terminales es que cada aula tiene su propia VLAN111, es decir, es independiente a las demás VLAN111 (no se comunican entre ellas) y no sale ningún tráfico de la red de terminales fuera de su propia aula.

El switch secundario se utiliza simplemente para ampliar los puertos necesarios para los terminales y por ello no hace falta que sea gestionable. Se enlaza con el switch principal mediante un puerto que pertenezca a la VLAN111(generalmente el puerto 24) por lo que todas sus bocas pertenecerán a dicha VLAN111.

Aunque los terminales funcionan a 100MBps es necesario que al menos el puerto de enlace del switch secundario con el switch principal sea a velocidad Gigabit(1000Gbps). En los equipos de ISLA, la interfaz de red que se utiliza para la comunicación con los terminales tiene que hacer frente mínimo a 10 dispositivos y la interfaz de red para la VLAN110 tiene que soportar la carga de perfiles móviles desde el servidor de centro además del tráfico de navegación a Internet, por ello igualmente es imprescindible que ambas interfaces también funcionen a velocidad Gigabit.

Todos los IIT disponen de un servidor de centro. Este no es necesario para la implantación de una aula con terminales pero en el caso de los IIT se convierte en algo imprescindible debido al valor que ofrece para la gestión de usuarios y equipos. El servidor se compone de un dominio Windows(configurado mediante SAMBA en un S.O. Linux) que permite a cada usuario tener su propio perfil de trabajo siendo éste perfil de tipo móvil, lo que significa que pueden iniciar sesión en cualquiera de los equipos teniendo disponible su escritorio. Además de la administración de usuarios permite cierto control de los equipos, por ejemplo para programar su encendido y apagado.



### 3. Tolerancia a Fallos

Uno de los problemas que nos podemos encontrar cuando se centraliza un servicio es el fallo del mismo. Según la arquitectura de la figura 3 por cada isla que falle se pierde el servicio en 10 puestos. La ventaja que tienen los terminales NComputing es que se pueden configurar rápidamente para que su conexión la realicen a cualquier otra ISLA que haya disponible. En el caso de los IIT, cuando falla una ISLA lo ideal es dividir sus 10 terminales entre las otras dos ISLAS, quedando estas con una carga de 15 terminales, algo que es totalmente asumible dadas su características(ver el apartado siguiente).

Sí un equipo puede con 15 terminales se podría pensar en utilizar sólo dos equipos por aula ampliando si hiciera falta sus características, por ejemplo mas memoria. Desde el punto de vista económico puede salir más rentable emplear dos equipos potentes a tres equipos más sencillos, pero teniendo sólo dos equipos si falla una ISLA la otra tendría que soportar el doble de terminales, es decir, 30 terminales, lo que sería ya demasiada carga para una sola ISLA siendo necesario una máquina extremadamente potente de manera que dos equipos con tales características saldrían mas caros que tres con menos prestaciones. Por ello, desde el punto de vista para la tolerancia es preferible tener mas ISLAS con menos prestaciones a tener menos islas aunque estas sean mas potentes.

Como norma general, si se desea tolerancia a fallos para al menos el fallo de una ISLA, se debería cumplir la regla de que el reparto de carga final en el resto de ISLAS sea aceptable.

El software de gestión de los terminales instalado en los equipos(VSpace) permite realizar el cambio de configuración para que un terminal se conecte a otra ISLA sin demasiada dificultad, además de que se puede realizar seleccionando un grupo de terminales para que no haya que hacerlo uno por uno. Aun así lo ideal sería que el balanceo de terminales fuera automático para que en caso de fallo, el proceso fuera transparente para el usuario y no tuviera que realizar ninguna intervención, algo que de momento no está implementado.

En la configuración de los terminales se permite especificar un listado de ISLAS a las que el terminal intentará conectar de forma secuencial, de manera que si una ISLA no está disponible intentará realizar la conexión con la siguiente. Esta configuración que a priori puede parecer ventajosa para realizar un balanceo automático no lo es ya que no se consigue un balanceo activo y se puede sobrecargar con facilidad una de las ISLAS mientras que el resto no tendrían ningún terminal asociado, por ello de momento la mejor opción es realizar el balanceo manualmente cuando se detecte el fallo.



#### 4. Requisitos para montar un aula

El montaje de un aula de terminales implica los siguientes pasos:

- Lo primero es establecer el número de terminales que se instalarán en el aula. En los IIT son 30 puestos. Con el número de terminales fijados hay que decidir cuantos equipos serán necesarios para darles servicio sin apurar los recursos de la máquina. Este valor dependerá de la potencia de la máquina. Como referencia en los IIT según las características de los equipos que se montan(ver más adelante) se asignan diez terminales por ISLA.
- Se necesitará electrificar el aula con las tomas de corriente eléctrica necesaria. Cada puesto de alumno necesita dos tomas de corriente, una para el terminal y otra para monitor. Dos para puesto de profesor(tres si lleva monitor auxiliar). Cada equipo ISLA necesita una toma si se deja sin monitor. Y habrá que tener en cuenta periféricos adicionales como impresoras o escáneres y alguna toma extra para uso general.
- Tomas de red:
  - Una por terminal(suponemos 30): 30
  - 2 por ISLA(suponemos 3 islas con dos tarjetas de red): 6
  - Puesto de profesor: 1
  - Impresora de red: 1

Total 38 tomas. Se recomienda alguna toma adicional en el puesto del profesor.
- Los switches necesarios(uno o dos según su número de puertos) para dar servicio a las tomas de red teniendo en cuenta que en al menos uno de los switches hay que configurar una VLAN y por ello tiene que ser gestionable.
- Red de acceso a internet. Para una o dos aulas, podrían funcionar perfectamente utilizando la red educativa VLAN100 que normalmente tienen los centros, no haría falta disponer de una subred interna como la VLAN110, solo es algo recomendable y que se vuelve imprescindible cuando el centro quiere gestionar su red interna para poder crear sus propios servicios de red.

Los requisitos hardware de una ISLA dependen del número de terminales que vaya a soportar y del software que se use. A modo de referencia se indica los requisitos mínimos para una carga de 10 terminales para un uso normal de software de ofimática y navegación por Internet:

- Procesador tipo Intel Core i5 o AMD equivalente.
- Memoria RAM 8GB
- Dos tarjetas de red Gigabyte.
- No es necesario tarjeta gráfica específica, basta con la integrada en el equipo.
- Discos duros: Depende de las necesidades. Las maquetas de educación elaboradas por la Consejería llevan arranque dual(Windows y MAX) mas el sistema de restauración local(SRP) por lo que se requiere un mínimo de espacio de 300GB aproximadamente.




## 5. Configuraciones de red

Si la red depende de Madrid Digital, habrá que pedir que las tomas de red estén en la VLAN correspondiente. En los IIT sólo hace falta solicitar una toma en la VLAN110 para enlazar el switch principal del aula.

En el switch principal se configura una VLAN para partir sus puertos de manera que unos quedan asignados a la VLAN110 y otros en la VLAN111. La siguiente imagen muestra un parcheo típico de los switches del aula:

VLAN 110

POR DEFECTO



SWITCH 1

1	3	5	7	9	11	13	15	17	19	21	23	bocas switch
MIES	3	7	LIBRE	2	6	10	12	14	16	18	20	bocas del Patch-panel
1	5	8	LIBRE	4	9	11	13	15	17	19	INTER	bocas switch
2	4	6	8	10	12	14	16	18	20	22	24	bocas switch

SWITCH 2

1	3	5	7	9	11	13	15	17	19	21	23	bocas switch
21	23	25	27	29	31	33	35	37	LIBRE	LIBRE	LIBRE	bocas del Patch-panel
22	24	26	28	30	32	34	36	38	LIBRE	LIBRE	INTER	bocas switch
2	4	6	8	10	12	14	16	18	20	22	24	bocas switch

PANEL 1

1	ISLA1
2	ISLA1
3	ISLA2
4	ISLA2
5	ISLA3
6	ISLA3
7	PROFESOR
8	LIBRE
9	ALUMNO 1
10	ALUMNO2
11	ALUMNO3
12	ALUMNO4
13	ALUMNO5

PANEL 2

25	ALUMNO17
26	ALUMNO18
27	ALUMNO19
28	ALUMNO20
29	ALUMNO21
30	ALUMNO22
31	ALUMNO23
32	ALUMNO24
33	ALUMNO25
34	ALUMNO26
35	ALUMNO27
36	ALUMNO28
37	ALUMNO29

Imagen 4: Conexión de los switches de un aula

El puerto 1 del switch se utiliza para el enlace con la VLAN110 que en la imagen se muestra como MIES. Cada equipo de ISLA necesita dos tomas, una toma en la VLAN110 y otra en la VLAN111 para la comunicación con los terminales, por ello se observa cómo en el listado cada equipo de ISLA aparece duplicado. Los equipos de profesor sólo tienen una interfaz que trabajará en la VLAN110. De la imagen anterior se deducen las rosetas de pared que corresponden a los equipos:

isla1 = D01(VLAN110) = puerto del switch 2, D02(Red NComputing) = Puerto del switch 9 isla2 = D03(VLAN110) = puerto del switch 3, D04(Red NComputing) = Puerto del switch 10 isla3 = D05(VLAN110) = puerto del switch 4, D06(Red NComputing) = Puerto del switch 11 profesor= D07(VLAN110) = puerto del switch 5

El switch 2 esta plano(sin ninguna vlan adicional a la default) y simplemente se conectan los dos switches por sus puertos 24 que en la imagen se identifican como INTER. La función del switch 2 es simplemente aumentar el número de bocas para poder conectar todos los terminales. Es conveniente que los switches estén etiquetados para saber cual es el principal y cual el secundario:



*Imagen 5: Switch secundario de un aula*

Uno de los trabajos es asignar las direcciones IP de los dispositivos que componen en aula, para ello hay que tener claro cuales son estos dispositivos. Tenemos:

- El switch principal del aula.
- Tres equipos de ISLA.
- Equipo de profesor.
- Impresora de red(opcional)

El switch principal por tanto necesitará una dirección IP para su administración, sin embargo el secundario, aunque también fuera gestionable no es necesario reservar IP ya que como es sólo una extensión del principal dentro de la VLAN111, este switch al igual que los terminales queda aislado y sólo es accesible desde la propia red de terminales dentro del aula.

Como los equipos de ISLA tienen dos tarjetas de red hay que decidir cual se va a conectar a cada VLAN. En los IIT se sigue la norma de manera que la tarjeta que está mas arriba del equipo y que suele coincidir con la tarjeta integrada de la placa base, es la que se conecta a la VLAN110 y la tarjeta que está mas abajo es la que se conecta a la red de los NComputing.

Para los terminales se ha utilizado la red 192.168.11.0/24. Como esta red esta completamente aislada, la configuración IP del adaptador correspondiente en cada ISLA puede ser **la misma en todas las aulas**, siendo en los IIT la siguiente:

islaX1 = 192.168.11.1  
islaX2 = 192.168.11.2  
islaX3 = 192.168.11.3

Como las IPs 1, 2 y 3 ya están reservadas para las ISLAS, a los terminales se les asigna una IP a partir de la 101 para que exista cierta relación entre su número de orden y su IP.:





192.168.11.101 = terminal1  
192.168.11.102 = terminal2  
192.168.11.103 = terminal3  
...  
192.168.11.129 = terminal29  
192.168.11.130 = terminal30

Una vez que tenemos clara la configuración de IPs sólo falta configurar los dispositivos. A modo de ejemplo a continuación se muestra cómo quedaría esta configuración en Windows y MAX. Por último que daría configurar las IPs en los terminales, esta configuración se muestra en el apartado siguiente donde se explica la configuración completa del terminal.

#### a) Configurar la red en Windows

1. Configurar los adaptadores de red. Hacemos *clic* en el icono de red del área de notificación y vamos al “**Centro de redes y recursos compartidos**”, o acceder a él desde el panel de control:



2. En el “**Centro de redes y recursos compartidos**” en el menú de la izquierda entramos en “Cambiar configuración del adaptador” donde veremos la lista de adaptadores de red. Para averiguar el adaptador correspondiente a cada red no nos guiaremos por el nombre que Windows muestra “Conexión de área local...” si no que pondremos esta vista en modo detallado para visualizar el “Nombre del dispositivo” hardware de cada adaptador:

Conexiones de red				
Panel de control > Redes e Internet > Conexiones de red				
Organizar				
Nombre	Estado	Nombre del dispositivo	Conectividad	Categoría de red
Conexión de área local	Red 3	Intel(R) 82579LM Gigabit Network Connection #2	Acceso a Internet	Red pública
Conexión de área local 2	Red no identificada	Intel(R) Gigabit CT2 Desktop Adapter	Sin acceso a Internet	Red pública
OpenVPN	Cable de red desconectado	TAP-Win32 Adapter V9		

3. El adaptador correspondiente al modelo “**Intel(R) 82579LM Gigabit**” es el de la VLAN110. Configuramos tal como se muestra en la siguiente imagen, cambiando su IP por la correspondiente, este sería un resumen de los datos:

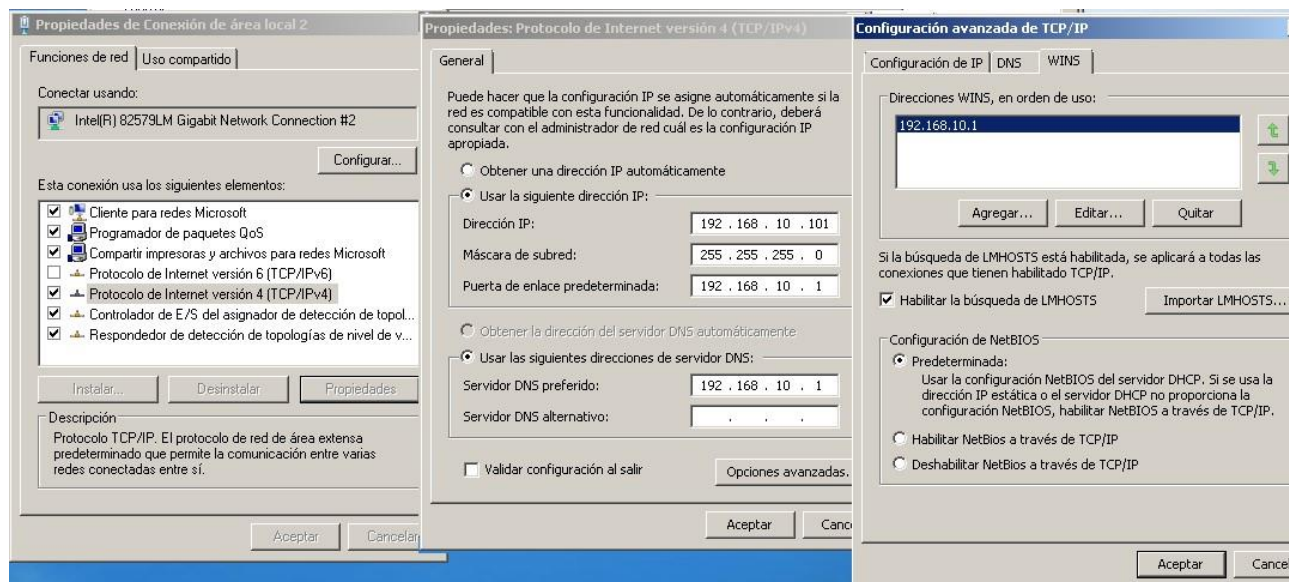




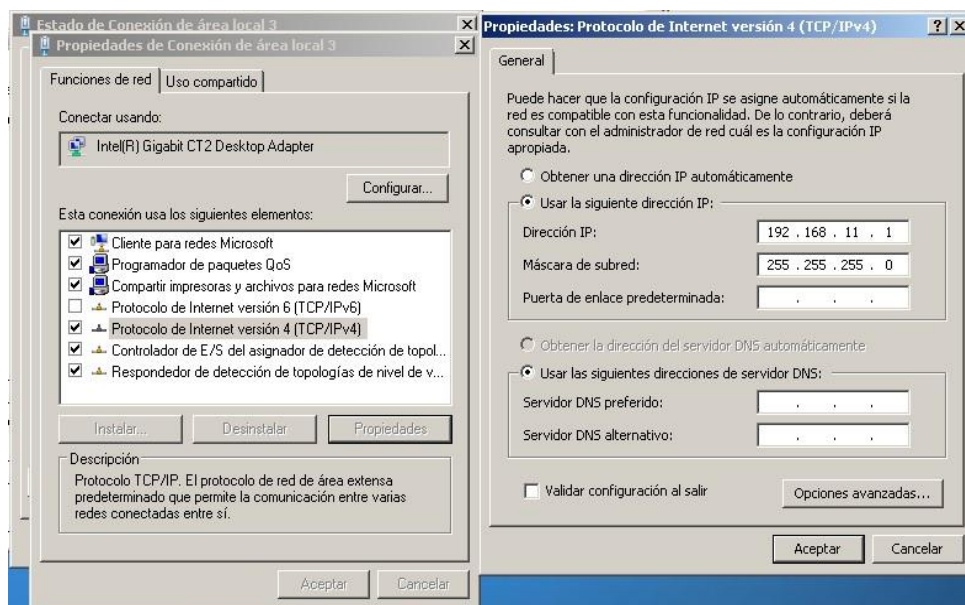
## Desactivar protocolo IPv6

Dirección IP : 172.20.10.XY  
Máscara de red : 255.255.240.0

Puerta de enlace, servidor DNS y servidor WINS: 172.20.10.1



- El adaptador modelo “**Intel(R) Gigabit CT2 Desktop Adapter**” corresponde a la red de los terminales NComputing, lo configuramos con la IP correspondiente. Este adaptador no lleva ni puerta de enlace ni servidor DNS:



Importante: En ambos adaptadores se ha desactivado el protocolo IPv6.



b) Configurar la red en MAX

Adaptador de red para la VLAN110.

Este adaptador tendrá

IPs del tipo:

profesorX0 = 172.20.10.X0

islaX1 = 172.20.10.X1

islaX2 = 172.20.10.X2

islaX3 = 172.20.10.X3

Nombre de la conexión: VLAN110

☒ Conectar automáticamente

Cableada Seguridad 802.1x Ajustes de IPv4 Ajustes de IPv6

Método: Manual

**Dirección**

Dirección	Máscara de red	Puerta de enlace
192.168.10.101	255.255.255.0	192.168.10.1

+ Añadir  
Eliminar

Servidores DNS: 192.168.10.1

Dominios de búsqueda: madrid

ID del cliente DHCP:

☐ Requiere dirección IPv4 para que esta conexión se complete

Rutas...

☒ Disponible para todos los usuarios Cancelar Guardar...

Adaptador de red para la VLAN111.

Este adaptador tendrá las  
siguientes IPs:

islaX1 = 192.168.11.1

islaX2 = 192.168.11.2

islaX3 = 192.168.11.3

Nombre de la conexión: NComputing

☒ Conectar automáticamente

Cableada Seguridad 802.1x Ajustes de IPv4 Ajustes de IPv6

Método: Manual

**Dirección**

Dirección	Máscara de red	Puerta de enlace
192.168.11.1	255.255.255.0	0.0.0.0

+ Añadir  
Eliminar

Servidores DNS:

Dominios de búsqueda:

ID del cliente DHCP:

☐ Requiere dirección IPv4 para que esta conexión se complete

Rutas...

☒ Disponible para todos los usuarios Cancelar Guardar...

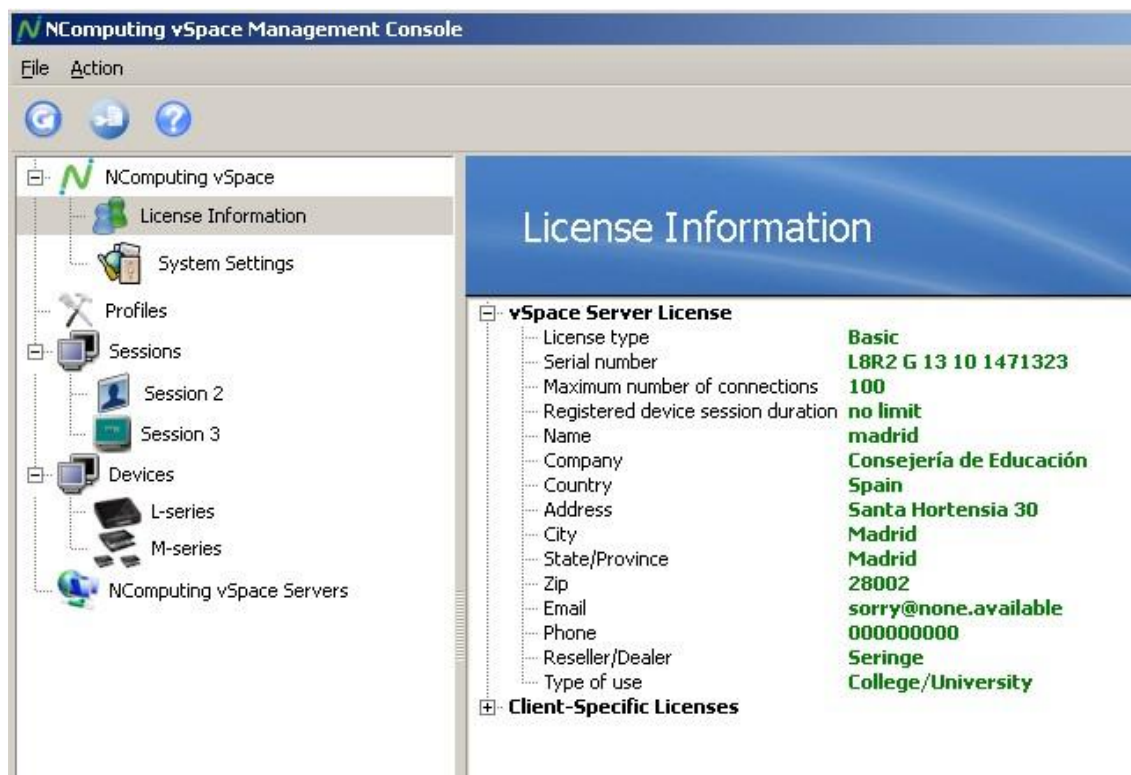


## 6. Configuración de Vspace (software de Ncomputing)

**IMPORTANTE:** Con algunos drivers de tarjetas gráficas el software de NComputing no es estable por lo que no se recomienda actualizar el driver de la gráfica a la ligera incluso en algunos casos es necesario no instalar dicho driver para que el software de Ncomputing funcione adecuadamente.

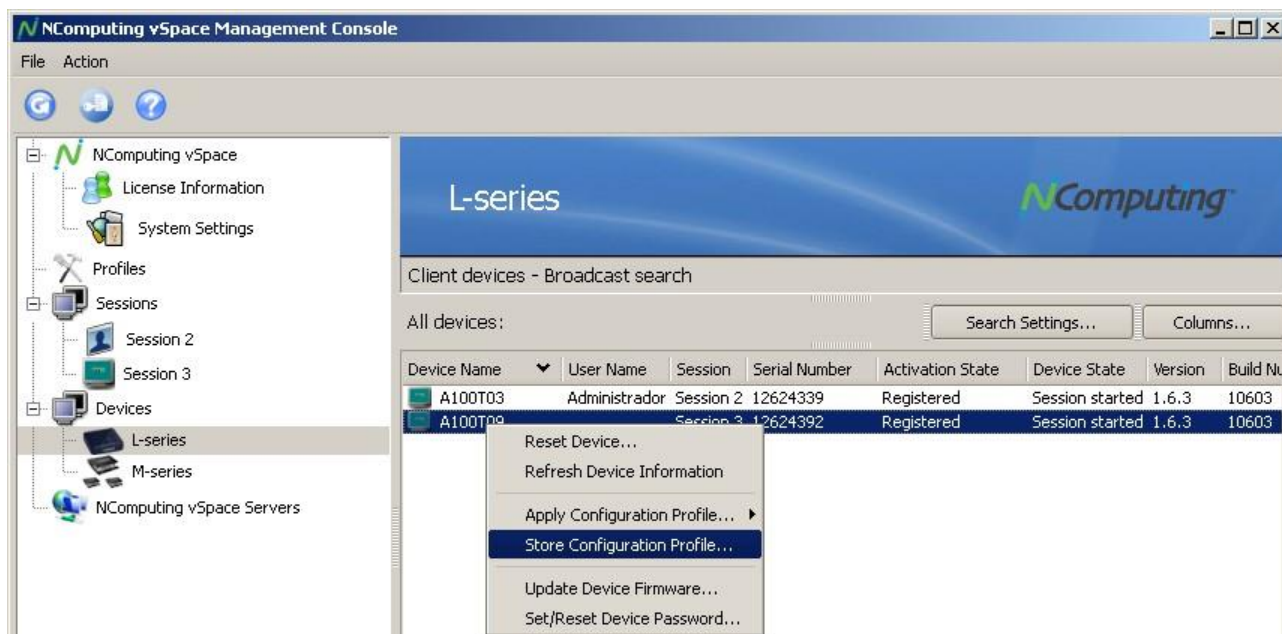
VSpace es el software de NComputing con el que se controlan los terminales. Abriremos la consola de administración ejecutando el icono llamado “NC-Console” en un equipo de ISLA:

1. Lo primero que hay que comprobar es que el software se ha conseguido registrar. El proceso de registro se hace de forma transparente, se intenta en cada inicio del equipo y luego en intervalos de una hora. Si el software está registrado veremos una pantalla como la siguiente en la sección “License Information”:



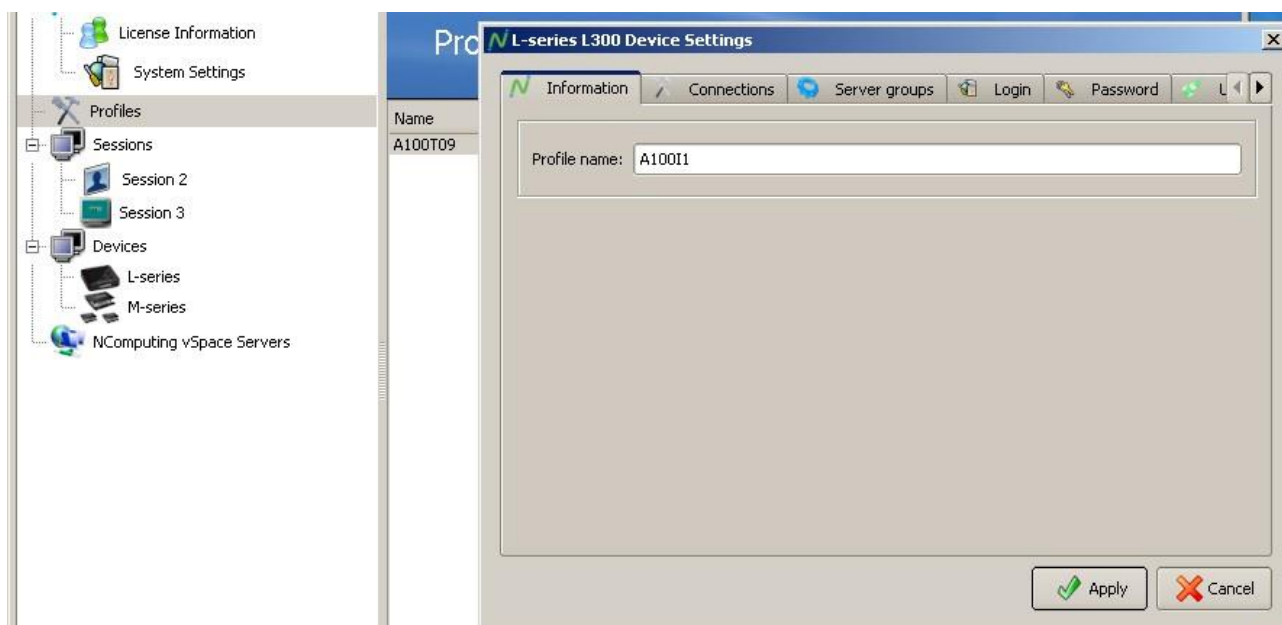
2. Lo siguiente es crear perfiles de configuración de terminales(uno por cada isla del aula), para ello vamos a la sección “Devices > L-series” donde aparecerán los 30 terminales del aula:





Hay que seleccionar un terminal correspondiente a la “islaX1”, hacer clic derecho sobre él y seleccionar “Store Configuration Profile...”. Repetiremos el mismo paso con un terminal que pertenezca a la islaX2 y a la islaX3. Hay que tener en cuenta que este paso sólo se puede hacer cuando haya al menos un terminal de cada isla completamente configurado.

- Una vez almacenados los perfiles de los tres terminales, los podemos encontrar en la sección “Profiles”(en la imagen de ejemplo sólo aparece el A10T09 correspondiente a la islaX1 pero ahí deberán aparecer también los otros dos perfiles creados):





Ahora simplemente renombramos el nombre del perfil para que haga referencia a la isla correspondiente, para ello hacemos doble clic sobre el nombre del perfil y en la primera ficha cambiamos el “Profile name” según la siguiente relación:

AXI1 para el perfil perteneciente a un terminal de la islaX1

AXI2 para el perfil perteneciente a un terminal de la islaX2

AXI3 para el perfil perteneciente a un terminal de la islaX3

... donde la X corresponde al número ordinal del aula que se está montando.

Esta configuración hay que realizarla en los tres equipos de isla, es decir, los tres equipos tendrán una copia de los tres perfiles de configuración.

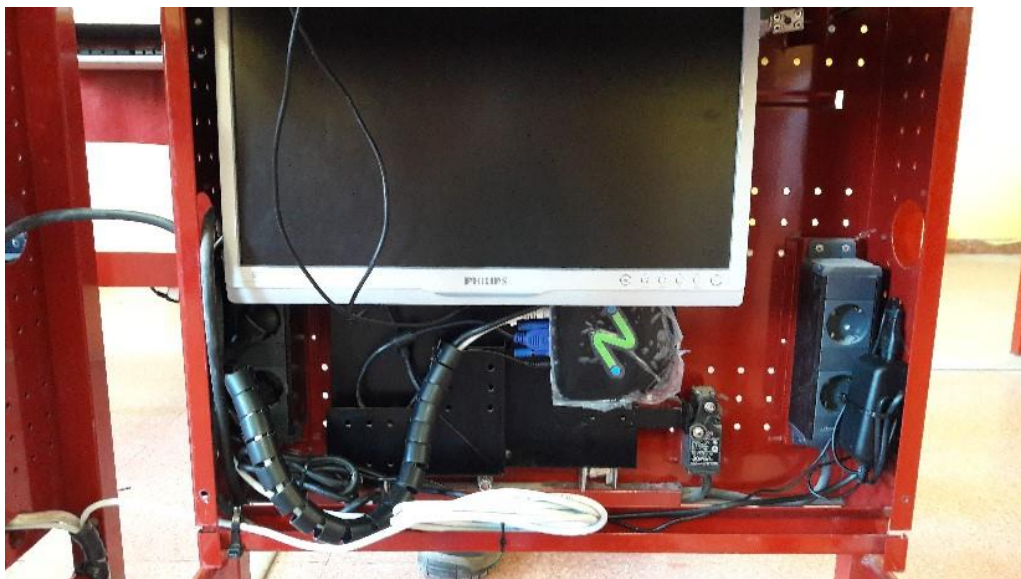
## **7. Instalación de los terminales**

Los terminales vienen con un soporte de plástico preparado para ser instalado en la parte trasera de los monitores que vengán preparados para ser instalados en soportes VESA 75 o VESA100(75 o 100 mm de distancia entre agujeros para los tornillos):



En caso de los IIT se utiliza un mobiliario especial y el monitor ya usa su anclaje VESA para acoplarse a la mesa del alumno por lo que los terminales se instalan en algún hueco de la mesa. Su ubicación varía según el modelo de mesa.





## 8. Configuración de los terminales

Al encender el terminal, este tarda unos 30 segundos en inicializarse, mostrando finalmente la siguiente pantalla:



Pulsaremos el botón “Device setup” he iremos a la ficha “Managed Groups”:





Eliminamos cualquier grupo que exista con el botón “Remove” y añadimos un grupo nuevo con el botón “Create New Group”. Haciendo clic sobre el nuevo grupo podemos renombrarlo, poniendo como nombre la letra “A” y el número del aula, por ejemplo “A07”, “A11”, etc. En el grupo creado añadimos la IP de un servidor pulsando el botón “New

Host/IP”. Como IP ponemos 192.168.11.1(islaX1), 192.168.11.2(islaX2) o 192.168.11.3(islaX3) según corresponda sabiendo que los terminales 1 a 10 se asocian a la islaX1, los terminales 11 a 20 a la islaX2, y los terminales 21 a 30 a la islaX3. Hay algunos casos excepcionales de que el aula tiene más de treinta terminales, por ejemplo 33 o 35. En estos casos repartiremos de manera equitativa estos terminales extras, por ejemplo:

Si tiene 33: Terminal 31 = islaX1, 32 = islaX2, 33 = islaX3 Si tiene

34: Terminal 31 y 32 = islaX1, 33 = islaX2, 34 = islaX3

Si tiene 35: Terminal 31 y 32 = islaX1, 33 y 34 = islaX2, 35 = islaX3

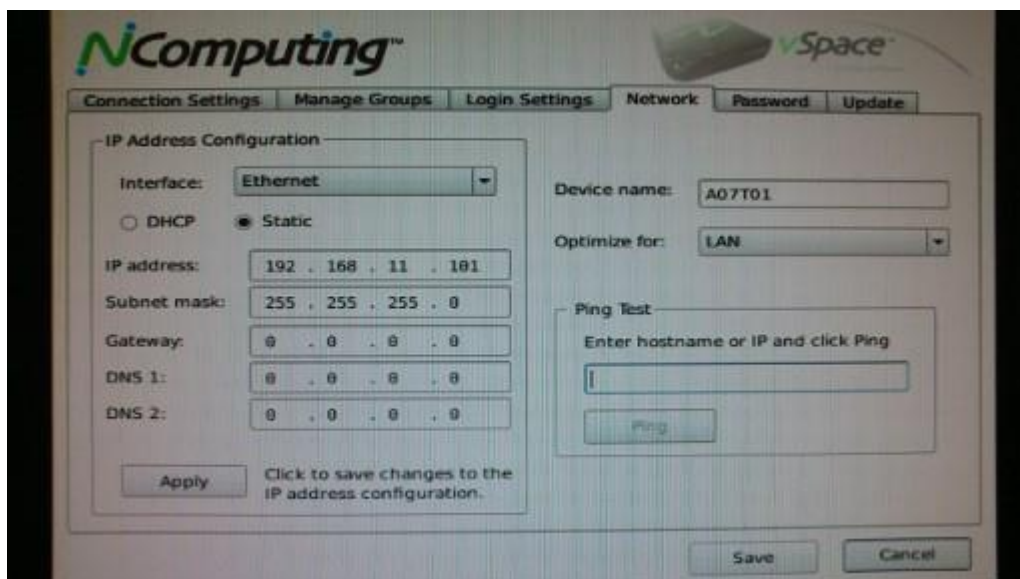
Pasamos a la siguiente pantalla “Login Settings” y configuramos la resolución de pantalla con la nativa en la que trabajan los monitores en este caso 1600x900. El resto de configuraciones las dejamos como se muestra en la figura:







Pasamos a la ficha "Network", seleccionamos interfaz "Ethernet" y modo "static". Configuramos la IP del tipo 192.168.11.X teniendo en cuenta que la IP de los terminales se empiezan a numerar en el 101. En "Device name" ponemos primero el grupo del aula tal como lo hemos creado en "Managed Group", por ejemplo "A07" seguido de la letra "T" y el número de orden del terminal. Por ejemplo en el aula siete las etiquetas serían: A07T01, A07T02, A07T03, ..., A07T29 y A07T30.



En esta pantalla pulsamos ahora el botón "Apply" lo que hará que el terminal se reinicie, cuando aparezca el menú principal del terminal pulsamos el botón "Device setup" para volver a entrar en la configuración.

Vamos la ficha "Connection Settings", marcamos "Autoconnect to:" y seleccionamos el grupo que habíamos creado en la ficha "Manage Groups":



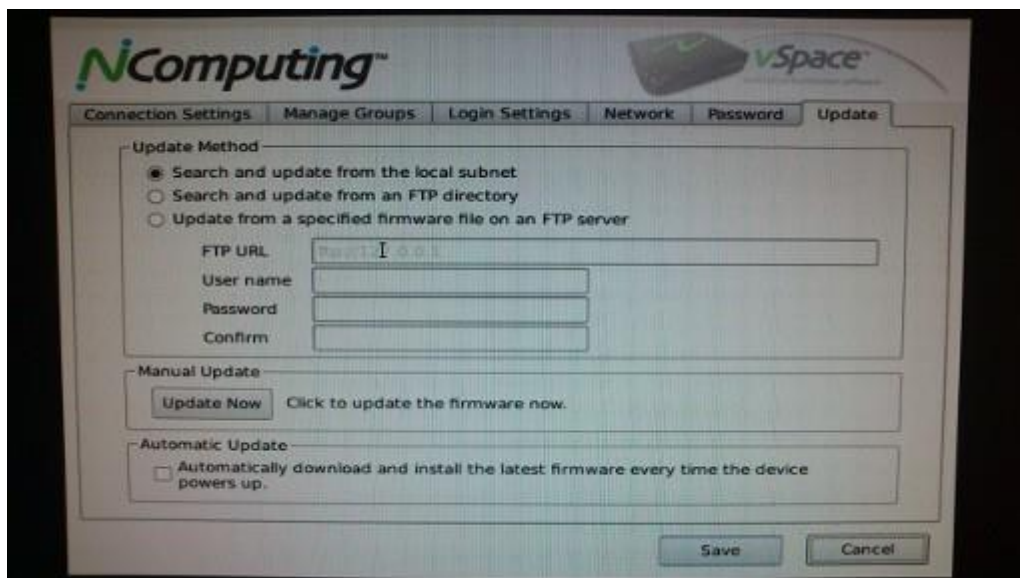


Vamos a la ficha “Password”, marcamos “Require password...” y configuramos la contraseña:



Por último vamos a la ficha “Update” y comprobamos que está configurada tal como muestra la imagen:





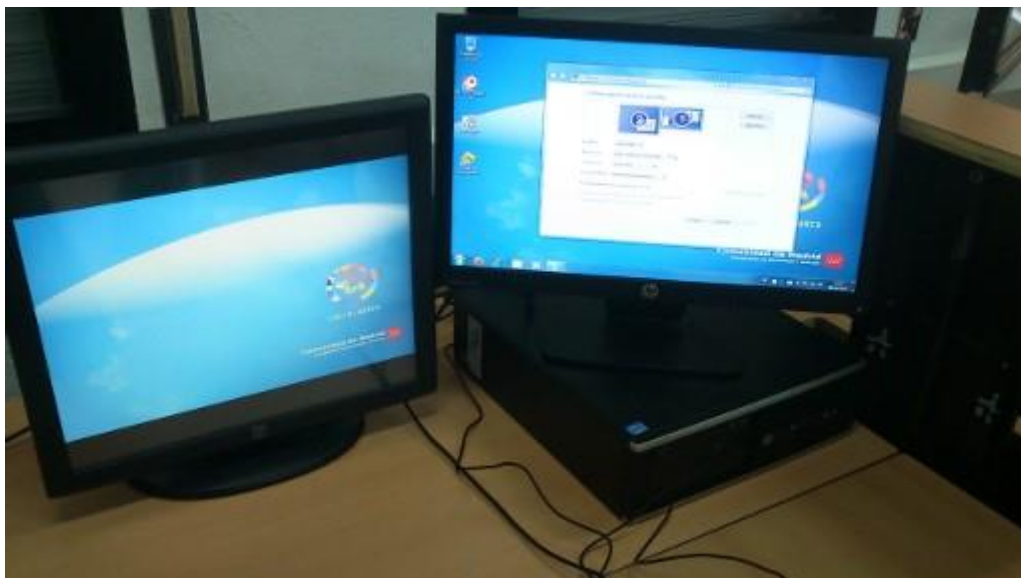
Pulsamos el botón “Save” para grabar los últimos cambios realizados y el terminal se reiniciará. Ahora hay que tener en cuenta que el terminal ha quedado configurado para realizar la autoconexión a una isla concreta por lo que el menú inicial del terminal ya no aparece. La configuración del terminal está terminada pero si fuera necesario volver a entrar en la configuración del terminal hay que pulsar la tecla ESC repetidamente hasta que se cancele la autoconexión de manera que vuelve a salir la pantalla inicial del terminal.

En caso de problemas, en la pantalla inicial del terminal existe el botón “Device information” el cual nos muestra información que nos puede ayudar a detectar el problema:



## 9. Configuración para el puesto del profesor

Describimos aquí la configuración de un puesto de profesor con dos pantallas, una de ellas táctil y conexión a una pizarra digital interactiva. Según quede la disposición de la mesa del profesor, a derechas o a izquierdas, colocaremos los monitores como se muestra en las siguientes imagenes:



*Ilustración 1: Mesa en el lado izquierdo del aula*



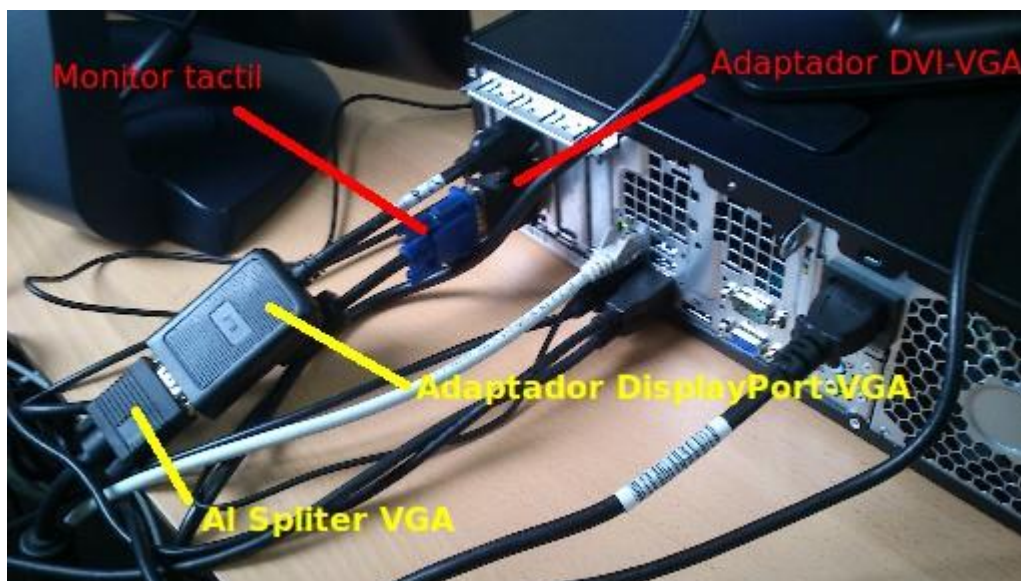
*Ilustración 2: Mesa en el lado derecho del aula*

Como se observa, el puesto del profesor lleva conectados dos monitores, uno de ellos es táctil, además también se conecta el proyector de la pizarra mediante un splitter de vídeo VGA. La imagen del monitor que no es táctil (el monitor que está encima del equipo) es el que se proyecta en la pizarra utilizando el splitter. El monitor táctil se conecta directamente a la salida DVI del equipo, pero como su entrada es también VGA se necesita intercalar un conversor DVI-VGA en la salida de la gráfica.

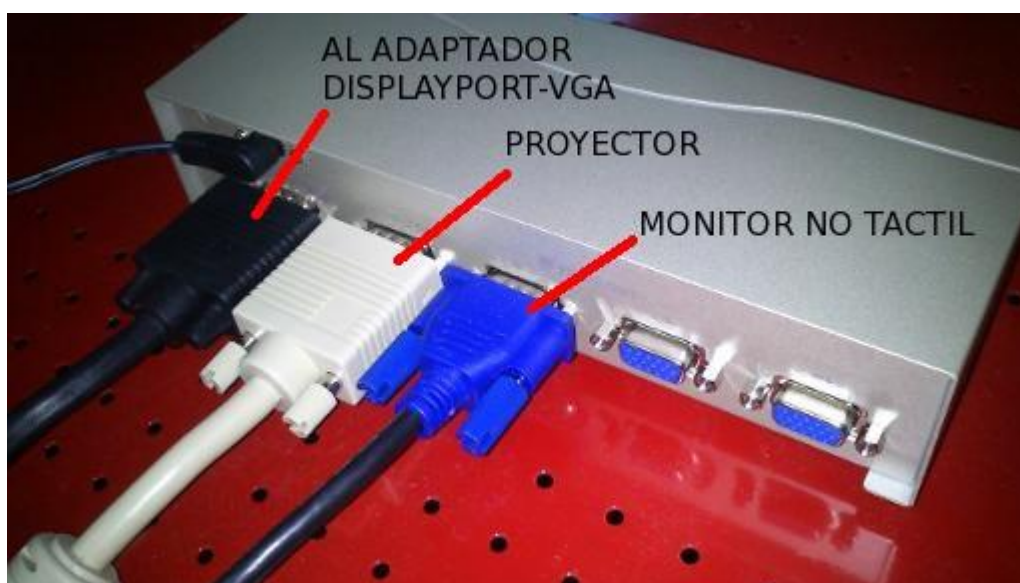




En la siguiente imagen se observa donde va conectado cada elemento:

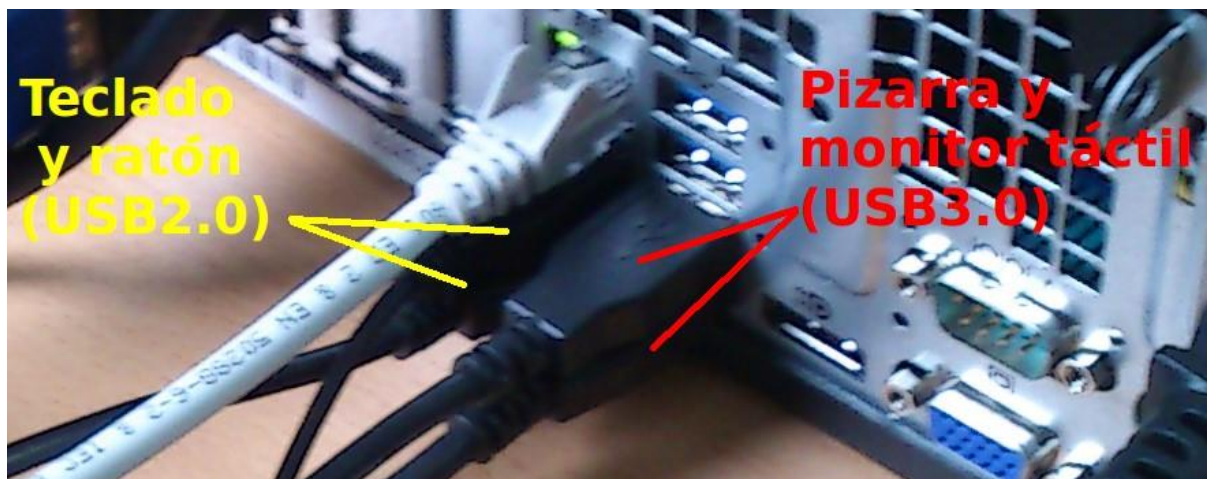


En el splitter es importante el orden de conexión de las salidas de vídeo para que el equipo reconozca correctamente las resoluciones, de manera que el proyector va conectado en la primera salida de vídeo y el monitor HP (el que no es táctil) se conecta en la segunda salida):



En la parte trasera el equipo tiene dos puertos USB 2.0 donde se conectará el teclado y el ratón. Los otros cuatro conectores son USB3.0 donde se conectará la pizarra y el monitor táctil. El cable USB del monitor viene con el propio monitor, mientras que el cable USB para la pizarra así como el cable VGA para la conexión del proyector, viene con la instalación de la pizarra y deberá suministrarlo el centro.





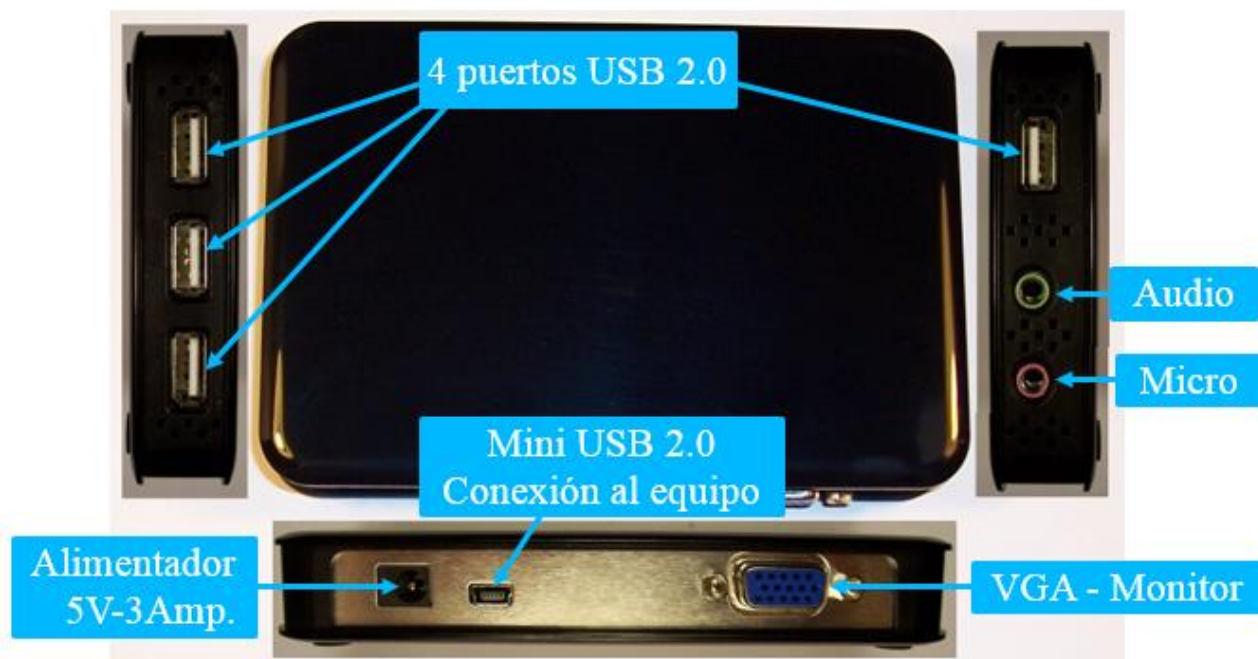
Además de configurar la IP, nombre de equipo y meterlo en el dominio, en el profesor se realizan las siguientes configuraciones:

1. Configurar disposición de monitores y resolución:  
La resolución del monitor HP(formato 16:9) debe ser 1280x800.  
La resolución del monitor táctil debe ser 1280x1024.  
Según quede el monitor táctil a la derecha o izquierda se debe configurar para que el ratón pase de un monitor a otro por el lado correcto(debido a problemas con el driver de vídeo no se puede realizar esta configuración en MAX).
2. Calibrar pizarra. Tan sólo se realizará un calibrado de la pizarra para comprobar que la conexión es correcta. El ajuste de la imagen será realizado posteriormente por la empresa instaladora de la pizarra(PRODEL).
3. Calibrar pantalla táctil: Mediante el icono "ELO" que aparece en el área de notificación, se realizará la calibración del monitor táctil para comprobar su funcionamiento (Debido a que el driver del monitor táctil no funciona correctamente con doble monitor, no se puede realizar esta configuración en MAX).
4. Configurar ABTutor. Para la configuración del ABTutor es necesario tener configurados las tres islas y todos los terminales.



## B. PUESTOS CON TERMINALES USB (MULTIPOINT)

### 1. Hardware Multipoint, conexiones del MWS300



VGA Resolutions Supported		Platform	VGA Resolutions Supported		Platform
1600 x 1200	16 / 32 Bit	PC	1280 x 800	16 / 32 Bit	PC
1680 x 1050	16 / 32 Bit	PC	1280 x 768	16 / 32 Bit	PC
1600 x 900	16 / 32 Bit	PC	1280 x 720	16 / 32 Bit	PC
1400 x 1050	16 / 32 Bit	PC	1152 x 864	16 / 32 Bit	PC
1440 x 900	16 / 32 Bit	PC	1024 x 768	16 / 32 Bit	PC
1360 x 768	16 / 32 Bit	PC	800 x 600	16 / 32 Bit	PC
1280 x 1024	16 / 32 Bit	PC	640 x 480	16 / 32 Bit	PC
1280 x 960	16 / 32 Bit	PC			





## 2. Conexión de una isla Multipoint

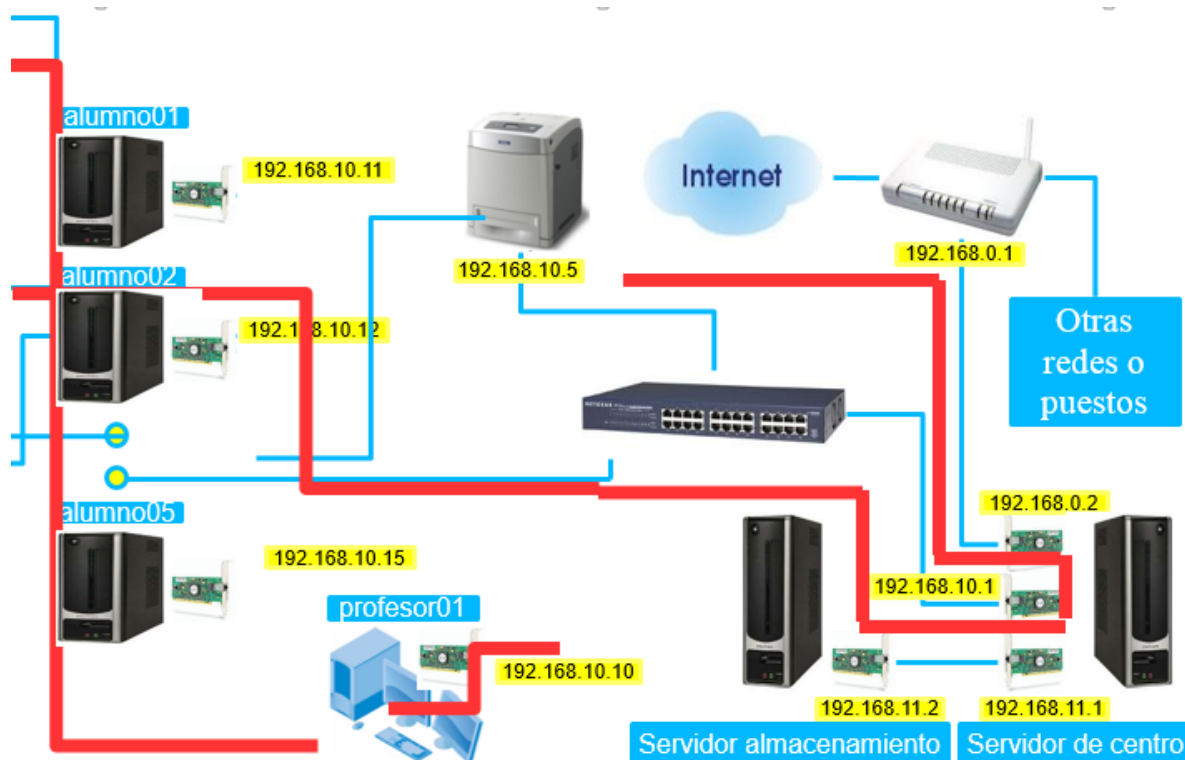


Ratón, teclado y monitor conectados directamente al PC se utilizan solo para la fase de configuración.

Luego no son necesarios.



a) Conexionado de la red



b) Montaje de equipos Multipoint Aislados

- Biblioteca
- Sala profesores
- Puestos de consultas
- etc...



Pueden estar de manera independiente, no es obligatorio que estén unidos al dominio ni a la red multipoint.

c) Requisitos para montar un sistema Multipoint

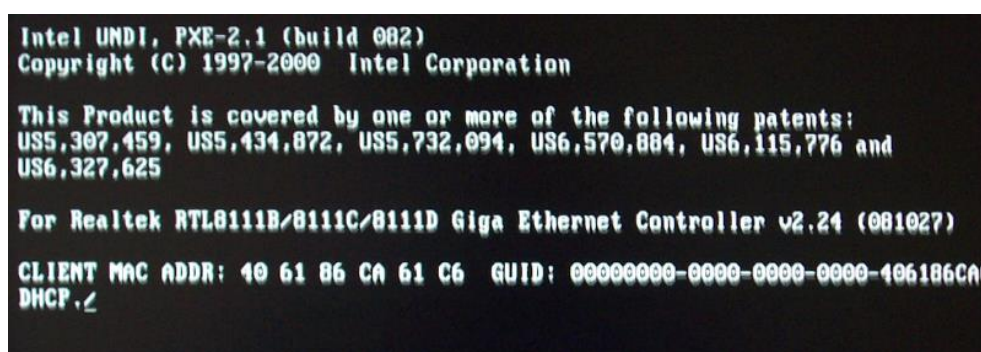
- Software, 2 opciones:
  - Microsoft Windows Multipoint Server 2011



- Coste: Tantas CAL's como terminales + propio S.O.
  - MAX 6.0 o 6.5
  - Coste: 0 euros.
- Hardware:
  - CPU mínimo un Core Quad(4 nucleos)
  - Mínimo 4GB de RAM
  - Gráfica compatible con el driver multipoint(sólo Windows)

### 3. Proceso de arranque de un equipo

- Arranque por red:

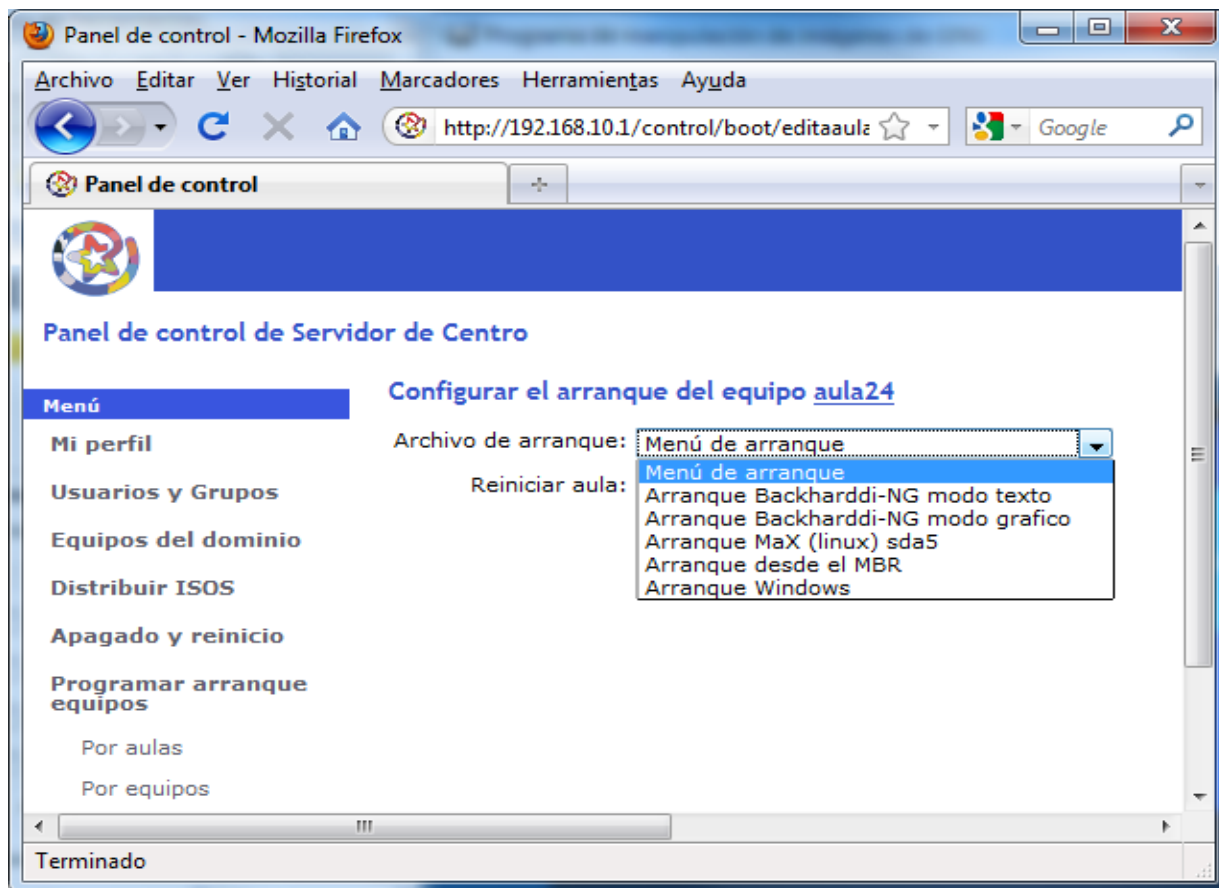


- Menú suministrado por el servidor:

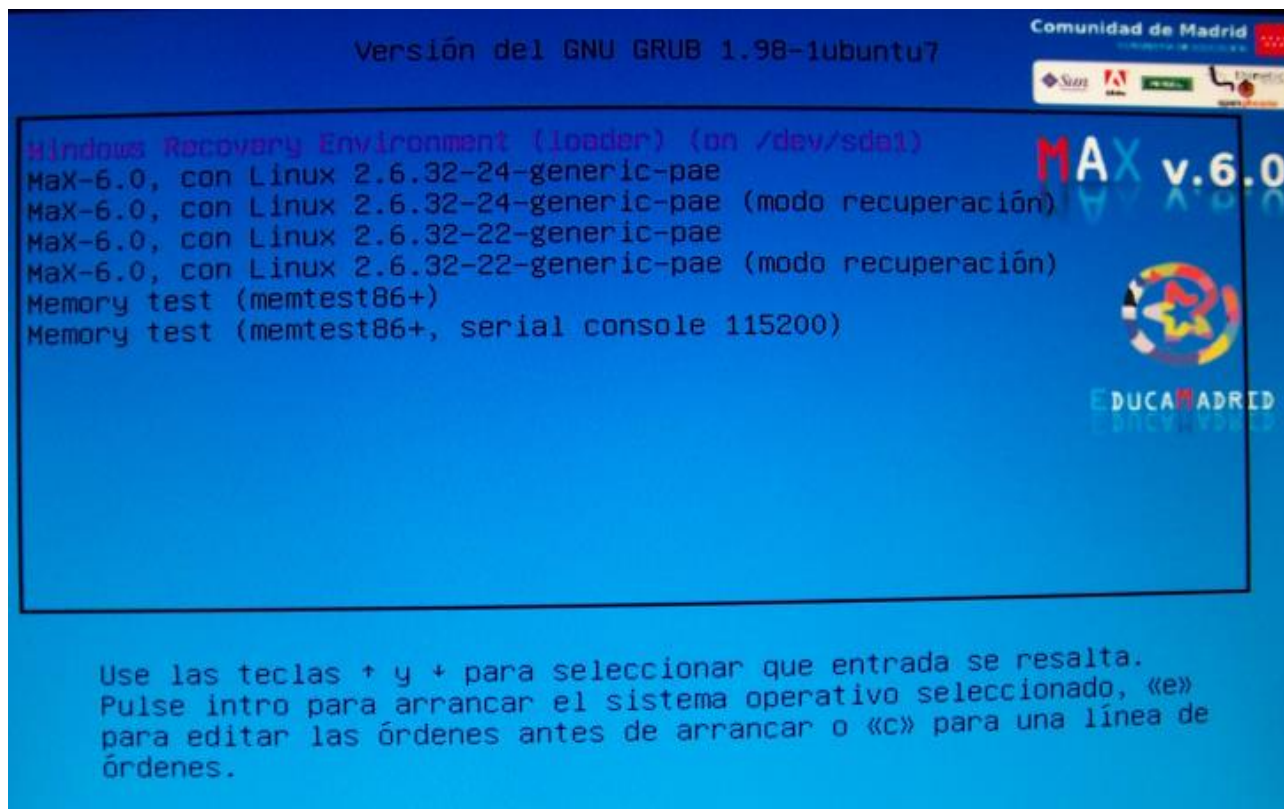


Corresponde a la opción “Menú de arranque” (default)

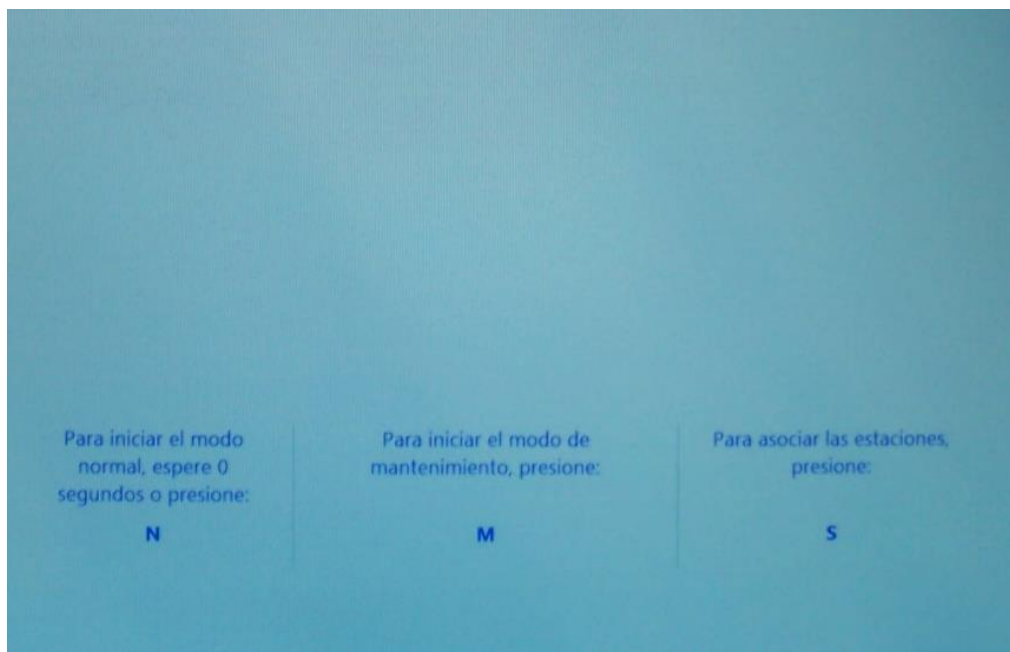




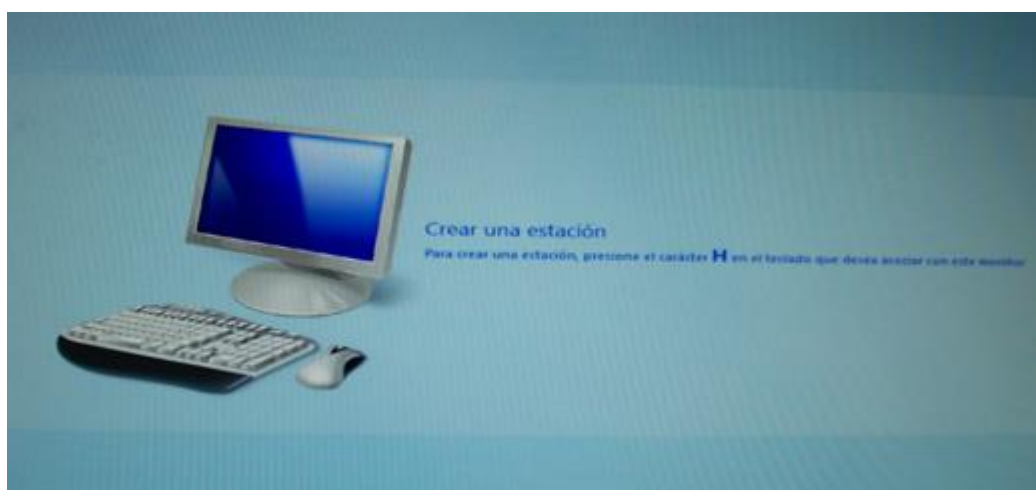
- Menu de grub, arranca Windows por defecto:







- Modo mantenimiento:
  - Instalaciones criticas(driver multipoint, gráfica)
  - Después de unir al dominio (multipoint desactivados)
  - Forzará la entrada en este modo si es necesario.
- Modo normal:
  - Entra automáticamente en 10seg si no se pulsa nada
- Pantalla final del servidor multipoint:



No se debe abrir otra sesión.

Excedemos el número de sesiones(licencias)



#### 4. Perfiles de usuario

##### a) ¿Que es el perfil del usuario?

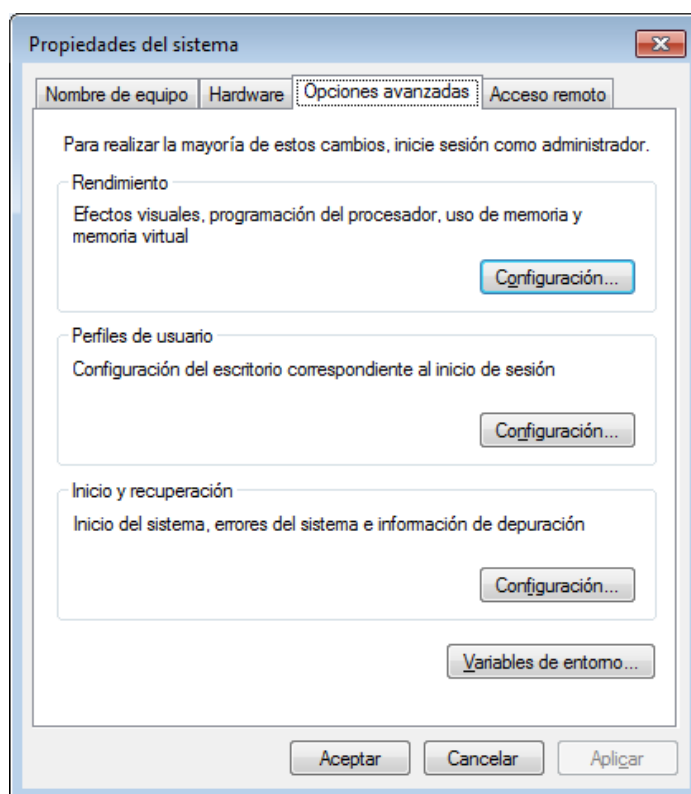
- o Carpeta donde se guardan sus datos y configuraciones
  - o Datos = Carpetas de trabajo: Escritorio, Mis documentos, etc..
  - o Configuraciones: Preferencias de programas, apariencia, etc...
- o C:\Document and setting (XP) C:\User (Win7/2008/2010)

##### b) ¿Que significa que sea móvil?

- o Desde cualquier equipo estarán disponible mis carpetas de trabajo(Escritorio, Mis documentos, etc...) y mis configuraciones
- o Los perfiles móviles necesitan sincronización
- o Para mejorar la sincronización: perfil móvil partido en dos:
  - o Carpetas de trabajo: escritura directa en el servidor.
  - o Configuraciones: Se sincronizan al cerrar la sesión

##### c) Borrado de perfil en Windows

- o Al ser móvil es seguro borrar el perfil del servidor multipoint
- o En otros sistemas o perfiles fijos: NO BORRAR!!!
- o ¿Como?:
  - Ficha opciones avanzadas > Perfiles de usuario



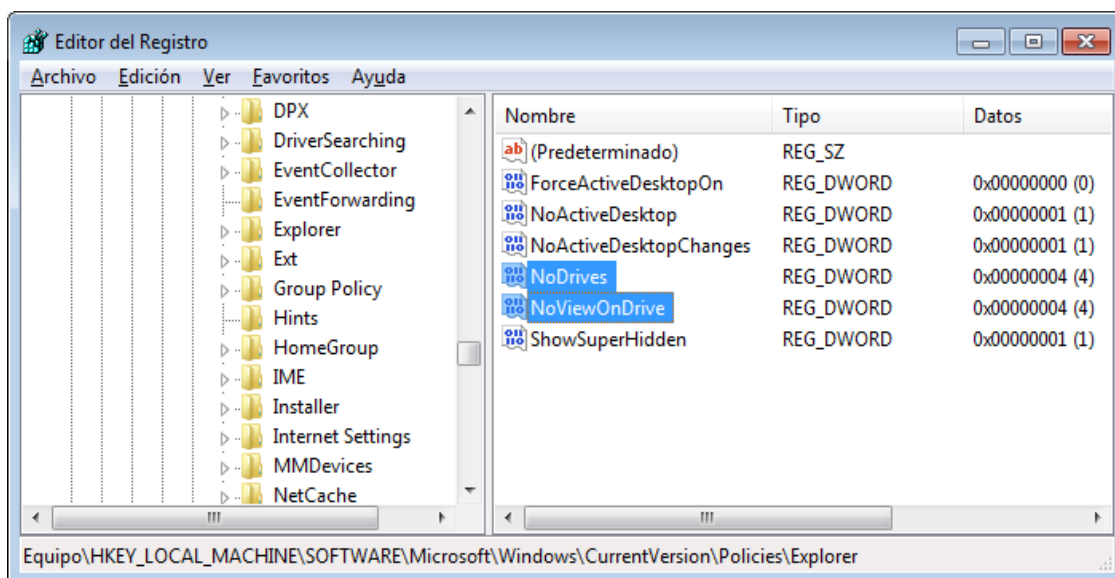
## 5. Políticas o directivas de grupo

### a) ¿Qué son las políticas de grupo?

- Son configuraciones avanzadas para cambiar el comportamiento por defecto de Windows
- Normalmente son del tipo restricciones
- Editor de políticas: gpedit.msc
- Escritura directa en el registro de windows.

Ejemplo:

- Ocultar la unidad C:





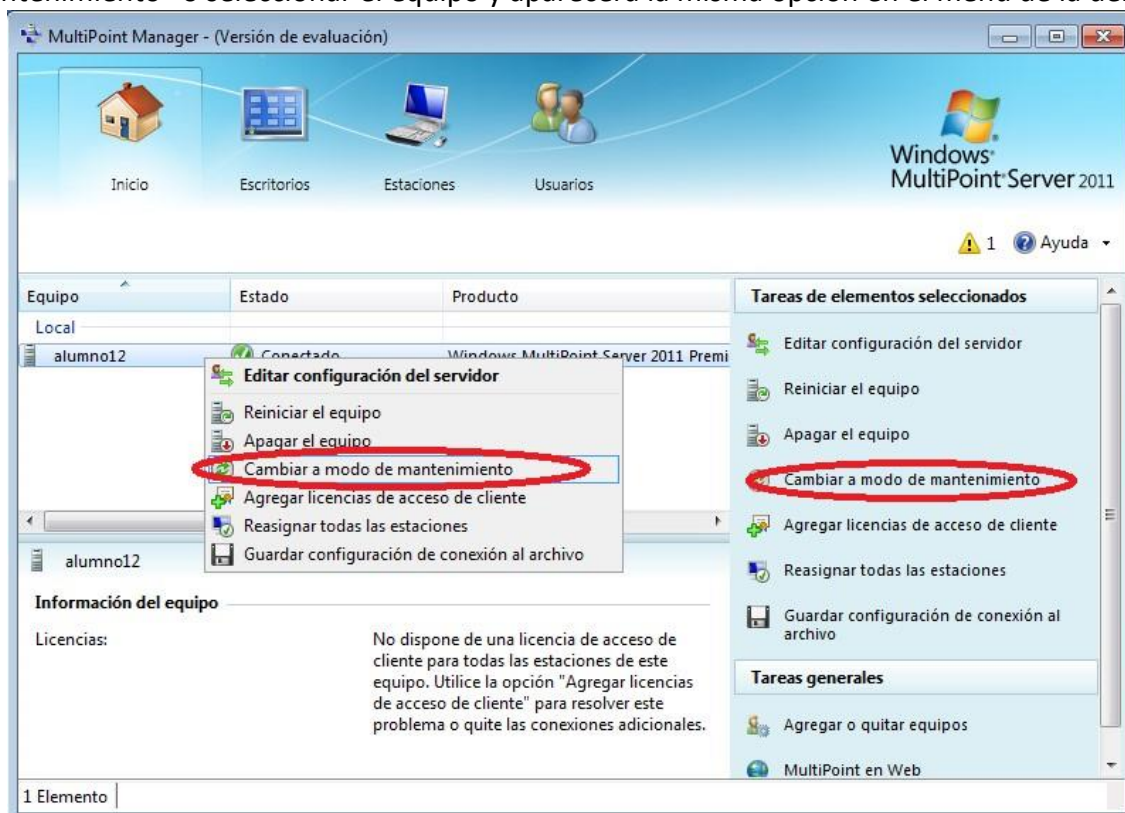
## C. PROCEDIMIENTO DE ACTUALIZACION DEL DRIVER MCT

- La versión del driver probada es “MWS-11.05.0503.0177\_WoOIP”.
- En todo el proceso siempre se utiliza la cuenta “Administrador” local del equipo. - Aunque el driver pide desconectar los USB de los terminales, no es necesario.

### Procedimiento:

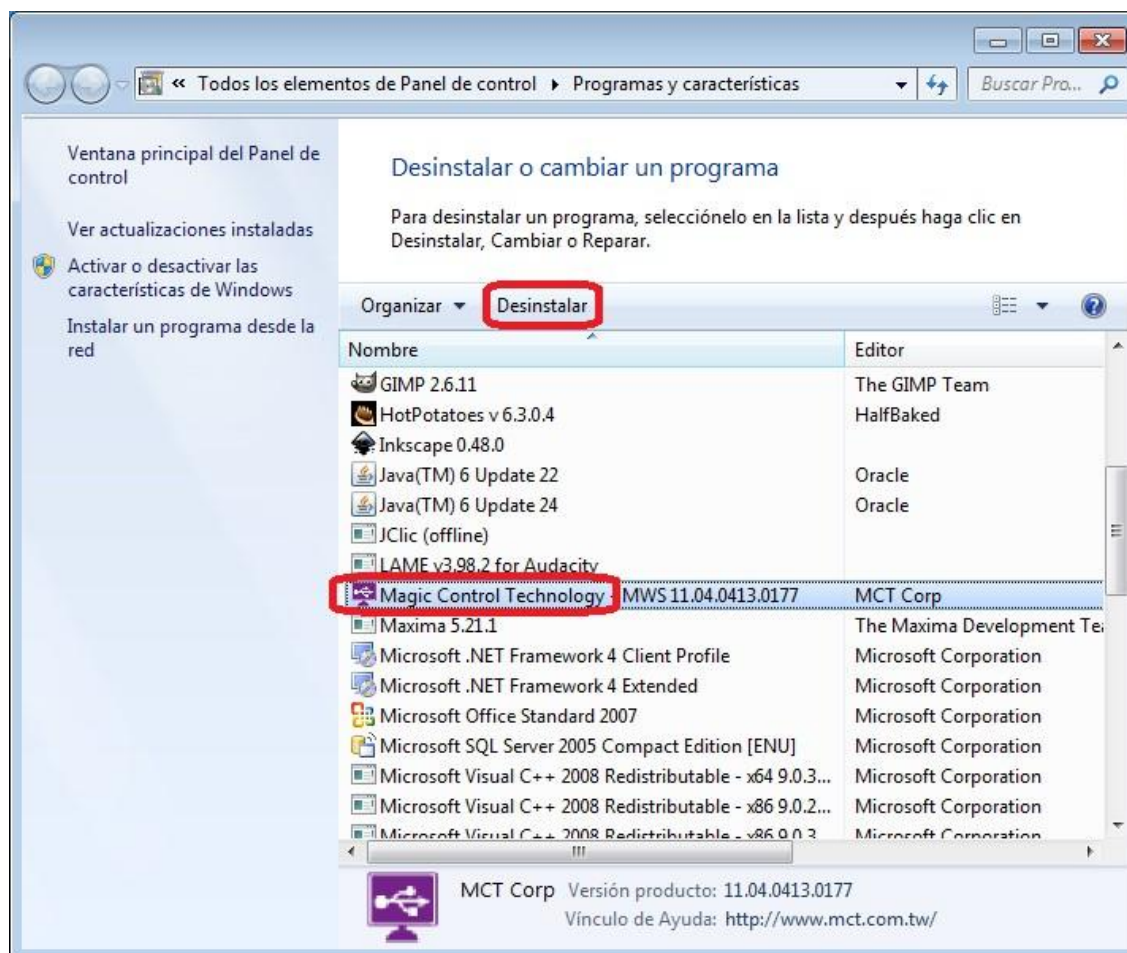
Conectar un teclado, ratón y monitor de forma directa (es indiferente que el equipo esté ya apagado o encendido), iniciar sesión con el usuario Administrador y cambiar a modo mantenimiento.

Para cambiar a modo mantenimiento desde el “Multipoint Manager” (se abre automáticamente después de unos segundos al iniciar sesión con un usuario administrador, o se puede ejecutar en “Inicio > Todos los programas > Windows MultiPoint Server > MultiPoint Manager”) hacer clic derecho en el equipo de “alumnoXX” y en el menú que aparece seleccionar “Cambiar a modo mantenimiento” o seleccionar el equipo y aparecerá la misma opción en el menú de la derecha:



Una vez en modo mantenimiento, pulsar el botón inicio, escribir en el cuadro de búsqueda “Desinstalar” y seleccionar “Desinstalar un programa”. De la lista de programas seleccionar el driver “Magic Control Technology” y desinstalarlo:





Al final de la desinstalación pedirá reiniciar, aceptamos para que reinicie el equipo.

Volver a entrar en modo mantenimiento e instalamos el nuevo driver, pero ahora cuando pregunte para reiniciar seleccionamos “No, reiniciaremos el equipo más tarde”. Apagamos el equipo y desconectamos el monitor, teclado y ratón local, conectamos los terminales multipoint si no estaban conectados y encendemos el equipo.

Se puede dar el caso de que una vez conectados los terminales, en el primer inicio no se active ninguno siendo necesario un segundo reinicio para que ya cargue correctamente el driver. Se puede reiniciar el equipo por medio del panel de “max-control” o accediendo por escritorio remoto.

Comprobar que ahora se activan todos los terminales, si no se activan todos revisar si hay algún problema de cableado o el terminal está averiado.



## **D. PROCEDIMIENTO PARA UNIR UN EQUIPO AL DOMINIO**

### **1. Windows**

Para poder unir un equipo al dominio, las versiones de Windows a utilizar tienen que ser la *Professional* o superior, no valen versiones como la HOME o inferiores ya que no disponen de la funcionalidad para poder unirse a un dominio. No se permite Windows XP, tiene que ser a partir de Windows 7.

### **2. MAX**

Se necesita MAX 9, de momento solo está desarrollado el procedimiento para esta versión.

### **3. En general...**

Los equipos a unir en el dominio tienen que estar en la misma red que la del servidor decentro, en los IIT (Institutos de innovación Tecnológica) es la VLAN110. Lo ideal antes de proceder es una vez que tenemos configurada la IP en el equipo, comprobar con un ping si llegamos al servidor de centro que tiene la IP 172.20.10.1.

Los datos para configurar la red del equipo son:

IP del equipo: entre la 172.20.0.1 y la 172.20.15.254

Máscara de red: 255.255.**240**.0

Puerta de enlace: 172.20.10.1

Servidor DNS: 172.20.10.1

Servidor WINS : 172.20.10.1

Dominio: iit.lan



## 4. Cómo unir un equipo al dominio

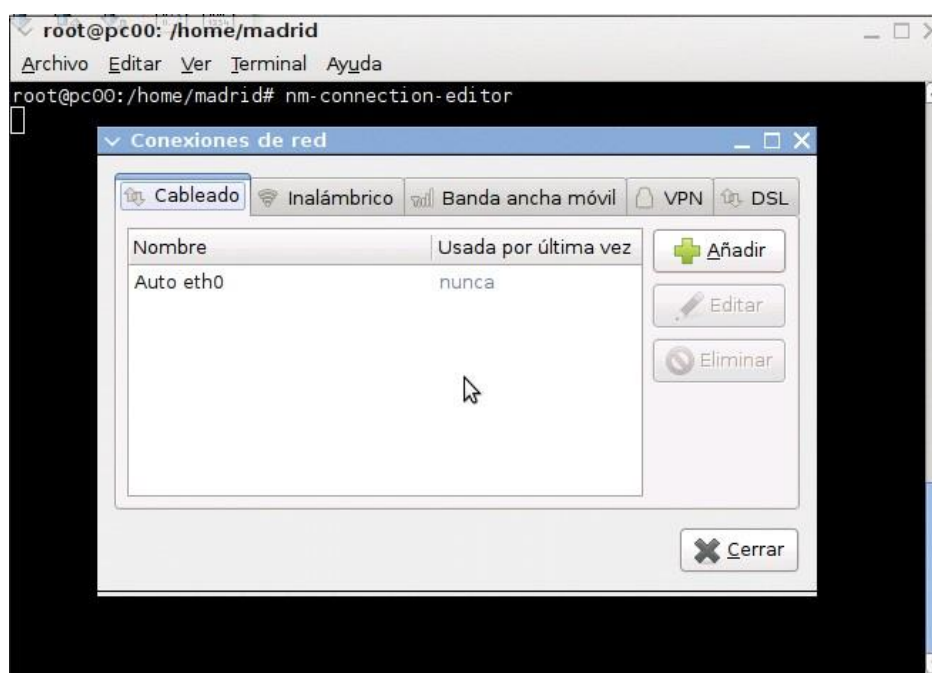
### 1) Procedimiento para MAX

NOTA: Si la maqueta es de un equipo de aulas tecnológicas existe el comando **“configurar\_equipo”** el cual es un *script* que podemos ejecutar (como *root*) para configurar de seguido los pasos 2,3,4,5 y 6.

1. Iniciar el equipo en MAX. Abrir un terminal desde “Inicio > Accesorios > Terminal” y tomar privilegios de *root*, para ello ejecutamos el comando “*sudo su*” y ponemos la contraseña cuando pregunte:

```
Archivo Editar Ver Terminal Ayuda
madrid@pc00:~$ sudo su
[sudo] password for madrid:
root@pc00:/home/madrid#
```

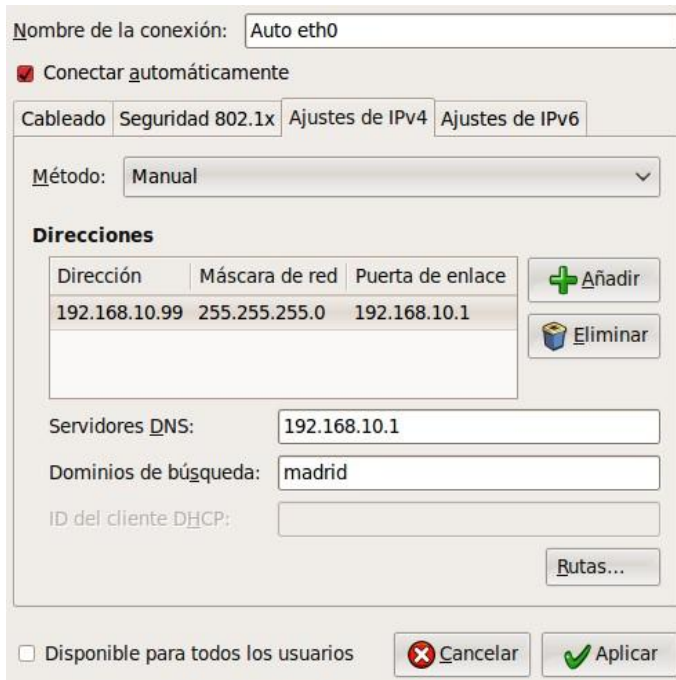
2. Configurar el adaptador de red. Es preferible que la IP sea estática, sobre todo para poder administrarlo desde el panel de control del servidor. La IP tiene que estar en el rango del servidor de centro (vlan110) por lo que tiene que ser de estilo *172.20.10.X*. Para configurar el adaptador de red ejecutamos desde el terminal el comando **“nm-connection-editor”** y se abrirá una ventana con los adaptadores disponibles:



- En dicha ventana seleccionamos el adaptador correspondiente, normalmente el **"Auto eth0"** y pulsamos el botón editar.

Aparecerá la siguiente ventana en la que tenemos que ir a la ficha **"Ajustes de Ipv4"** la cual configuraremos como se muestra en la imagen, cambiando la dirección IP **192.168.10.99** por una adecuada a nuestra red que esté libre.

Recuerdo que a partir de la 200 están reservadas para el DHCP por lo que no se deben utilizar:



Nombre de la conexión: Auto eth0

☒ Conectar automáticamente

Cableado Seguridad 802.1x Ajustes de IPv4 Ajustes de IPv6

Método: Manual

**Direcciones**

Dirección	Máscara de red	Puerta de enlace
192.168.10.99	255.255.255.0	192.168.10.1

+ Añadir  
Eliminar

Servidores DNS: 192.168.10.1

Domínios de búsqueda: madrid

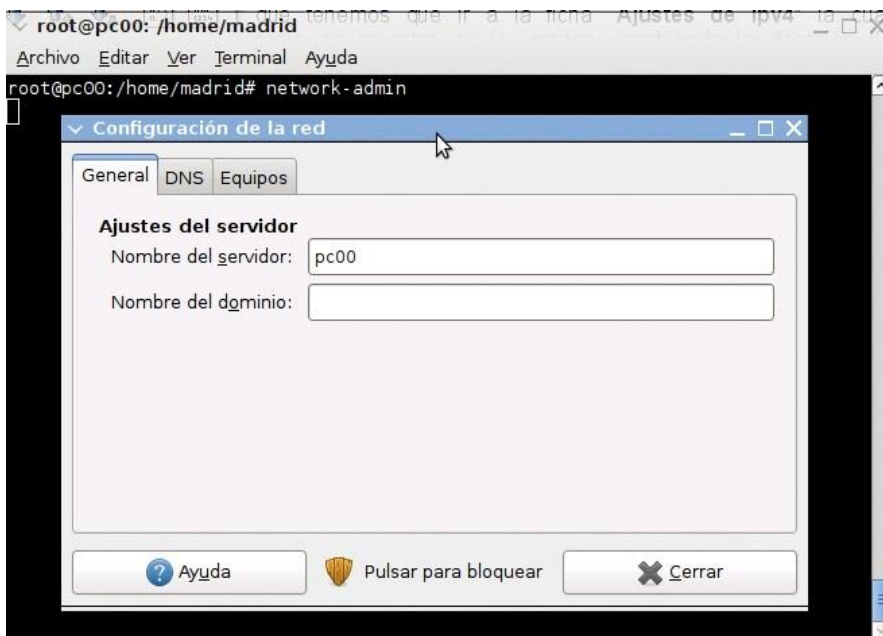
ID del cliente DHCP:

Rutas...

☐ Disponible para todos los usuarios

Cancelar Aplicar

- Aplicamos los cambios y cerramos también la ventana de conexiones de red volviendo así de nuevo al terminal.
- Cambiar el nombre de equipo. Para cambiar el nombre ejecutamos en el terminal el comando **"network-admin"**, aparecerá la siguiente ventana:



root@pc00: /home/madrid

Archivo Editar Ver Terminal Ayuda

root@pc00: /home/madrid# network-admin

**Configuración de la red**

General DNS Equipos

**Ajustes del servidor**

Nombre del servidor: pc00

Nombre del dominio:

Ayuda Pulsar para bloquear Cerrar

Cambiamos el **"Nombre del servidor"** y pulsamos el botón **"Cerrar"**, se pedirá confirmar el cambio del nombre, confirmamos y volveremos al terminal.

- Reiniciamos el equipo para que el cambio de nombre tenga efecto.



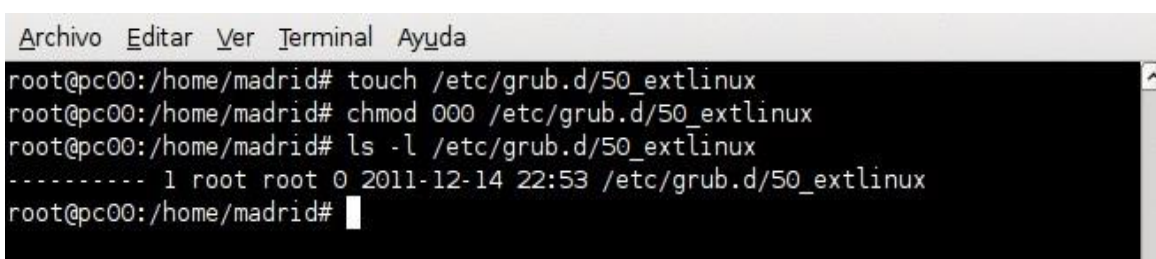


7. Volvemos a abrir un terminal y tomamos privilegios de *root* (paso 1).

NOTA: Los dos siguientes puntos (8 y 9), no hay que hacerlos en los equipos que tengan una maqueta de consejería para aulas tecnológicas ya que estas maquetas ya tienen realizada dicha configuración.

8. Ahora hay que instalar el paquete “max-ldap” el problema es que este paquete está preparado para las maquetas de las aulas tecnológicas ya que fuerza también la instalación del paquete “extlinux” que es un cargador de arranque que puede estropear el inicio de MAX si el equipo no se ajusta a un particionado concreto. No se puede evitar la instalación de “extlinux” pero sí anular su configuración para que no modifique el sistema, para ello hay que ejecutar estos dos comandos:

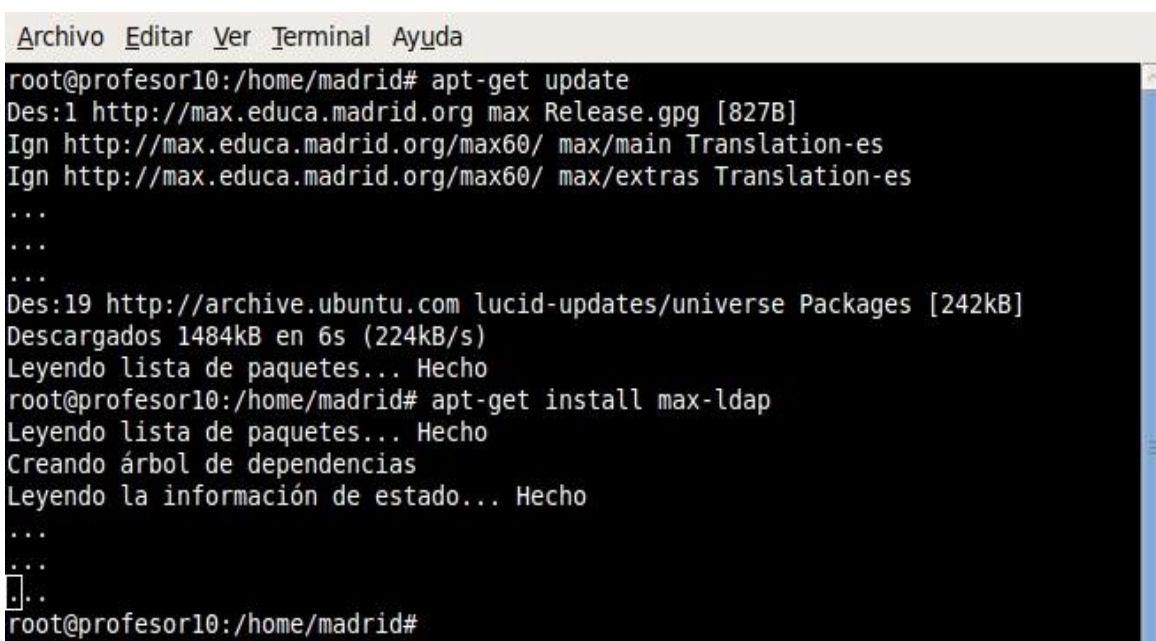
```
touch /etc/grub.d/50_extlinux chmod 000  
/etc/grub.d/50_extlinux
```



```
Archivo Editar Ver Terminal Ayuda  
root@pc00:/home/madrid# touch /etc/grub.d/50_extlinux  
root@pc00:/home/madrid# chmod 000 /etc/grub.d/50_extlinux  
root@pc00:/home/madrid# ls -l /etc/grub.d/50_extlinux  
----- 1 root root 0 2011-12-14 22:53 /etc/grub.d/50_extlinux  
root@pc00:/home/madrid#
```

Es conveniente con el comando “ls” asegurarse de que el fichero se ha creado y no tiene ningún permiso tal como se ve en la imagen.

9. Ahora ya se puede instalar el paquete “max-ldap”, ejecutamos: `apt-get update apt-get install max-ldap`



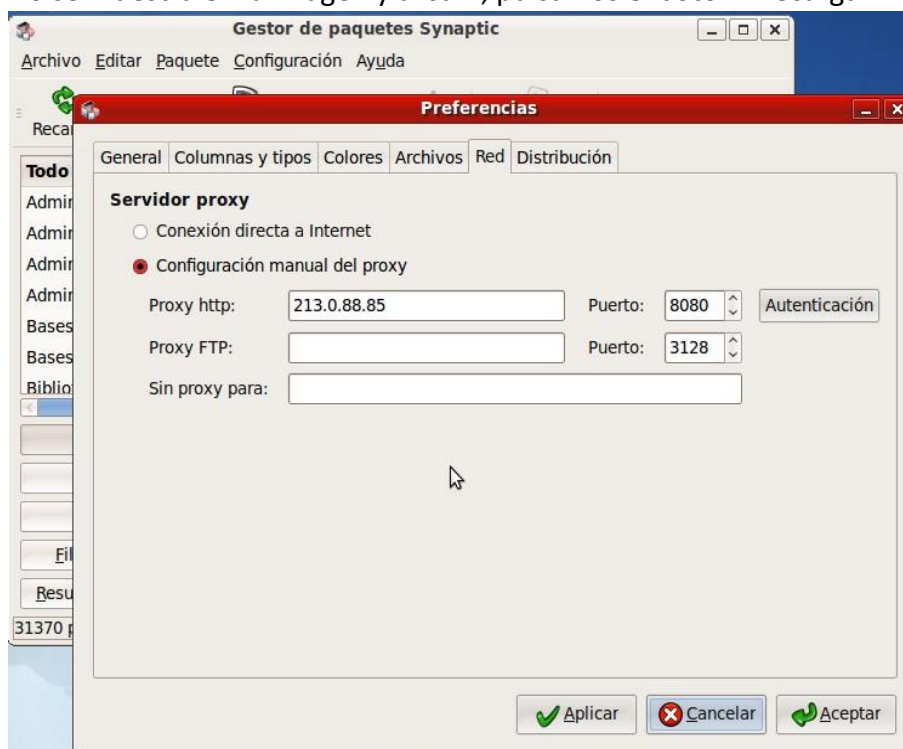
```
Archivo Editar Ver Terminal Ayuda  
root@profesor10:/home/madrid# apt-get update  
Des:1 http://max.educa.madrid.org max Release.gpg [827B]  
Ign http://max.educa.madrid.org/max60/ max/main Translation-es  
Ign http://max.educa.madrid.org/max60/ max/extras Translation-es  
...  
...  
...  
Des:19 http://archive.ubuntu.com lucid-updates/universe Packages [242kB]  
Descargados 1484kB en 6s (224kB/s)  
Leyendo lista de paquetes... Hecho  
root@profesor10:/home/madrid# apt-get install max-ldap  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
...  
...  
[.]...  
root@profesor10:/home/madrid#
```



Si tenemos problemas con el “apt-get update” probablemente es por que necesitamos configurar “apt” para que salga por el proxy(filtro). Para ello hay que crear el fichero de texto “/etc/apt/apt.conf.d/proxy” con el contenido:

Acquire::http::Proxy "http://213.0.88.85:8080";

Una alternativa a instalar el paquete por consola es utilizar el “Gestor de paquetes Synaptic” llendo al menú “Configuración > Preferencias > Red”, configuramos el proxy como se muestra en la imagen y al salir, pulsamos el botón “Recargar”:



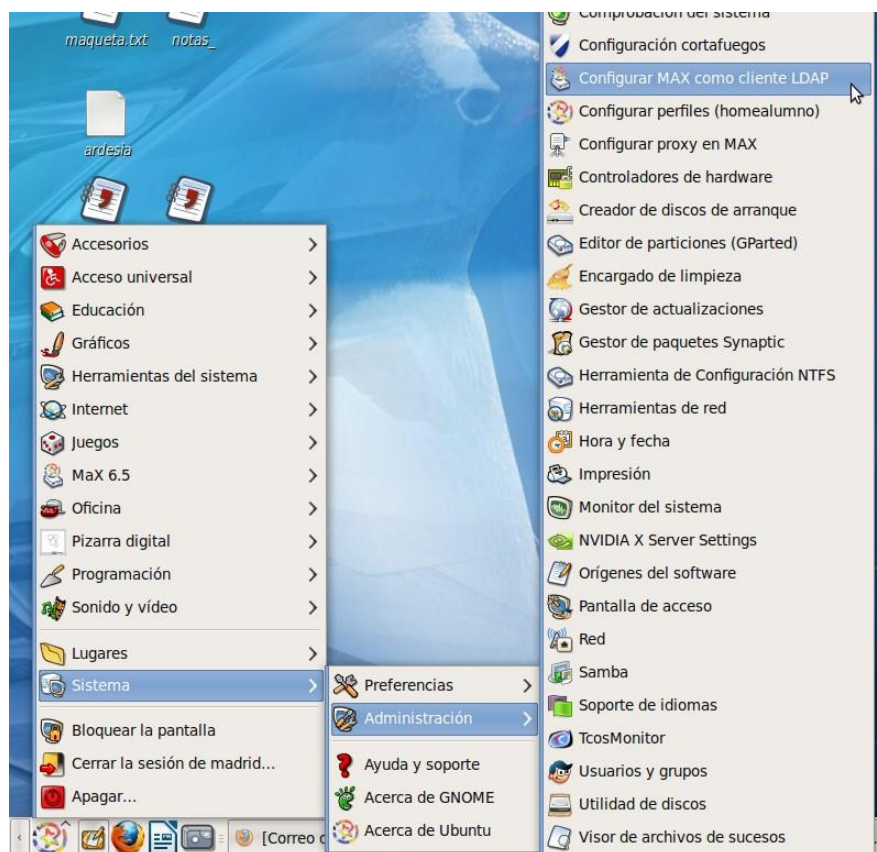
Ahora desde Synaptics se puede buscar el paquete *max-ldap* e instalarlo.





10. Una vez terminada la instalación del paquete *max-ldap* se habrá creado un icono en “Inicio > Sistema > Administración > Configurar MAX como cliente LDAP”:

11. Ejecutamos dicho icono, pedirá contraseña para obtener privilegios de *root*, una vez validados aparecerá la siguiente ventana que hay que configurar tal como muestra la imagen:



The image shows the 'MAX v.6.0 Configuración LDAP' window. It has a title bar with the MAX logo and version. The window is divided into two main sections: 'Datos' and 'Configuración LDAP'. The 'Datos' section contains the following fields:

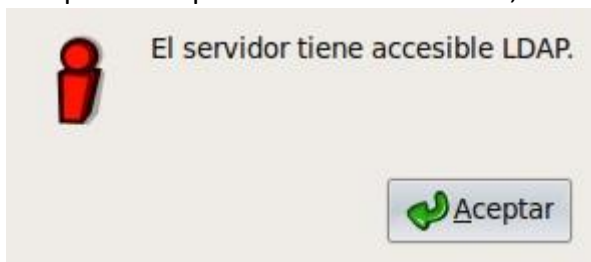
- IP/Nombre de maquina del servidor LDAP: 192.168.10.1
- Dominio: madrid
- Base DN: dc=max-server
- Administrador: uid=coordinadortc,ou=Users,dc=max-server
- Contraseña administrador: [masked with dots]

There is a 'Probar' button next to the IP field. At the bottom, there is a checkbox for 'ver contraseña' (unchecked) and two buttons: 'Aplicar' (with a green checkmark icon) and 'Salir' (with a red exit icon).

Como contraseña ponemos la que tenga el usuario *coordinadortc*.



12. Para comprobar que el equipo tiene conectividad con el LDAP del servidor de centro podemos pulsar el botón “Probar”, si todo es correcto mostrará:

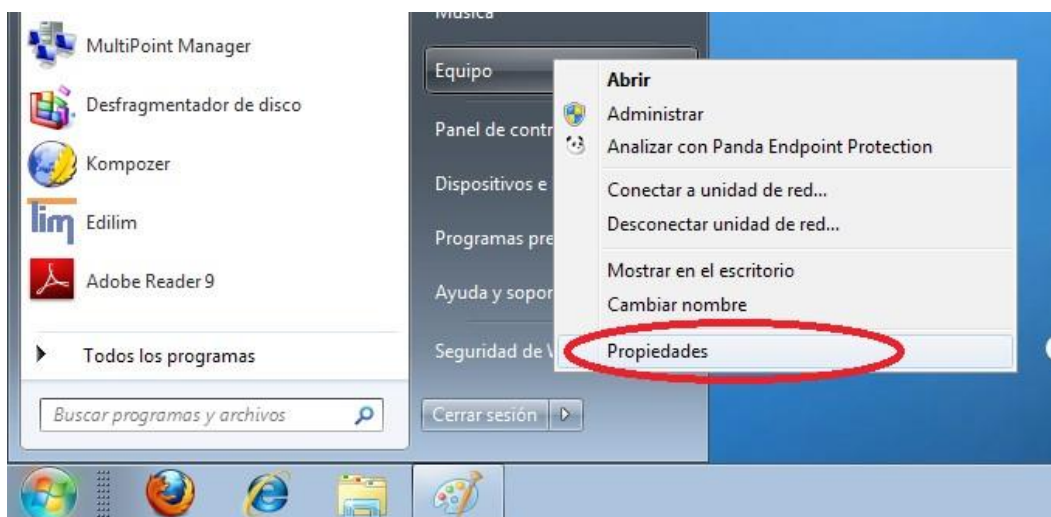


13. Pulsamos el botón “Aplicar” y comenzará a descargarse unos paquetes de *internet*, por lo que es importante comprobar antes que tenemos acceso a *internet*. Puede que pregunte para sobrescribir algún fichero de configuración como los de SAMBA, dejaremos la opción predeterminada que es mantener la configuración actual. Una vez terminado el proceso se mostrará un aviso para que reiniciemos el equipo.

14. El proceso ha terminado y una vez reiniciado el equipo ya podemos iniciar sesiones con usuarios del dominio.

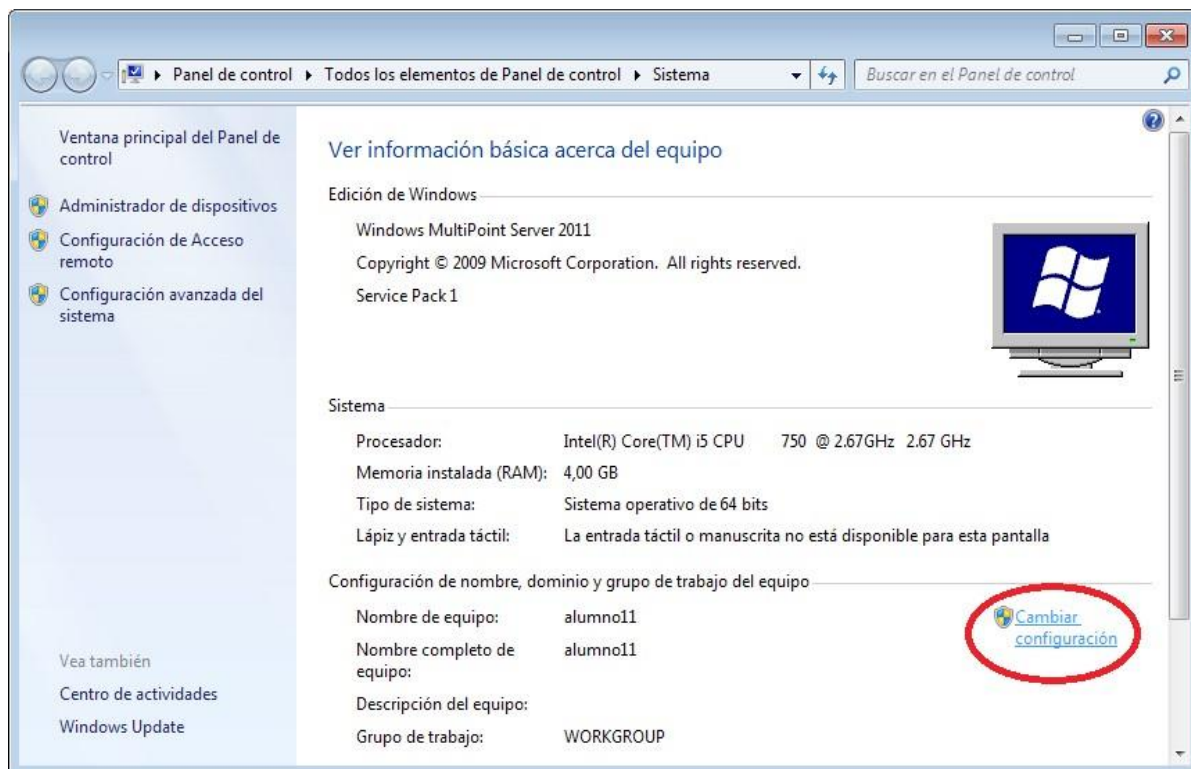
## 2) Procedimiento para Windows:

- 1) Iniciar el equipo en Windows y abrir sesión con algún usuario que tenga permisos de administrador.
- 2) Cambiar el nombre de equipo. Vamos al botón inicio y hacemos clic derecho en “Equipo” y seleccionamos “Propiedades”:

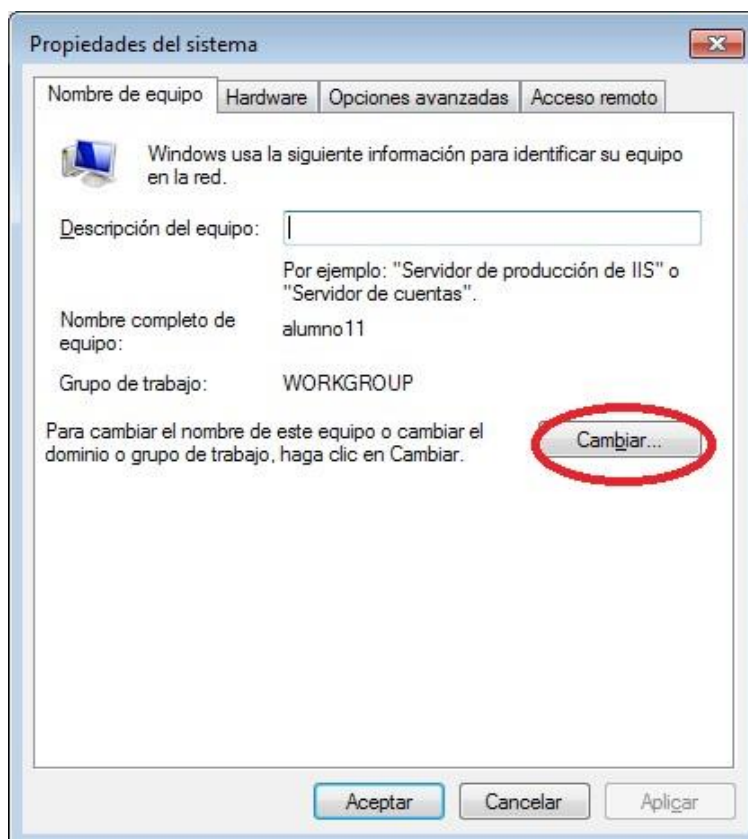


- 3) En la ventana que aparece pulsamos en “Cambiar configuración”:

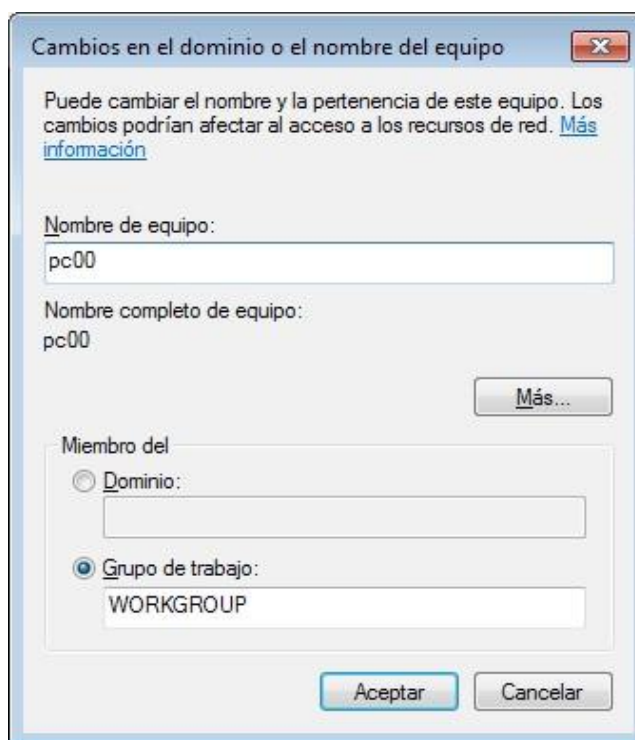




4) Pulsamos en el botón “Cambiar”:



- 5) En nombre de equipo ponemos el mismo nombre que hayamos puesto en MAX. Pulsamos en el botón “Aceptar” en las dos ventanas y aparecerá un mensaje indicando que es necesario reiniciar el equipo pero le diremos **“Reiniciar mas tarde”**.



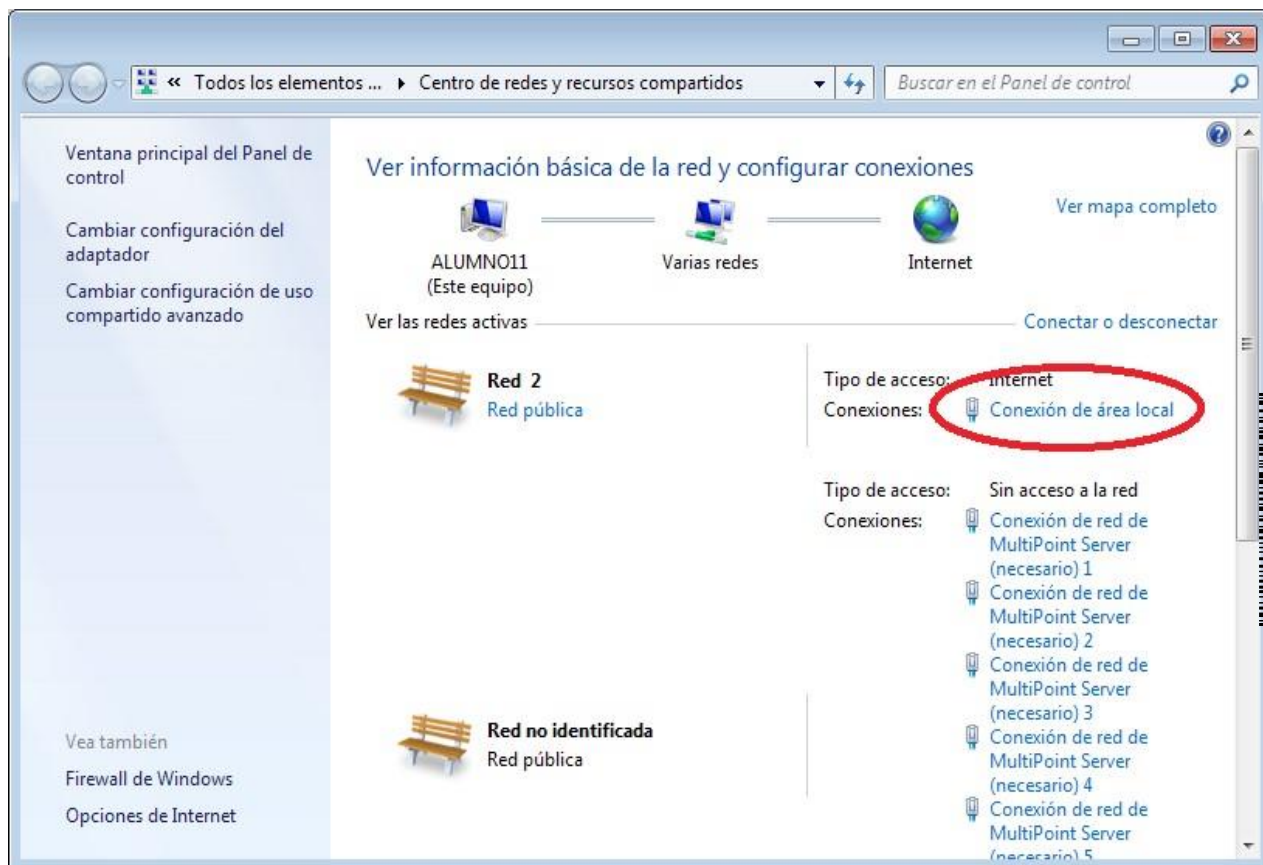
- 6) Configurar el adaptador de red. Hacemos *clic* en el icono de red del área de notificación y vamos al **“Centro de redes y recursos compartidos”**, también podemos acceder a él desde el panel de control:



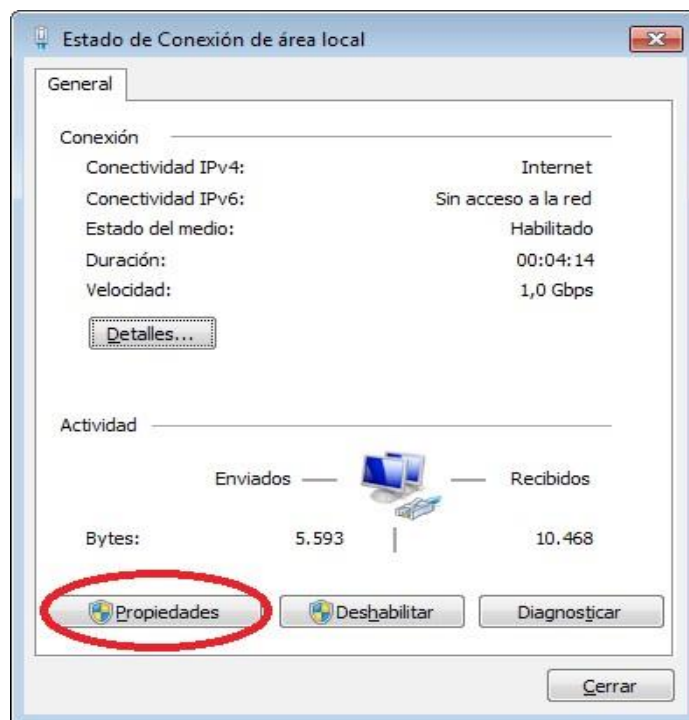
- 7) Entramos en la “Conexión de área local”. Si no aparece la conexión en esta primera ventana se puede encontrar en el menú de la izquierda en la opción “Cambiar configuración del adaptador”:



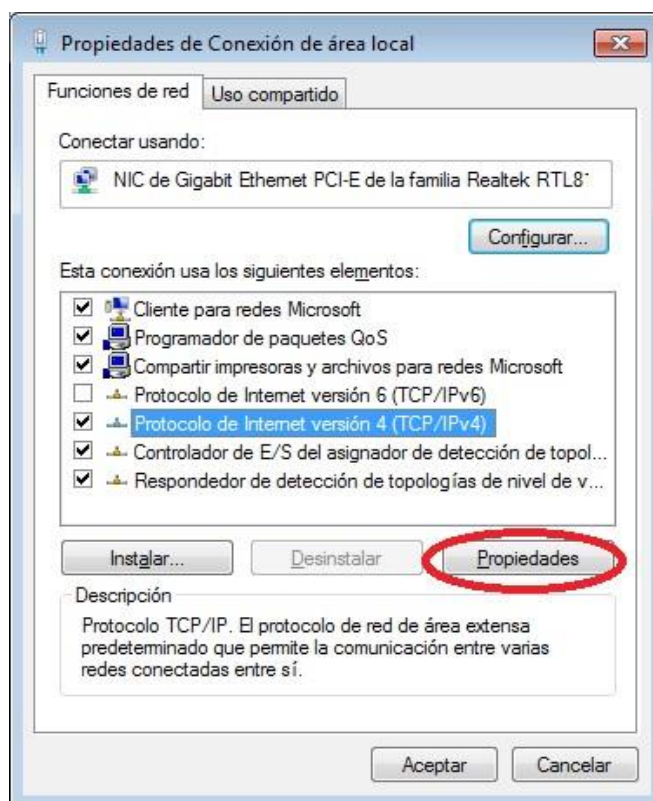




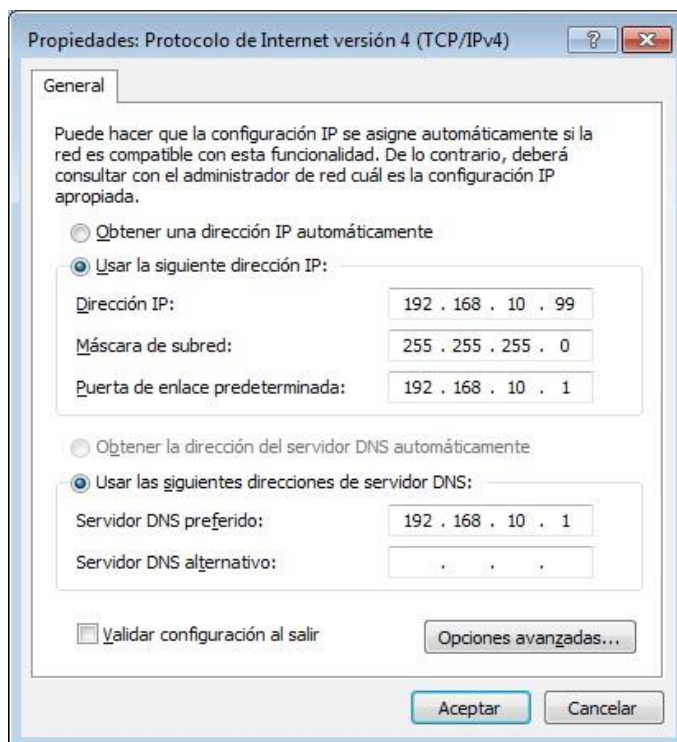
8) Pulsamos el botón de “Propiedades”:



- 9) Es conveniente desactivar el protocolo versión 6 si realmente nuestra red no tiene ninguna aplicación que haga uso de él, además en “Windows Multipoint Server 2011” existe un problema detectado que bloquea la conexión por “Escritorio remoto”. Seleccionamos el protocolo versión 4 y pulsamos el botón de propiedades:



- 10) Configuramos los datos del adaptador tal como se muestra en la imagen. La dirección IP tiene que ser la misma que se puso en MAX:



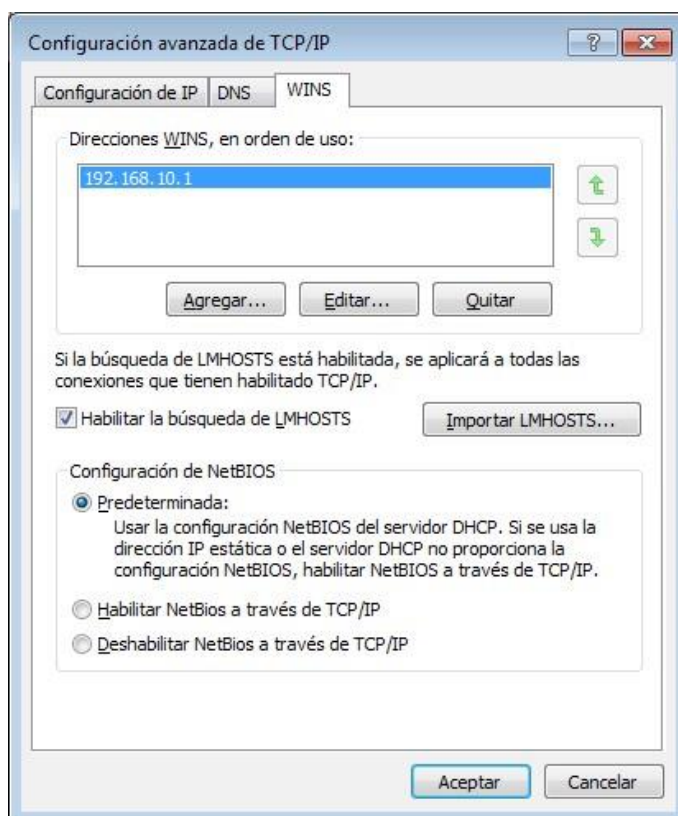


- 11) Pulsamos ahora en el botón de “Opciones avanzadas” y en la nueva ventana que aparece vamos a la ficha WINS y agregamos la dirección del servidor de centro. Cerramos todas las ventanas que han ido saliendo pulsando su botón de

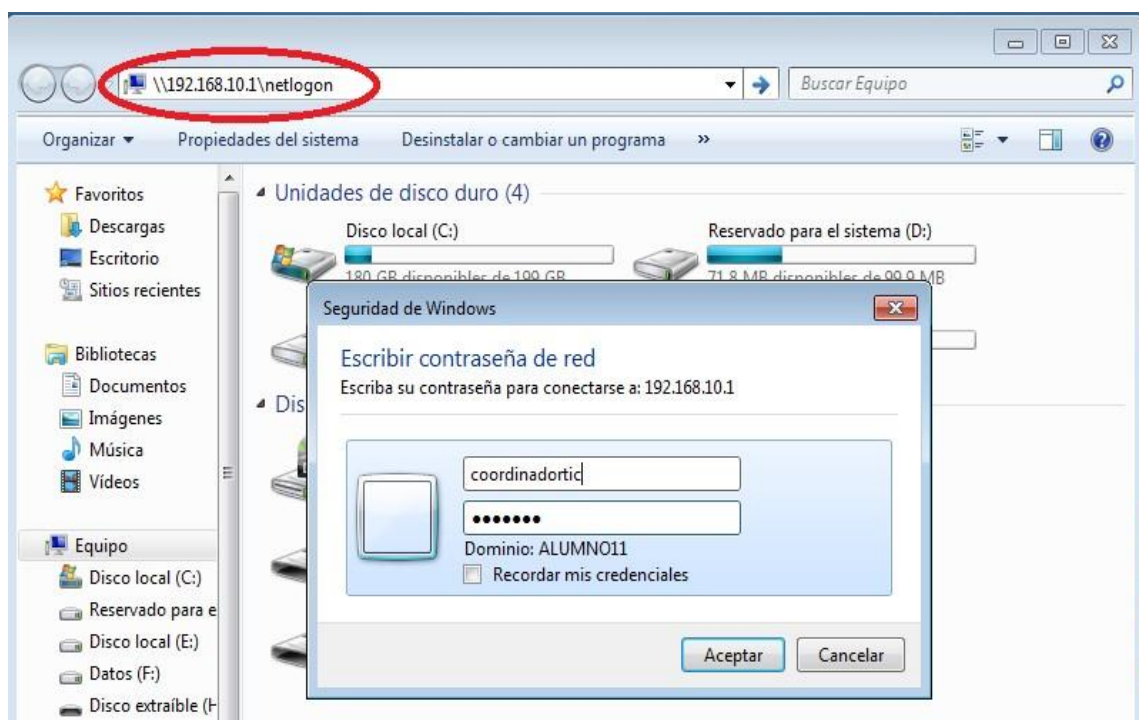
“Aceptar” para confirmar los cambios:

- 12) Ahora vamos a ejecutar un *script* ubicado en el servidor. Volvemos a iniciar sesión con un usuario administrador, vamos a “Inicio > Equipo” y en la barra de direcciones escribimos la siguiente dirección:

<\\192.168.10.1\netlogon>

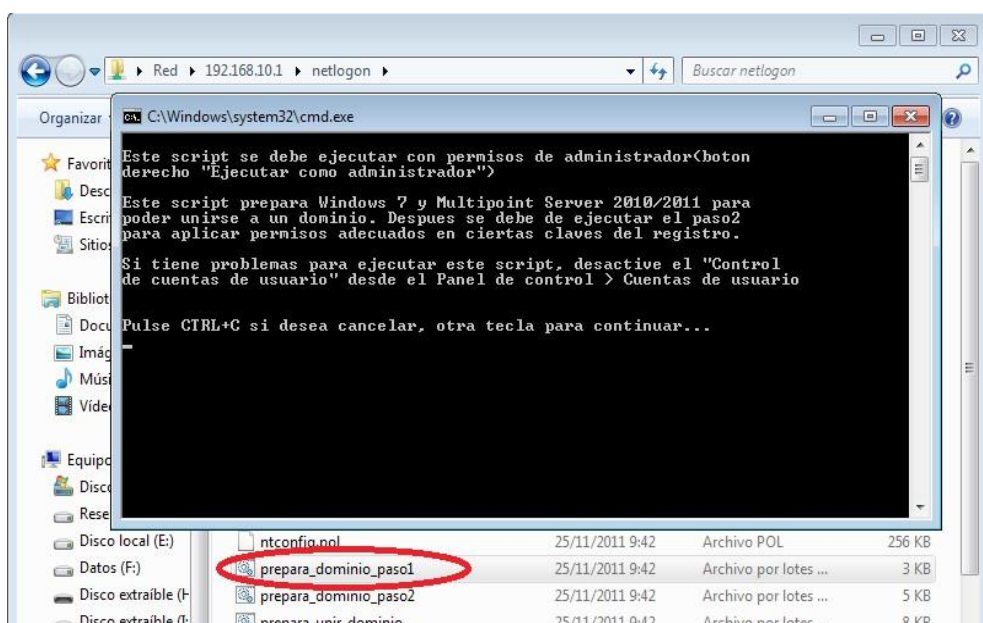


Pedirá usuario y contraseña, utilizaremos el usuario “coordinadortic”:

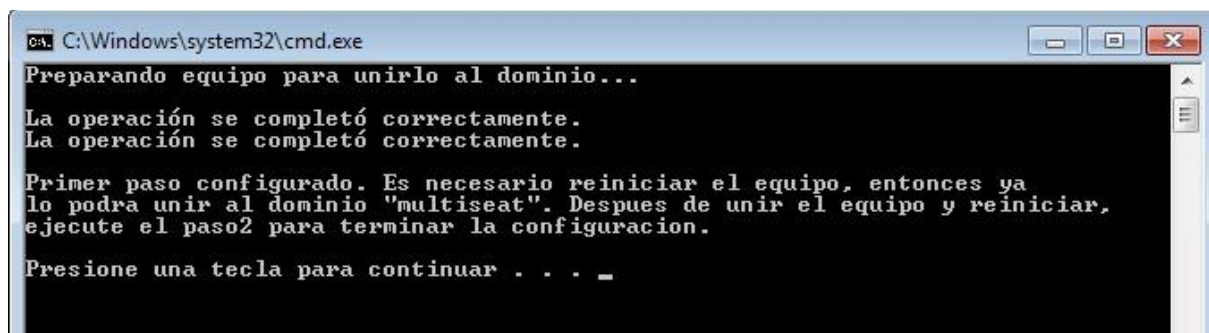


- 13) Se abrirá una carpeta en la que hay que ejecutar el fichero “**prepara\_dominio\_paso1**”. Si tenemos problemas para ejecutar el *script* deberemos desactivar desde el panel de control, el “Control de cuentas de usuarios”, también podemos probar a ejecutar el

*script* como administrador y si seguimos con problemas podemos copiarlo al escritorio y ejecutarlo desde ahí:



- 14) En la ventana de terminal que aparece pulsamos ENTER para confirmar la ejecución del *script*. Una vez terminada la ejecución pulsamos ENTER o cerramos directamente la ventana y reiniciamos el equipo para que los cambios surjan efecto:

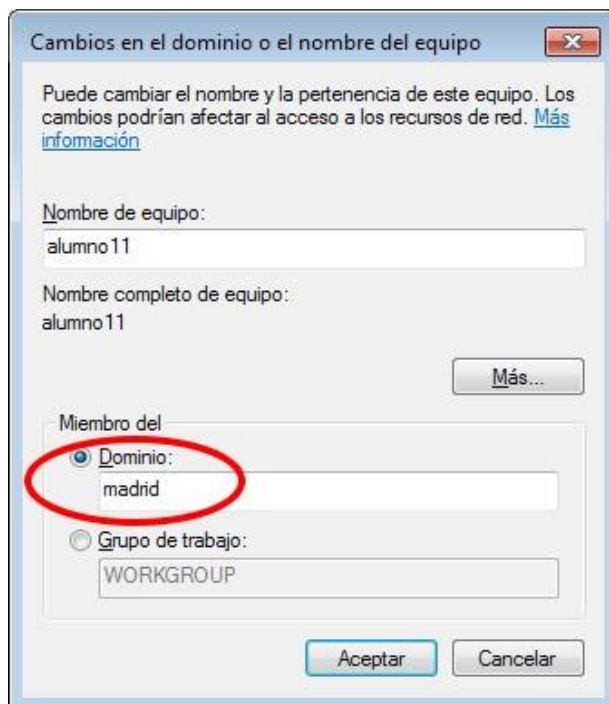


- 15) NOTA: Este *script* simplemente añade una clave al registro de Windows para que posteriormente pueda encontrar el dominio del servidor de centro. Si esta clave no existe Windows informará de que no encuentra el dominio "madrid" cuando intentemos unir el equipo al dominio.
- 16) Si estamos uniendo un equipo con Multipoint Server 2011, ahora instalaremos el driver de los terminales que se encuentra en "[C:\Driver MCT](#)". Nos aseguraremos que dicha carpeta tiene al menos una versión igual o superior al fichero:

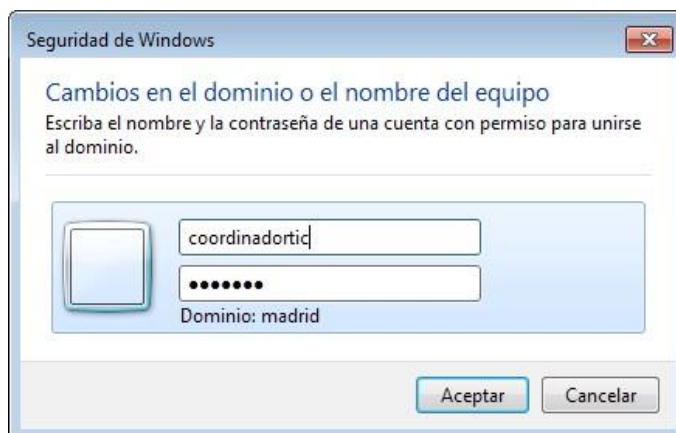
[MWS-via-USB-11.10.1209.0177.exe](#)

- 17) Una vez de nuevo en Windows ya podemos unir el equipo al dominio, para ello volvemos a la ventana donde cambiamos el nombre de equipo(ver los pantallazos anteriores) y ahí seleccionamos ahora "Dominio" y escribimos como dominio **madrid**:

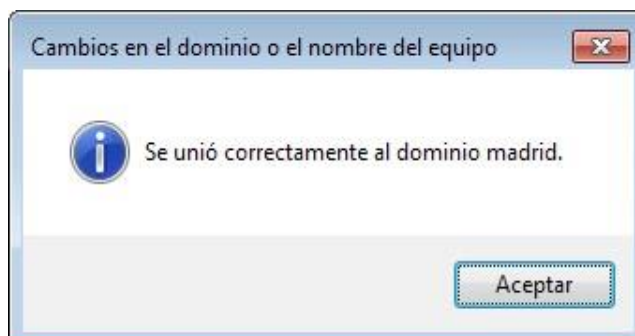




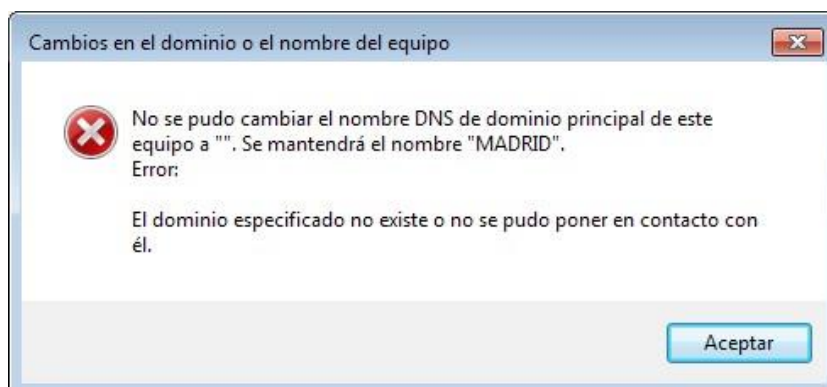
- 18) Al pulsar el botón “Aceptar” pedirá usuario y contraseña, utilizaremos el usuario “coordinadortic”:



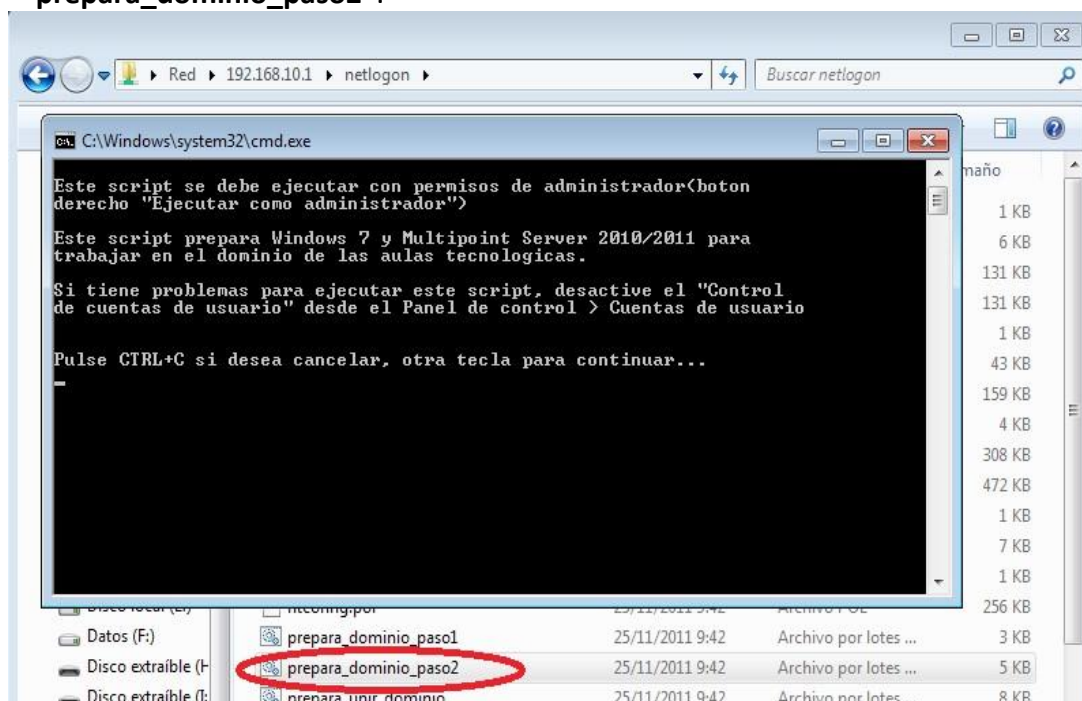
- 19) Después de unos segundos finalmente se mostrará el mensaje indicando que el equipo se ha unido al dominio con éxito:



- 20) **NOTA:** En algunas versiones de “Windows 7” se puede obtener antes un mensaje de error de DNS el cual podemos ignorar:



- 21) Lo importante es que después de este mensaje visualicemos el mensaje de que se ha unido correctamente el equipo al dominio.
- 22) Al cerrar las ventanas Windows pedirá reiniciar pero en este caso le diremos **“Reiniciar mas tarde”** ya que ahora hay que ejecutar el *script* “prepara\_dominio\_paso2” el cual también necesita reiniciar el equipo después de sus ejecución, de esta manera también nos ahorraremos otro reinicio. Por tanto cancelamos el reinicio del equipo, vamos de nuevo a la ruta [\\192.168.10.1\netlogon](http://192.168.10.1/netlogon) y ejecutamos el script **“prepara\_dominio\_paso2”**:



- 23) Confirmamos su ejecución pulsando ENTER, en este caso dependiendo del usuario con el que se ejecute puede pedir confirmación del usuario y contraseña. Si pregunta utilizaremos el usuario “coordinadortic”:





```
C:\Windows\system32\cmd.exe
Conectando unidad de red w:(\\max-server\netlogon)...
Escriba el nombre de usuario para "max-server": consejeria
Escriba la contraseña para max-server:
Se ha completado el comando correctamente.

Ya existe el subdirectorio o el archivo c:\Windows\educamadrid.
Copiando politicas de grupo a C:\Windows\System32\GroupPolicy...
C:\borrame\gpt.ini
C:\borrame\Machine\Registry.pol
C:\borrame\User\Registry.pol
C:\borrame\User\MICROSOFT\IEAK\install.ins
4 archivo(s) copiado(s)
Copiando mount.bat a C:\Windows\System32...
1 archivo(s) copiado(s).

Desconectando la unidad w:(\\max-server\netlogon)...
w: se ha eliminado.

Fase 2 de configuracion terminada.
Presione una tecla para continuar . . .
```

- 24) Cuando termine la ejecución hay que reiniciar el equipo, entonces ya podemos iniciar sesión con usuarios del dominio.
- 25) Si el equipo que se ha unido al dominio es un Windows Server Multipoint 2011, en el reinicio después de haberlo unido al dominio, los terminales dejarán de funcionar. Para que vuelvan a funcionar hay que iniciar sesión como administrador. Una vez iniciada la sesión esperamos a que aparezca el panel de control "Multipoint Manager" y simplemente reiniciamos el equipo. En el siguiente reinicio ya volverán a funcionar todos los terminales.
- 26) El nuevo equipo ya está unido en el dominio y podemos comprobar que aparece en el panel de control del servidor(max-control) pero en este panel necesita configurarse su IP y MAC:



Administrador  
Salir de sesión

Panel de control de Servidor de Centro

**Menú**  
 Mi perfil  
 Usuarios y Grupos  
 Aulas y Equipos  
     Aulas  
     Equipos  
 Distribuir ISOS  
 Apagado y reinicio  
 Programar arranque

### Listado de equipos (4)

Nombre ▲ ▼	IP ▲ ▼ / MAC ▲ ▼	Aula ▲ ▼	Editar	Estado	Borrar
profesor10\$	192.168.10.10 / 40:61:86:93:01:0e	aula1		✗	<input type="checkbox"/>
alumno12\$	192.168.10.12 / 40:61:86:93:19:2b	aula11		✗	<input type="checkbox"/>
alumno11\$	192.168.10.11 / 40:61:86:ca:63:df			✓	<input type="checkbox"/>
alumno13\$	○ / ○	○		✗	<input type="checkbox"/>

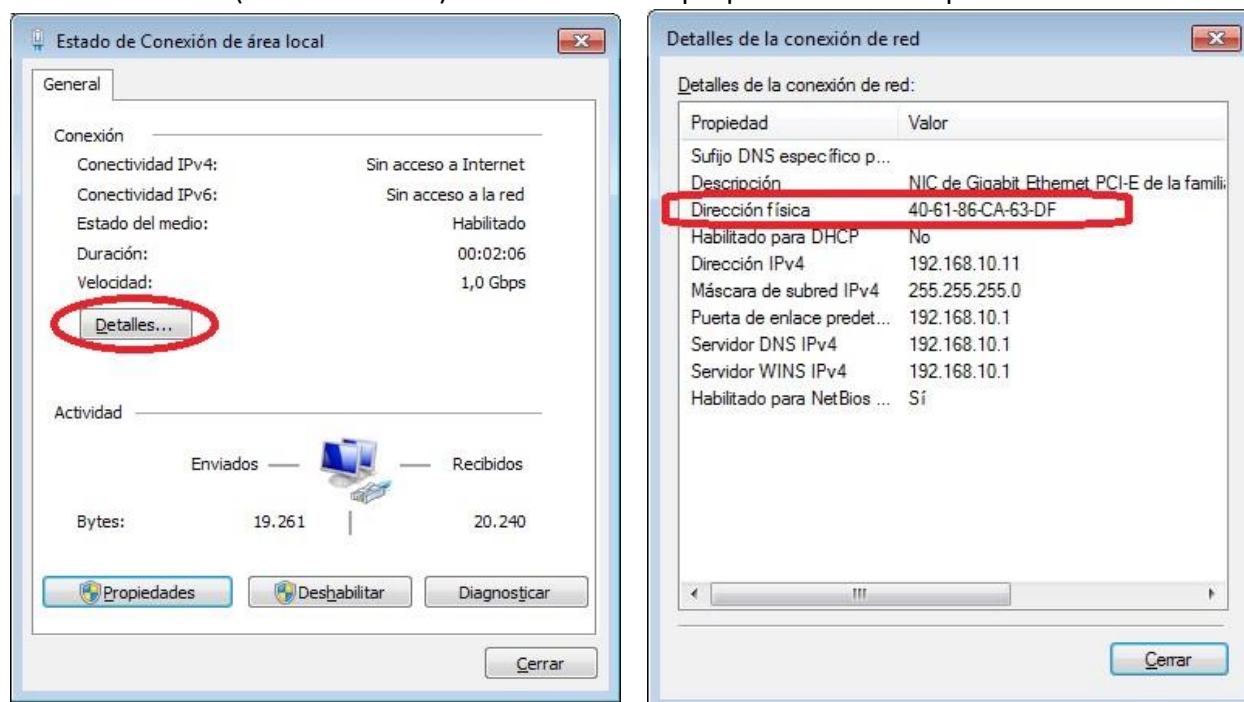
- 27) Esta configuración está restringida a personal de la consejería o de la empresa de mantenimiento. Para su configuración enviaremos un e-mail a la siguiente dirección:

[areatic@educa.madrid.org](mailto:areatic@educa.madrid.org)





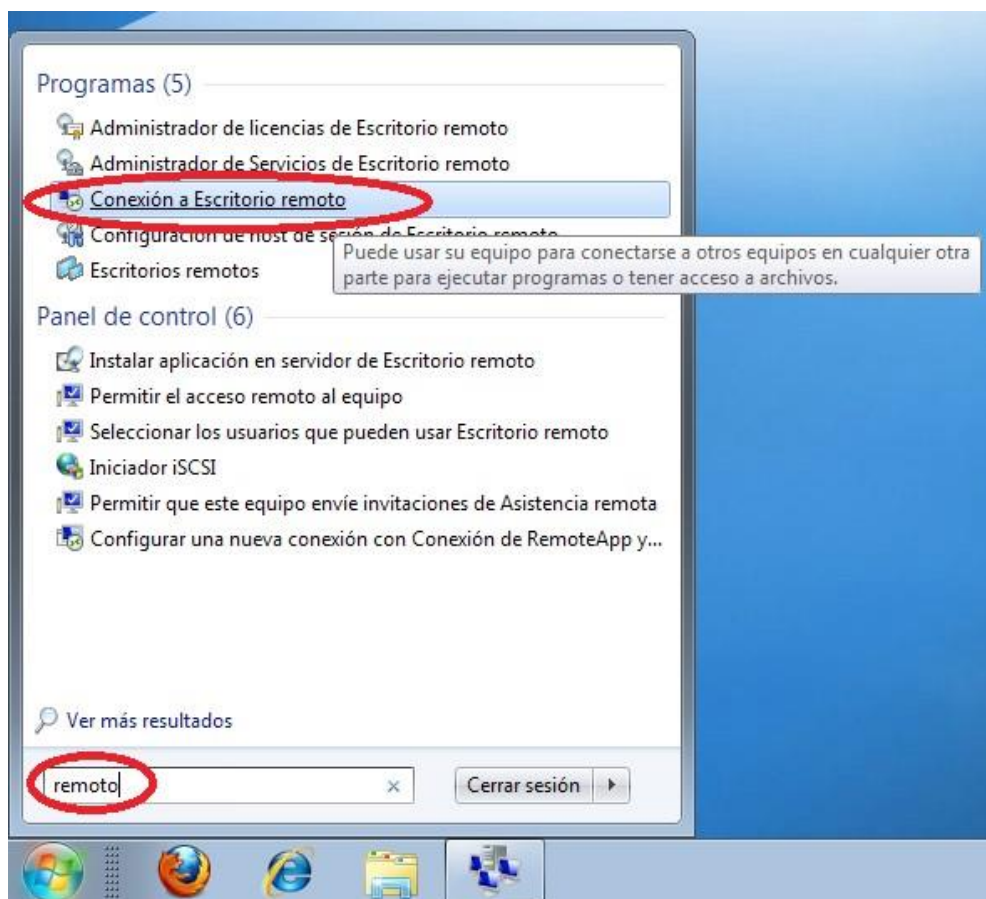
- 28) En el e-mail se debe especificar el nombre del centro, el nombre del equipo, la IP asignada su MAC y opcionalmente si se desea incluir ese equipo en un aula concreta. La MAC(Dirección física) se obtiene en las propiedades del adaptador de red:



### 3) ANEXO 1. Cómo conectarse por escritorio remoto a otro equipo

En la barra de búsqueda escribimos “remoto” y seleccionamos “Conexión a Escritorio remoto”. También podemos encontrar su icono en “Inicio > Todos los programas > Accesorios”:





Aparecerá la siguiente ventana donde introduciremos el nombre o la IP del equipo al que queremos conectar, es preferible utilizar la IP del equipo:



Preguntará por un usuario y contraseña, ponemos el usuario *administrador*, pero si el equipo ya está unido al dominio habrá que forzar que sea el propio equipo el que valide el usuario y no lo busque en el dominio, para ello se pone el nombre del equipo y el usuario separado por la barra “\”, por ejemplo:

alumno12\administrador

Aparecerá un aviso de seguridad en el que podemos marcar el “check” para que no vuelva a preguntar y pulsamos el botón

“Sí”:



En este momento se abrirá una ventana a pantalla completa con el escritorio del equipo remoto. Ahora mismo estamos conectados tal como si hubiéramos iniciado sesión localmente desde su consola. En la parte superior aparece una pequeña barra con los botones típicos de maximizar, minimizar y restaurar ventana. Al estar en una ventana a tamaño completo, a veces hay que tener precaución de comprobar en qué escritorio estamos, si en el local de nuestra máquina en la que estamos sentados, o en el remoto, para no ejecutar las acciones en el equipo equivocado.

Dependiendo de la versión de Windows o la configuración que se tenga del escritorio remoto puede que la ventana de credenciales en vez de mostrarse tal como hemos indicado, nos conectemos directamente al equipo y nos pida ahí las credenciales:



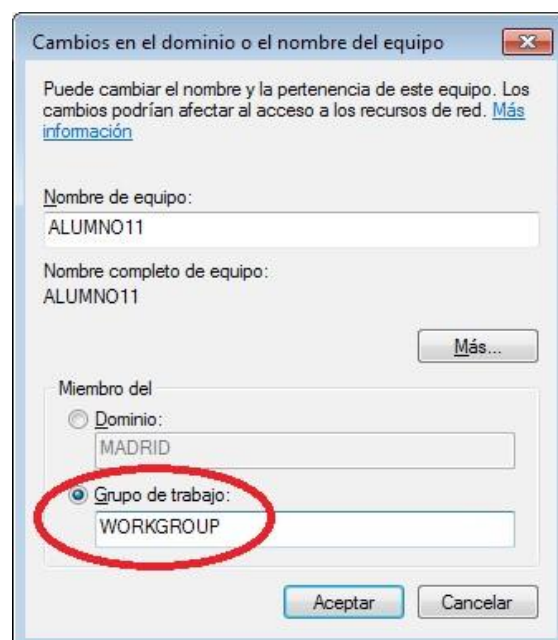
#### 4) ANEXO 2. Cómo sacar un equipo del dominio

**EN MAX:** Para sacar del LDAP un equipo en MAX se usa el mismo programa que se ejecutó para unirlo. Por tanto ejecutamos el programa que hay en “Inicio > Sistema > Administración > Configurar MAX como cliente LDAP”. La diferencia es que cuando el equipo ya está unido al dominio el programa detecta esta situación y entonces directamente pregunta si lo que queremos hacer es sacarlo de él:



Respondemos “Sí” a la pregunta y después de unos segundos terminará su proceso, entonces reiniciaremos el equipo para que los cambios surjan efecto.

**EN WINDOWS:** Para sacar un equipo del dominio en Windows lo que hay que hacer es pasarlo a un grupo de trabajo por lo que vamos a la ventana de cambio de dominio o nombre del equipo, seleccionamos “Grupo de trabajo” y escribimos un nombre, puede ser cualquiera. Una vez unido al grupo de trabajo habrá que reiniciar el equipo:





## E. MANUAL DEL SERVIDOR DE CENTRO

### 1. CARACTERÍSTICAS DEL SERVIDOR DE CENTRO



Procesador	Intel(R) Core(TM) i3 CPU 530 @ 2.93GHz
Placa base	ASUS modelo P7H57D-V EVO
Memoria	2 módulos de 2GB(1333MHz) – Total 4GB
Discos duros	6 discos SATA de 750GB – modelo SAMSUNG HD753LJ
BIOS	American Megatrends Inc. - versión 1204
Versión de Linux	max-server de 64bit (basada en Zentyal/Ubuntu 10.04.2)

### 2. CONFIGURACIÓN DE LA BIOS

Para acceder a la BIOS pulsar la tecla [Supr]. Configuraciones:

Poner la hora y fecha correctas.

[Power]

▢ APM Configuration

Restore on ACE Power Loss [Power On]

▢ Hardware Monitor

Chassis Q-Fan Control [Enabled]

Chassis Fan Profile [Standard]

[Boot]

▢ Boot Setting Configuration

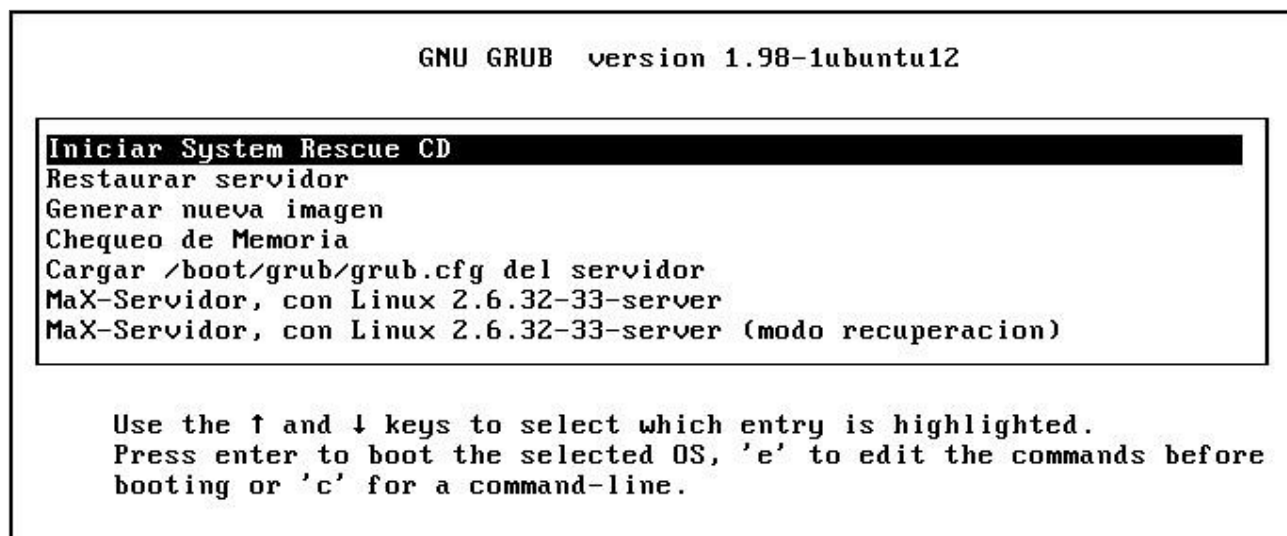
Quick Boot [Disabled]



Full Screen Logo [Disabled] Wait  
For 'Fl' If Error [Disabled]

### 3. INSTALACIÓN DESDE MAQUETA(USB)

La puesta en marcha de un servidor se realiza mediante una maqueta existente en una memoria USB. Dicha memoria está preparada para que arranque con un menú de *grub* personalizado el cual permite lanzar la remaquetación del servidor. Al iniciar desde la memoria se muestra el siguiente menú:



#### a) Iniciar System RescueCD

El sistema de remaquetación funciona en el entorno del SystemRescueCD. Esta opción permite iniciar la consola del SystemRescueCD y poder ejecutar comandos de forma manual.

#### b) Restaurar servidor

Esta opción remaqueta el servidor. No hay ninguna pregunta más de confirmación por lo que es importante estar seguros antes de continuar pues todo lo que hay en el servidor será eliminado. Al seleccionar dicha opción primero se carga el SystemRescueCD y automáticamente se lanzan los *scripts* de restauración de la maqueta.

#### c) Generar nueva imagen

Con esta opción podemos sacar una nueva imagen del servidor de centro, pero en este caso no se ejecuta nada de forma automática, tan sólo se carga el SystemRescueCD y antes de salir a la consola se muestra un mensaje de información con los pasos a seguir para crear una nueva imagen, por lo que prácticamente equivale a la primera opción con la diferencia de que aquí se monta automáticamente el USB en `"/mnt/backup"`.



d) Chequeo de Memoria

Carga el programa “memtest+” que permite comprobar el estado de la memoria.

e) Cargar /boot/grub/grub.cfg del servidor

El fichero /boot/grub/grub.cfg contiene el menú inicial que vemos al encender el equipo. En caso de que el *grub* del servidor falle, esta opción intenta cargar este fichero de configuración lo que nos permitiría iniciar el servidor.

f) MaX-Servidor, con Linux 2.6.32-33-server

Si la anterior opción no funciona podemos intentar iniciar el equipo tal como lo hace en su fichero de configuración cargando directamente el kernel. Hay que tener en cuenta que esta opción prueba a cargar el kernel 2.6.32-33-server que es la versión inicial que había cuando se instaló el servidor. Si el servidor a tenido alguna actualización puede que la versión del kernel actual con la que esté trabajando sea superior. En cualquier caso este kernel debería de funcionar ya que no se borran los kernels antiguos cuando se instala un nuevo kernel.

#### 4. CONFIGURACIONES DESPUÉS DE REMAQUETAR

Después de remaquetar un servidor hay que realizar las siguientes configuraciones:

1. Al clonar un servidor si luego queremos cambiar la contraseña al usuario *madrid* obtendremos un mensaje de error, para solucionarlo hay que ejecutar lo siguiente:

```
sudo dpkg-reconfigure -plow libpam-runtime
```

Ahora ya se puede cambiar la contraseña del usuario “madrid”.

2. Activar el parámetro “**GRUB\_TERMINAL=console**” en el fichero “/etc/default/grub”. Para ello sólo hay que quitar la almohadilla(#) del inicio de la línea. Después ejecutar **update-grub2**. Esto hace que el menú de grub se muestre en modo texto ya que se ha detectado que en caso de que falle el disco sda no se consigue iniciar desde sdb debido a un problema que se origina con el menú de grub en modo gráfico.

3. Para que funcione el control remoto de Fractalia y se pueda establecer una conexión

SSH al servidor mediante la VPN que crea su cliente, hay que añadir la siguiente regla del firewall:



**Filtrado de paquetes ▶ Desde redes externas hacia Zentyal**

**Editando regla**

Decisión: **ACEPTAR** ▼

Origen: **IP Origen** ▼ 10.5.0.1 / 32 ▼

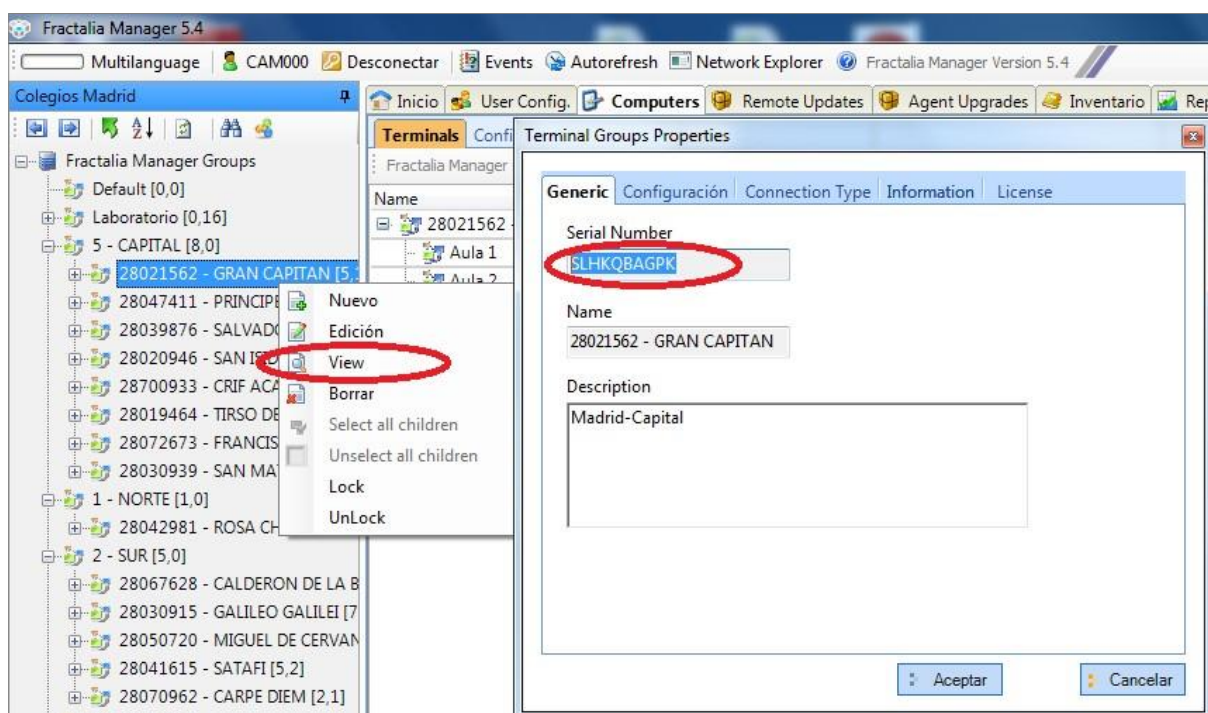
Servicio: **any TCP** ▼ Coincidencia inversa: ☐

Si la selección inversa está marcada, la regla será aplicada cualquier servicio excepto el seleccionado

Descripción: **FRA OpenVPN**

*Opcional*

4. Crear el fichero de licencia en “/var/www/licencia.txt” para los clientes de Fractalia. Este fichero simplemente contiene un número que se puede obtener del portal de administración de Fractalia:



5. Para evitar ciertos errores con las cabeceras http 1.1 (por ejemplo el fallo en la carga del componente de fractalia) hay que añadir la siguiente línea al final del todo del fichero de la plantilla del squid “/usr/share/zentyal/stubs/squid/squid.conf.mas”:

ignore\_expect\_100 on

Este error ha sido corregido en versiones superiores del “squid” pero no en la versión 2.7.STABLE7 que es actualmente la que tiene.

6. Desactivar la resolución de nombres IPv6. Editar el fichero:

/etc/init/ebox.bind9.conf

Modificar la siguiente línea para que quede así(se ha añadido el “-4”):

```
exec /usr/sbin/named -4 -u bind -f
```

Reiniciar el servicio: `service bind9 restart`

## 7. Desactivar los log del samba. Editar el fichero:

```
/usr/share/ebox/stubs/samba/smb.conf.mas
```

Comentar todas las líneas que empiezan por “vfs objects” añadiendo “#” al inicio de la línea. Comentar también las dos líneas que comienzan por “full\_audit”. Reiniciar el servicio desde el panel web desactivando y activando el módulo “Compartir ficheros”.

También se puede hacer desde consola si hacemos los mismos cambios en el fichero `/etc/samba/smb.conf` y ejecutamos `service smbd restart`.

## 8. Indexar campos en el ldap:

Si miramos el fichero `/var/log/syslog` podemos encontrar entradas como estas:

```
Oct 16 10:45:46 max-server slapd[2907]: <= bdb_substring_candidates: (uid) not indexed
Oct 16 10:45:46 max-server slapd[2907]: <= bdb_substring_candidates: (cn) not indexed
Oct 16 10:45:46 max-server slapd[2907]: <= bdb_substring_candidates: (sn) not indexed
Oct 16 10:47:25 max-server slapd[2907]: <= bdb_equality_candidates: (displayName) not indexed
```

Lo que indica que es recomendable crear un índice para ellas añadiendo una línea en el fichero

`"/etc/ldap/slapd.d/cn\=config/olcDatabase\=\{1\}hdb.ldif"` del tipo:

```
olcDbIndex: <campo> eq, sub
```

Los parámetros “eq” y “sub” indican la coincidencia de búsqueda (equal, substring) a la hora de buscar por ese campo, esta información la da la propia línea de log en las palabras: “bdb\_substring\_candidates” ó “bdb\_equality\_candidates”. Los pasos para crear los índices del ejemplo serían:

Parar el servicio del ldap:

```
$ sudo stop ebox.slapd
```

Añadir los índices adicionales que queremos:

```
$ sudo vi
/etc/ldap/slapd.d/cn\=config/olcDatabase\=\{1\}hdb.ldif
```

...casi al final del fichero encontraremos los índices que hay por defecto:

```
olcDbIndex: objectclass
eq olcDbIndex: entryCSN
eq olcDbIndex: entryUUID
eq olcDbIndex: uid eq
olcDbIndex: memberUid eq
olcDbIndex: uidNumber eq
```





```
olcDbIndex: cn eq
olcDbIndex: gidNumber eq
olcDbIndex: uniqueMember
eq olcDbIndex: sambaSID
eq olcDbIndex:
sambaGroupType eq
olcDbIndex: sambaSIDList
eq olcDbIndex:
sambaDomainName eq
```

...Añadiremos o modificaremos las siguientes líneas:

```
olcDbIndex: uid sub,eq
olcDbIndex: cn sub,eq
olcDbIndex: displayName eq
olcDbIndex: sn sub
```

Grabamos los cambios y actualizamos los índices:

```
$ sudo slapindex
WARNING!
Runnig as root!
There's a fair chance slapd will fail to start.
Check file permissions!
```

Se habrá creado un nuevo fichero con el nombre del índice terminado en ".db" en la ruta "/var/lib/ldap/" al cual hay que corregir los permisos:

```
$ sudo chown openldap:openldap /var/lib/ldap/*
```

Iniciamos el servicio slapd:

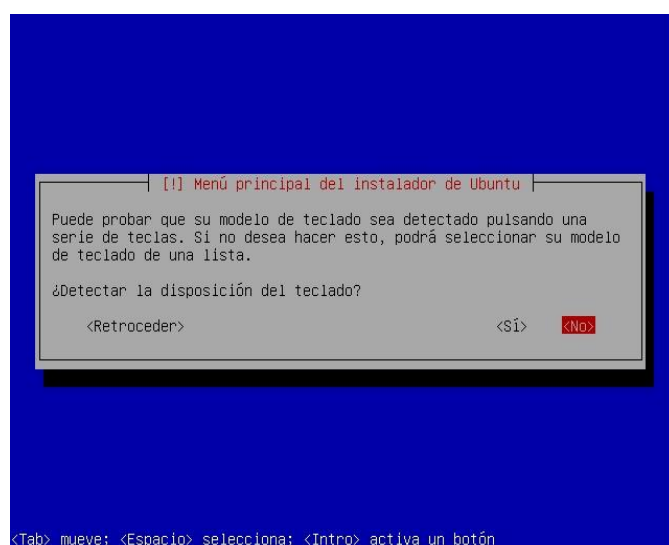
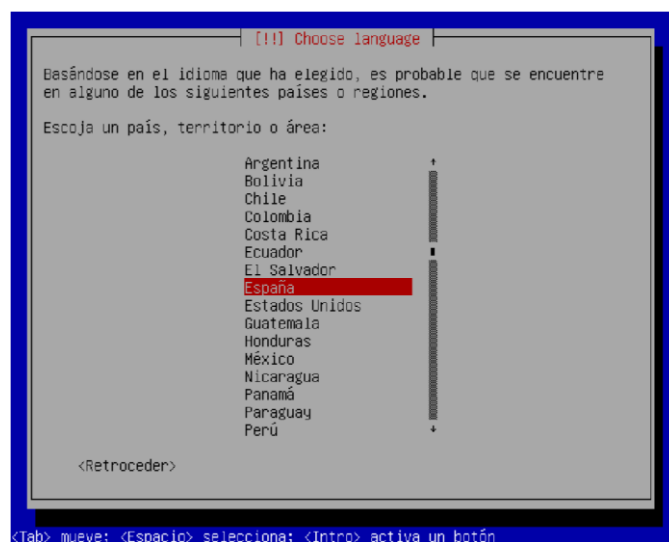
```
$ sudo startebox.slapd
```

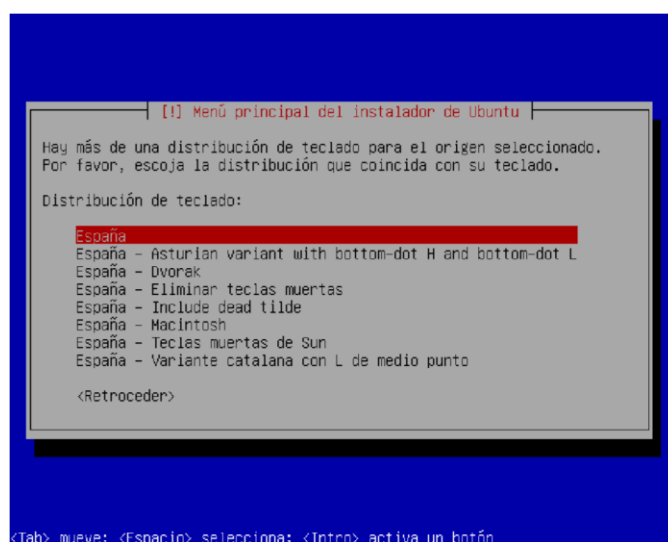
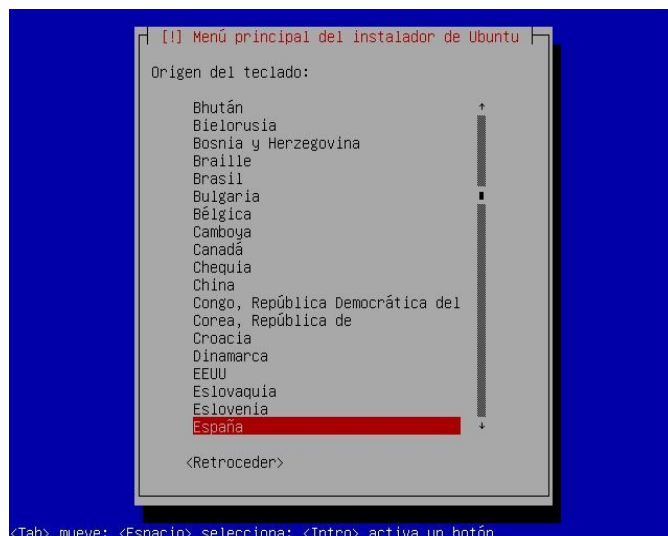
El resto de configuraciones (puerta de enlace, IPs de las interfaces, reglas de firewall, etc.) se explican ya en su sección correspondiente de este manual.

## 5. INSTALACIÓN DESDE CERO

A continuación se muestran los pasos a seguir para instalar “max-server” desde cero. La instalación se ha realizado en VirtualBOX utilizando sólo 4 discos de 2GB(el servidor real consta de de 6 discos de 750GB). Se ha realizado a propósito con 4 discos para comprobar luego cómo se puede ampliar el sistema de 4 a 6 discos.







El servidor tiene dos tarjetas de red. Se puede configurar cualquiera de las dos interfaces y elegir cualquier IP válida aunque sea temporal, teniendo en cuenta que luego nos tenemos que conectar al panel de administración por medio de la interfaz que configuremos utilizando la IP que pongamos aquí. La “eth1” es la interfaz que vamos a utilizar para la red interna así que va a ser la que vamos a configurar con la IP 192.168.10.1:



[[!]] Configurar la red

El sistema tiene varias interfaces de red. Por favor, elija la que quiere utilizar como interfaz de red primaria durante la instalación. Se ha seleccionado la primera interfaz de red conectada si había alguna que lo estaba.

Interfaz de red primaria:

eth0: Intel Corporation 82540EM Gigabit Ethernet Controller  
eth1: Intel Corporation 82540EM Gigabit Ethernet Controller

<Retroceder>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

[[!]] Configurar la red

La dirección IP es única para su ordenador y está formada por cuatro números separados por puntos. Consulte al administrador de red si no sabe qué usar aquí.

Dirección IP:

192.168.10.1

<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

[[!]] Configurar la red

La máscara de red se utiliza para determinar qué sistemas están incluidos en la red. Consulte al administrador de red si no conoce el valor. La máscara de red debería introducirse como cuatro números separados por puntos.

Máscara de red:

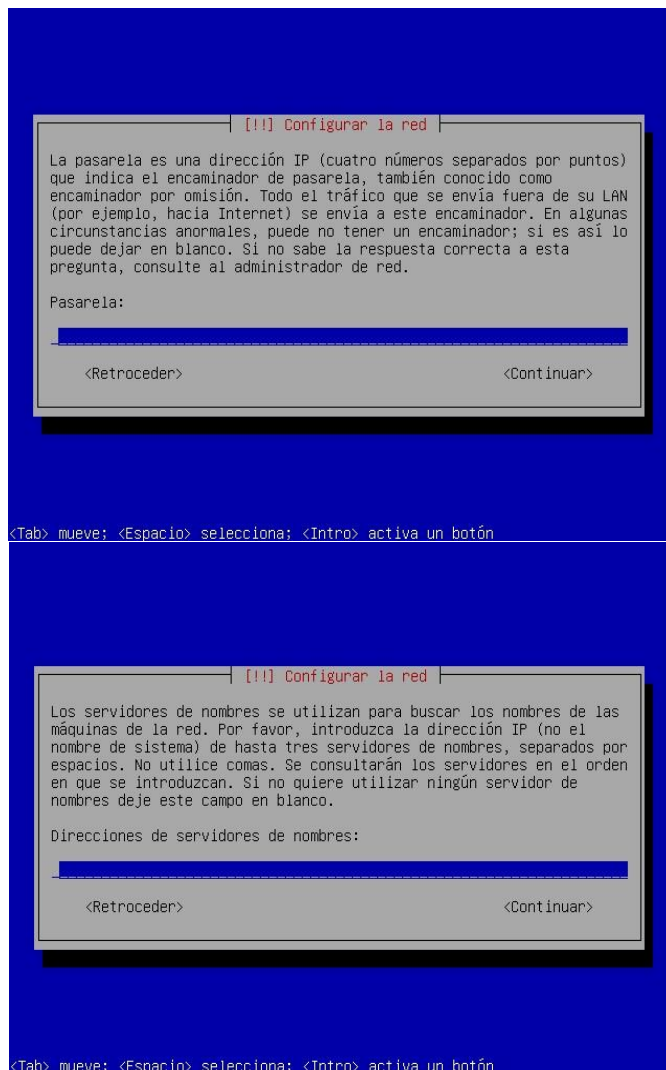
255.255.255.0

<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

Ahora no hace falta poner "pasarela" ni direcciones de servidores de nombres ya que estos datos se configurarán mas tarde por medio del panel de administración web, con poner la IP y la máscara es suficiente para poder conectarnos al servidor:





[!!] Configurar la red

La pasarela es una dirección IP (cuatro números separados por puntos) que indica el encaminador de pasarela, también conocido como encaminador por omisión. Todo el tráfico que se envía fuera de su LAN (por ejemplo, hacia Internet) se envía a este encaminador. En algunas circunstancias anormales, puede no tener un encaminador; si es así lo puede dejar en blanco. Si no sabe la respuesta correcta a esta pregunta, consulte al administrador de red.

Pasarela:

<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

[!!] Configurar la red

Los servidores de nombres se utilizan para buscar los nombres de las máquinas de la red. Por favor, introduzca la dirección IP (no el nombre de sistema) de hasta tres servidores de nombres, separados por espacios. No utilice comas. Se consultarán los servidores en el orden en que se introduzcan. Si no quiere utilizar ningún servidor de nombres deje este campo en blanco.

Direcciones de servidores de nombres:

<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

Llegamos a la parte del particionado. Vamos a explicar antes que tipo de configuración se va a realizar teniendo en mente que queremos que nuestro sistema sea escalable, para esto se utilizará LVM. Tenemos 4 discos de 2 GB, en los que vamos a realizar dos raid 1 con cada pareja de discos. Tenemos entonces dos raid1 de 2GB que ahora queremos unir para aumentar la capacidad total llegando a los 4GB, lo que se conoce como hacer “Data Striping”. Podíamos haber utilizando entonces un raid 10 pero en su lugar vamos a utilizar la capacidad que tiene LVM para proporcionar “Data Striping” aprovechándonos además de las ventajas que ofrece para ampliaciones futuras.

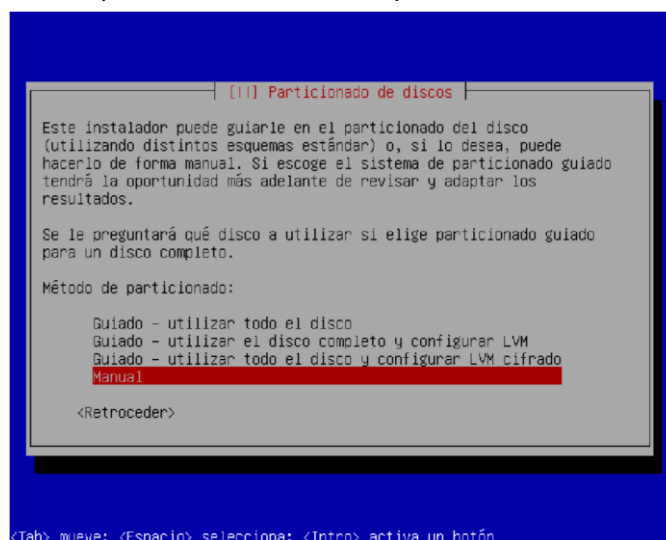
Por tanto, para unir los dos raid1 crearemos un VG(Volumen Group) compuesto por dos PV(Physical Volume), uno por cada raid que hemos creado, de esta manera hemos conseguido sumar el tamaño de las particiones con la ventaja además de que así se aprovecha mejor el espacio de los discos que si hubiéramos decidido hacer raids independientes por cada punto de montaje.





Ahora la forma ideal de ir ampliando el sistema es mediante grupos de dos discos unidos en un raid1, para que de esta manera siempre tengamos redundancia en caso de que falle un disco. En la realidad al VG se podría igualmente añadir un sólo disco independiente, LVM es así de versátil, pero entonces perderíamos la fiabilidad que estamos consiguiendo con los raid1 ya que en caso de que falle ese disco independiente el sistema quedaría totalmente inutilizable.

Comencemos pues la configuración:



Si los discos están vacíos y no tienen ni siquiera tabla de particiones veremos entonces sólo una línea correspondiente por cada disco. Seleccionaremos cada disco y pulsaremos ENTER para crear una tabla de particiones vacía:

```
[!!] Particionado de discos

Éste es un resumen de las particiones y puntos de montaje que tiene
configurados actualmente. Seleccione una partición para modificar sus
valores (sistema de ficheros, puntos de montaje, etc.), el espacio
libre para añadir una partición nueva o un dispositivo para
inicializar la tabla de particiones.

Particionado guiado
Configure iSCSI volumes

SCSI3 (0,0,0) (sda) - 2.1 GB ATA VBOX HARDDISK
SCSI4 (0,0,0) (sdb) - 2.1 GB ATA VBOX HARDDISK
SCSI5 (0,0,0) (sdc) - 2.1 GB ATA VBOX HARDDISK
SCSI6 (0,0,0) (sdd) - 2.1 GB ATA VBOX HARDDISK

Deshacer los cambios realizados a las particiones
Finalizar el particionado y escribir los cambios en el disco

<Retroceder>
```

<F1> para ayuda; <Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

```
[!!] Particionado de discos

Ha seleccionado particionar el dispositivo completo. Si continúa
creará una tabla de particiones en el dispositivo y se eliminarán
todas las particiones que existían previamente.

Observe que podrá deshacer esta operación más adelante si lo desea.

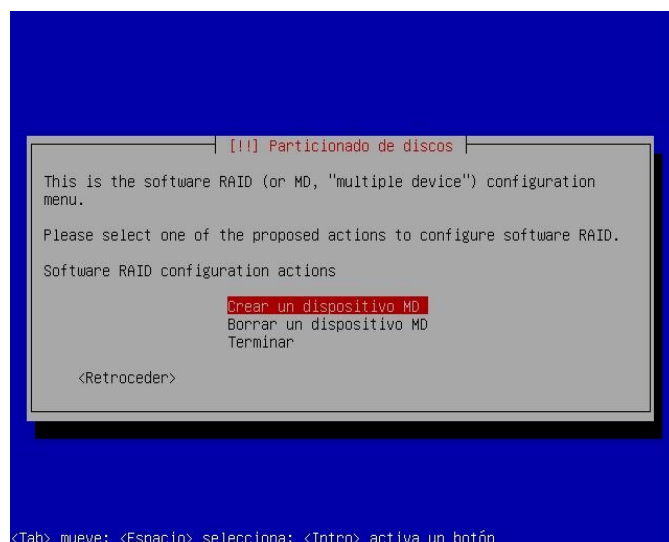
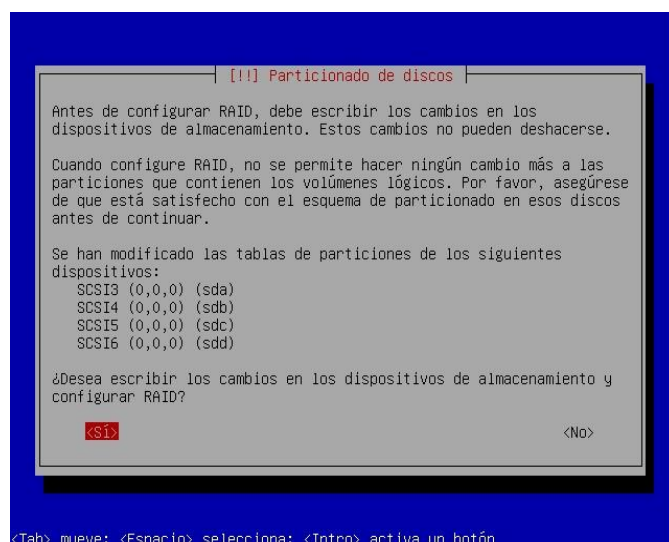
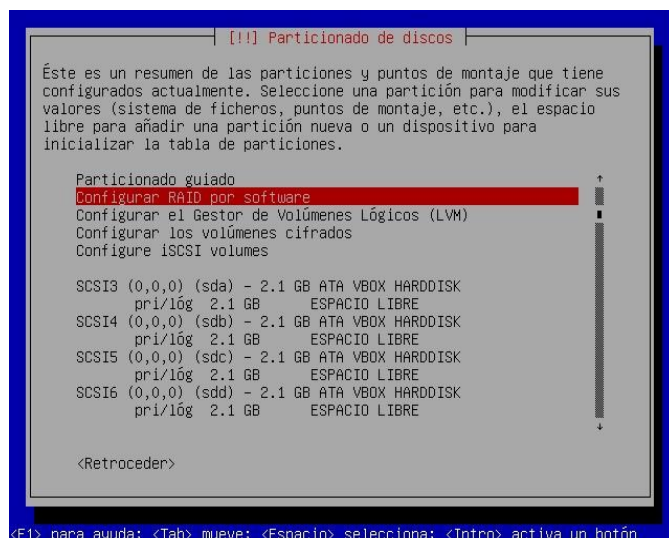
¿Crear una nueva tabla de particiones vacía en este dispositivo?

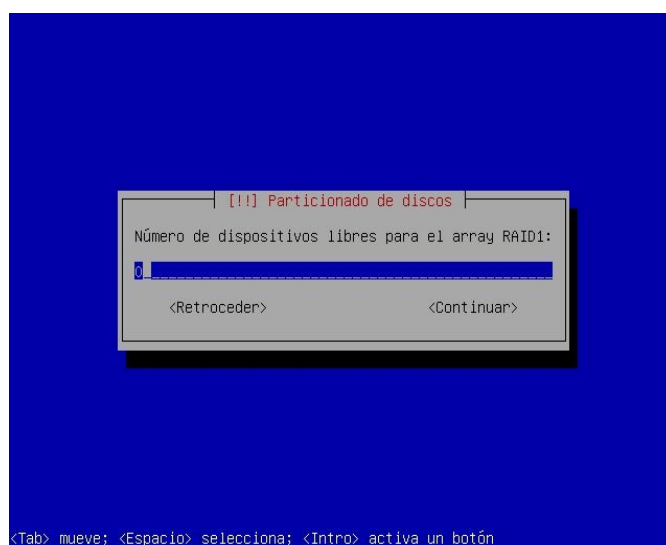
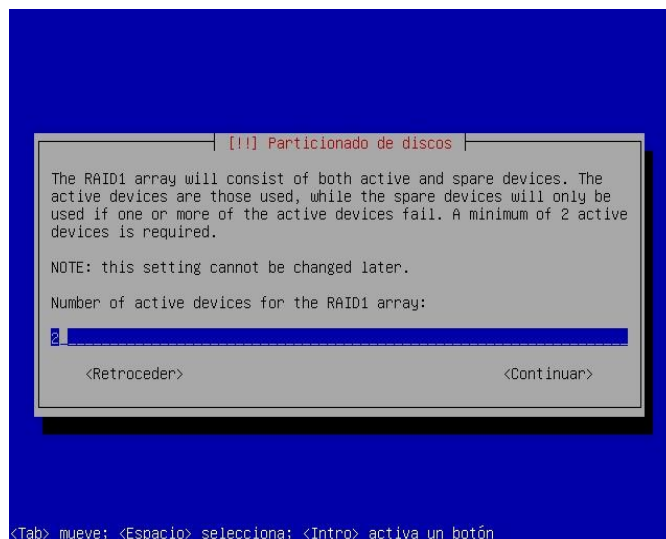
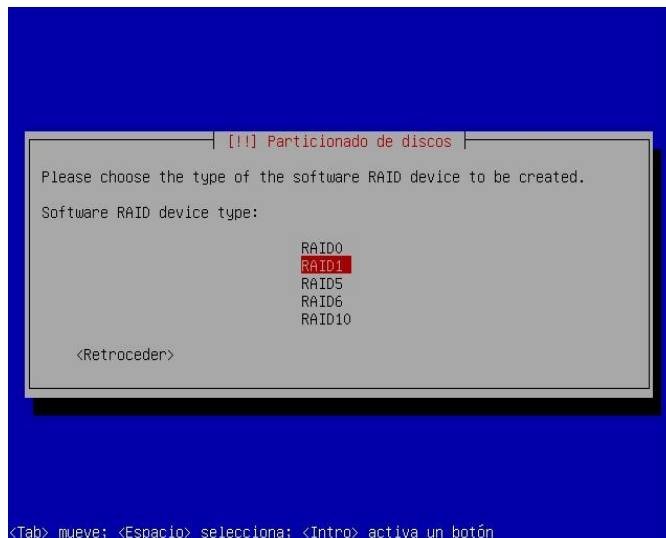
<Retroceder> <Si> <No>
```

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

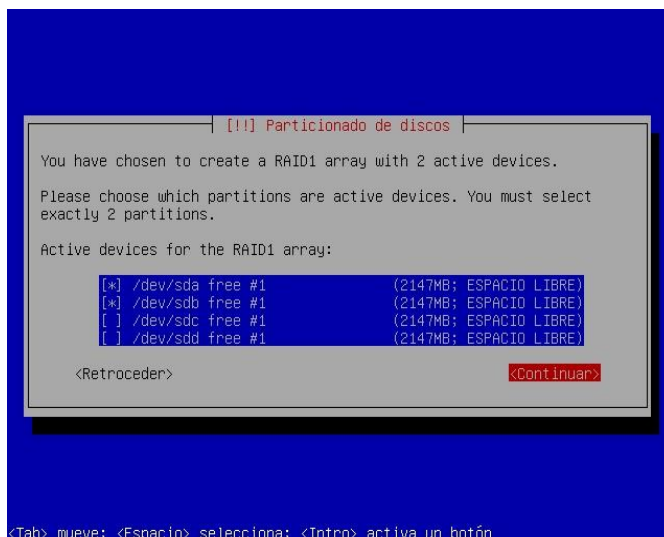
Una vez creadas las tabla de particiones en los 4 discos configuraremos el RAID por software:







Asociamos los raid de forma correlativa de forma que el primer raid esté compuesto por “sda” y “sdb” y el segundo por “sdc” y “sdd”. Es importante saber esta relación sobre todo a la hora de que falle un disco para saber cuando se ponga el disco nuevo con que otro disco lo tenemos que configurar.



Volvemos a realizar los mismos pasos para crear el raid compuesto por “sdc” y “sdd”. Una vez creados los raid elegimos “Terminar” y volvemos a la pantalla inicial del asistente donde podemos ver los dos raids creados. Realmente los raid ahora se están sincronizando, podemos cambiarnos a otro terminal(CTRL+F2) y comprobar la sincronización con “cat /proc/mdstat”:

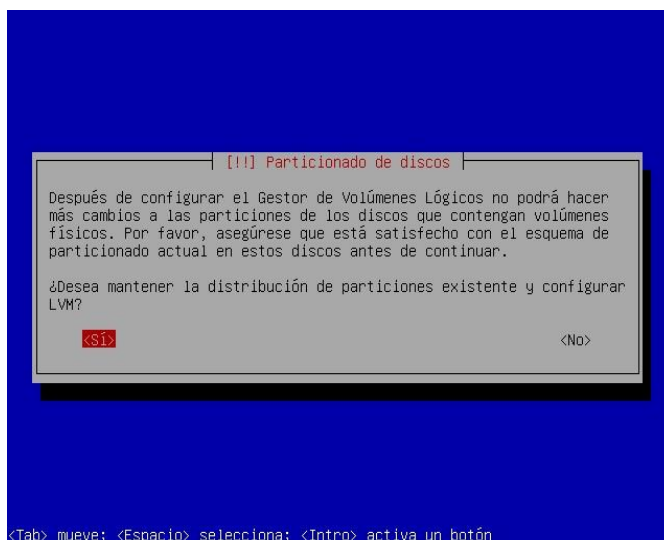
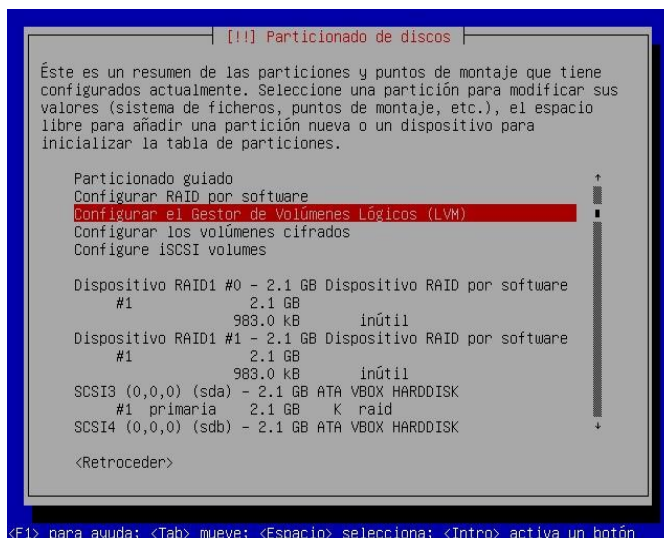
```
# cat /proc/mdstat
Personalities : [raid1]
md1 : active raid1 sdd1[f1] sdc1[f0]
      2096384 blocks [2/2] [UU]
      [==>.....] resync = 11.0% (231616/2096384) finish=1.4min speed=21056K/sec
md0 : active raid1 sdb1[f1] sda1[f0]
      2095040 blocks [2/2] [UU]

unused devices: <none>
#
```

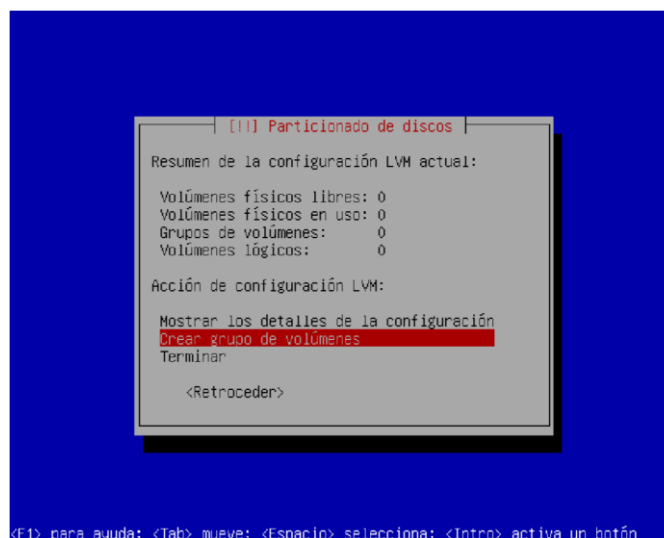
No hace falta que termine la sincronización así que podemos continuar creando ahora el LVM:



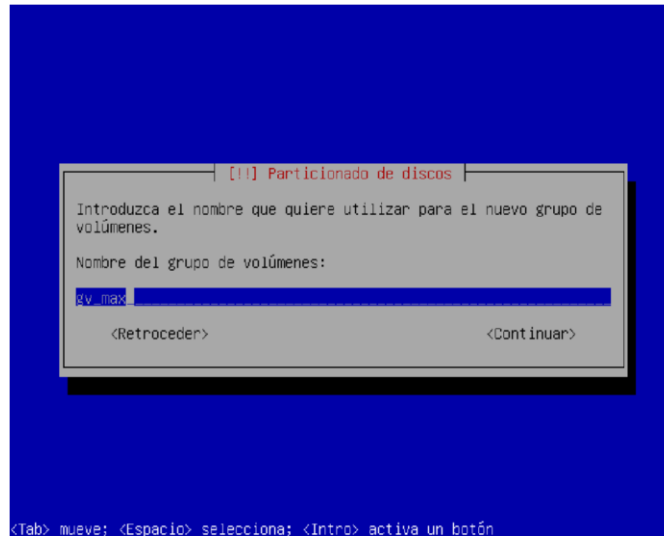




Lo primero que hay que crear(y lo único que nos deja de momento) es un grupo de volúmenes. Un grupo de volúmenes es la “caja” que va a contener los volúmenes físicos(los raid que añadiremos) y los volúmenes(las particiones):

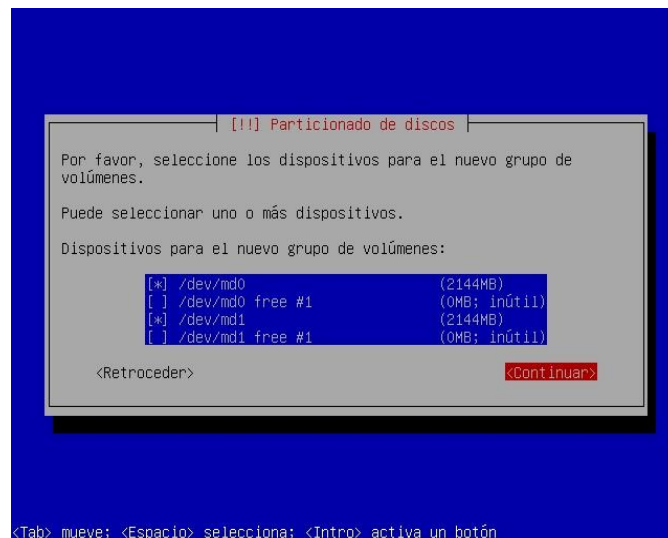


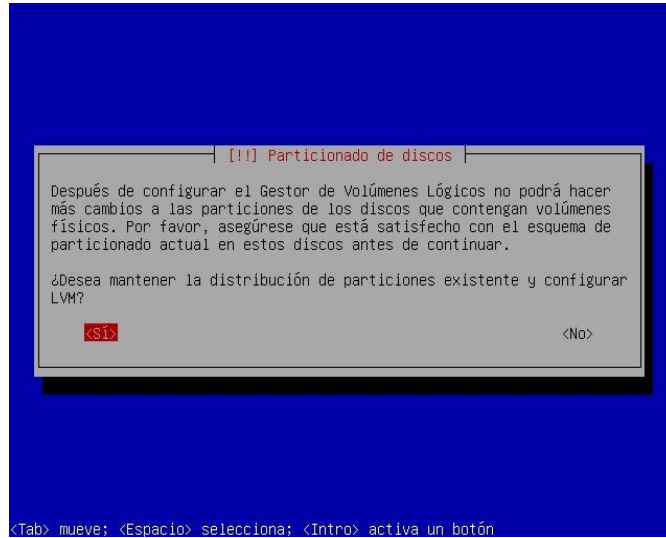
Ponemos como nombre de grupo “gv\_max”:



Una vez creado el grupo, hay que añadir los volúmenes físicos de los que se va a componer, en nuestro caso formado por los dos raid, es decir tendremos 4GB como una unidad lógica disponible para usarlos como queramos, el LVM se encarga de distribuir la información entre los dos raid según le convenga (sigue un algoritmo) y nos abstrae de los medios físicos de los que se compone.

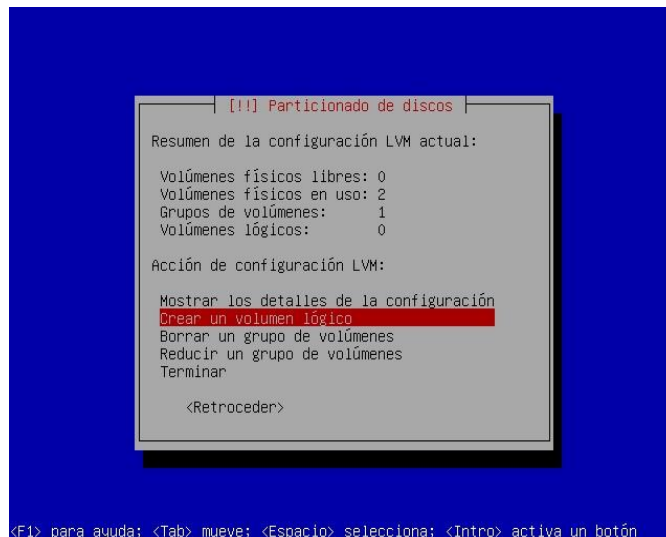
Marcamos los dos dispositivos raid “md” que aparecen:





Una vez que el grupo de volumen ha sido creado y contiene espacio físico(los dos raid1), el asistente ya nos deja crear volúmenes lógicos. Un volumen lógico es lo equiparable a una partición estándar con la que estamos acostumbrados a trabajar.

En nuestro sistema queremos utilizar 3 divisiones, una para la raíz(/) otra para la “swap” y otra para “/home” por ello hay que crear 3 volúmenes lógicos que llamaremos “raíz”, “swap” y “home” respectivamente. Los tamaños serán raíz=2GB, swap=1GB, home=el resto(algo menos de 2GB). Resaltar que en el servidor real se han utilizado para la raíz=50GB, swap=10GB y el resto para “home”(2TB aproximadamente).



[[!]] Particionado de discos

Seleccione uno de los siguientes grupos de volúmenes donde crear un nuevo volumen lógico.

Grupo de Volúmenes:

**sv\_max (4286MB)**

<Retroceder>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

[[!]] Particionado de discos

Introduzca el nombre que desearía utilizar para el nuevo volumen lógico.

Nombre del volumen lógico:

**raiz**

<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

[[!]] Particionado de discos

Introduzca el tamaño del nuevo volumen lógico. El tamaño puede ser introducido en los siguientes formatos: 10K (Kilobytes), 10M (Megabytes), 10G (Gigabytes), 10T (Terabytes). La unidad por omisión es megabytes.

Tamaño de volumen lógico:

**2 GB**

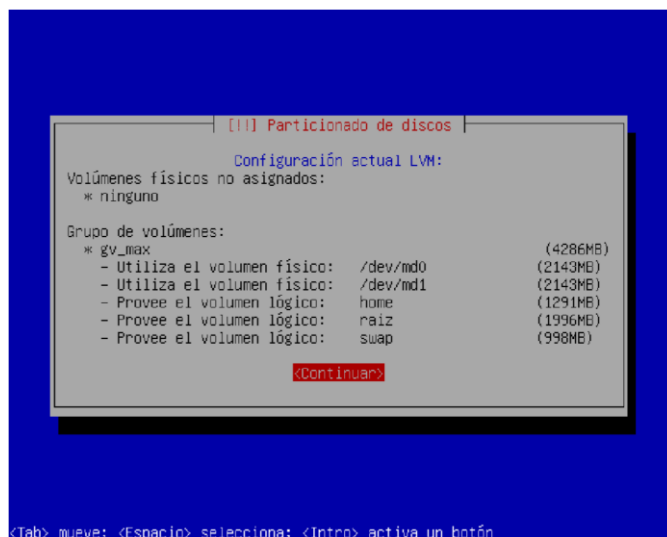
<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

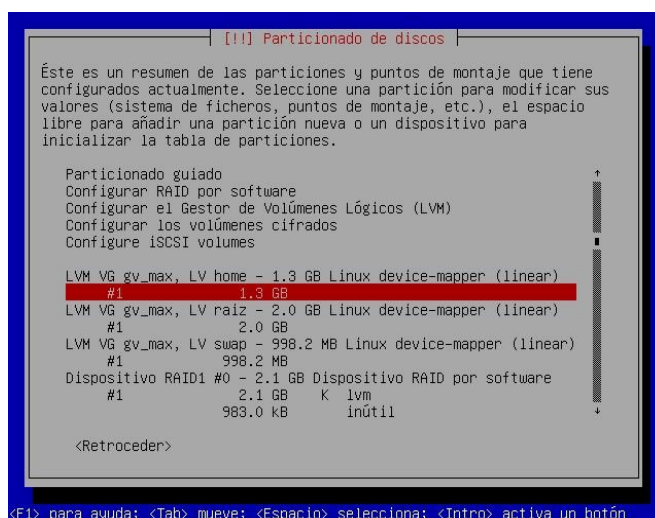


Con esto hemos creado el volumen “raíz”, procedemos igual para crear el de “swap” y luego el de “home”(en ese orden). Para elegir el tamaño de “home” vale con dejar el valor predeterminado que ofrece el asistente que siempre es el máximo disponible.

Una vez creados los volúmenes lógicos podemos elegir la primera opción del menú “Mostrar los detalles de la configuración” y comprobar que vemos algo parecido a la siguiente imagen:



Finalmente, en el menú de LVM pulsamos la opción “Terminar” y volveremos a la pantalla inicial de particionado donde podemos comprobar que ahora vemos los tres volúmenes lógicos que hemos creado de manera que ya los podemos formatear como una partición cualquiera:



Hay que pulsar ENTER en la línea del tamaño, no en la descripción del volumen y accederemos al menú de particionado.





La configuración de la partición “home” debería de quedar así:

```
[!!] Particionado de discos

Está editando la partición #1 de LVM VG gv_max, LV home. No se ha
detectado ningún sistema de ficheros en esta partición.

Configuración de la partición:

Utilizar como:      sistema de ficheros ext4 transaccional

Punto de montaje:   /home
Opciones de montaje: defaults
Etiqueta:           ninguno
Bloques reservados: 5%
Uso habitual:       estándar

Copiar los datos de otra partición
Borrar datos de esta partición:
Se ha terminado de definir la partición

<Retroceder>
```

<F1> para ayuda; <Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

La partición raíz sería

```
[!!] Particionado de discos

Está editando la partición #1 de LVM VG gv_max, LV raíz. No se ha
detectado ningún sistema de ficheros en esta partición.

Configuración de la partición:

Utilizar como:      sistema de ficheros ext4 transaccional

Punto de montaje:   /
Opciones de montaje: defaults
Etiqueta:           ninguno
Bloques reservados: 5%
Uso habitual:       estándar

Copiar los datos de otra partición
Borrar datos de esta partición:
Se ha terminado de definir la partición

<Retroceder>
```

<F1> para ayuda; <Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

Y la partición “swap”:

```
[!!] Particionado de discos

Está editando la partición #1 de LVM VG gv_max, LV swap. No se ha
detectado ningún sistema de ficheros en esta partición.

Configuración de la partición:

Utilizar como:      área de intercambio

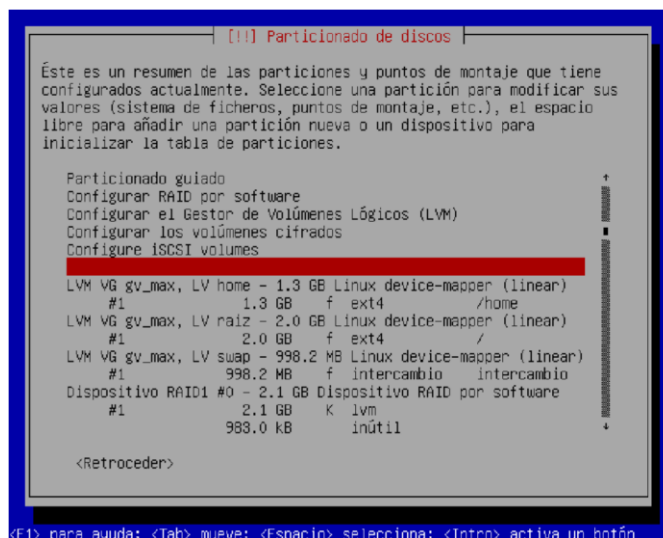
Copiar los datos de otra partición
Borrar datos de esta partición:
Se ha terminado de definir la partición

<Retroceder>
```

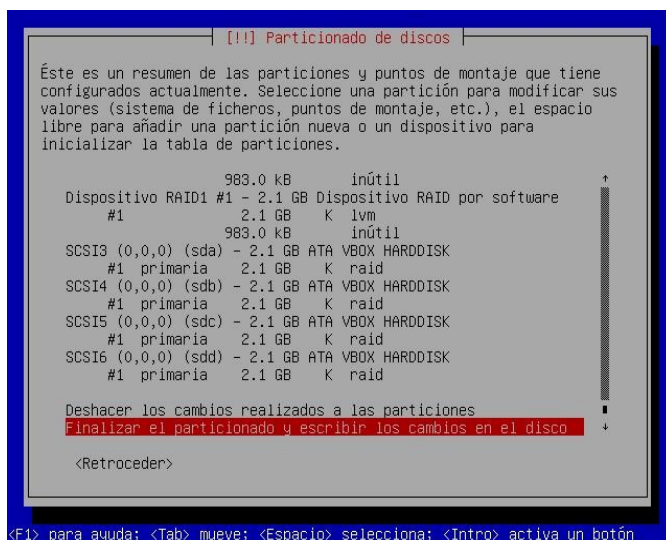
<F1> para ayuda; <Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

Ahora en cada volumen lógico se ven los detalles de cada partición:



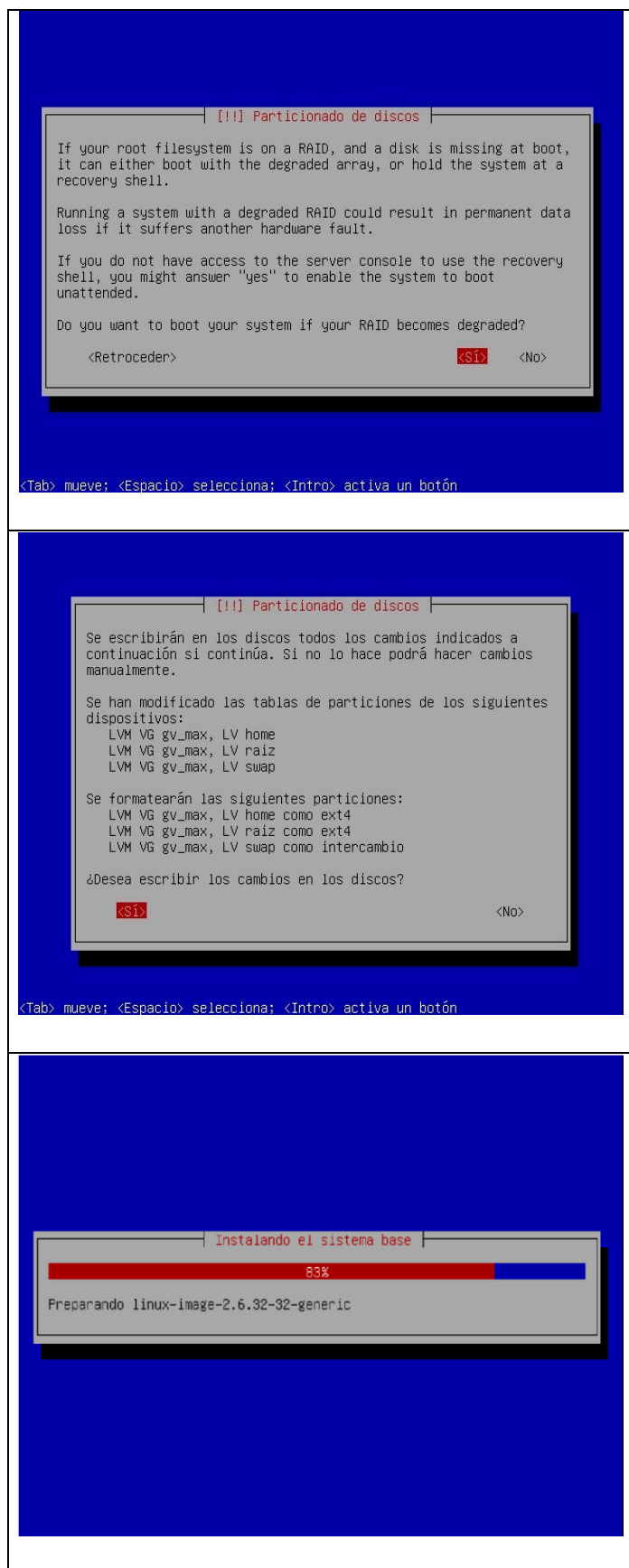


Con esto tenemos el particionado listo, así que pulsamos en “Finalizar...” y continuará la instalación:



El siguiente mensaje da la opción de si se quiere iniciar el sistema en modo degradado en caso de que falle algún disco, le decimos que sí:





De momento no indicamos ningún proxy, lo configuraremos más adelante desde el panel web:

[[!]] Configurar el gestor de paquetes

Si tiene que usar un proxy HTTP para acceder a la red, introduzca a continuación la información sobre el proxy. En caso contrario, déjelo en blanco.

La información del proxy debe estar en el formato  
<http://[usuario][:contraseña]@servidor[:puerto]/>

Información de proxy HTTP (en blanco si no desea usar ninguno):

<Retroceder><Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

Seleccionar e instalar programas

10%

Configurando language-pack-es-base

[[!]] Configuración de grub-pc

Parece que esta instalación es el único sistema operativo en el ordenador. Si esto es así, puede instalar sin riesgos el cargador de arranque GRUB en el registro principal de arranque del primer disco duro.

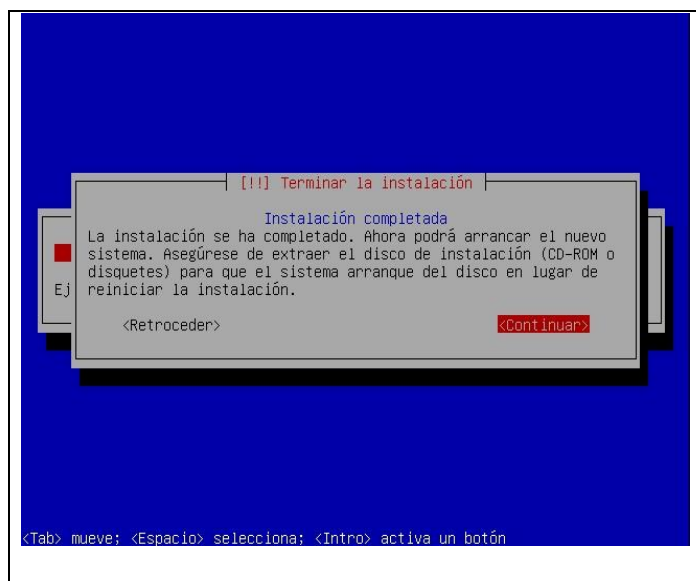
Aviso: Si el instalador no pudo detectar otro sistema operativo instalado en el sistema, la modificación del registro principal de arranque hará que ese sistema operativo no puede arrancarse. Sin embargo, podrá configurar GRUB manualmente más adelante para arrancarlo.

¿Desea instalar el cargador de arranque GRUB en el registro principal de arranque?

<Retroceder><Si><No>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón





Llegados a este punto la instalación ha finalizado y el equipo reiniciará. En el primer inicio configurará los servicios por lo que tardará algo más de lo normal.

El usuario por defecto para iniciar sesión es “madrid” y la contraseña “cmadrid”.

La red estará desactivada por lo que hay que hacer un “ifup eth1” para activar la interfaz que elegimos en la instalación. Una vez vemos con el comando “ifconfig” que aparece la interfaz con la configuración esperada, ya podemos conectarnos al panel web.





## 6. ACTIVAR EL PANEL DE MAX-CONTROL

El panel de max-control se accede por medio de la dirección IP del servidor seguido de la palabra "control". Si el panel no está configurado, la primera vez que se accede informa del procedimiento para su activación tal como muestra la siguiente imagen:



Panel de control de Servidor de Centro

### MAX Control no está configurado.

1. Dentro de EBox / Zentyal cree un usuario con permisos de **administrador**.  
(luego se puede borrar ese usuario desde max-control)

2. Dentro de EBox / Zentyal active los módulos:

- Red
- DHCP
- Compartir ficheros
- Usuarios y grupos
- MAX Control

3. **Reinicie el servidor**

4. Ejecute desde una consola local o por SSH:

```
sudo configure-max-control
```

5. Vuelva a esta página y podrá entrar con cualquier usuario del dominio

## 7. PARTICIONES Y RAID

El servidor de almacenamiento lleva 6 discos duros de 750GB y por cada pareja de discos se ha realizado un raid1 por software con *mdadm*, obteniendo en total tres raid1 y luego se ha utilizado LVM para crear un grupo de volumen compuesto por estos tres raid1. Se muestra la salida de algunos comandos que ofrecen información sobre los discos:

```
root@max-server:/home/madrid# fdisk -l /dev/sda
```

```
Disco /dev/sda: 750.2 GB, 750156374016 bytes
255 cabezas, 63 sectores/pista, 91201 cilindros
Unidades = cilindros de 16065 * 512 = 8225280 bytes
Tamaño de sector (lógico / físico): 512 bytes / 512 bytes
Tamaño E/S (mínimo/óptimo): 512 bytes / 512 bytes Identificador de
disco: 0x00025d61
```



Disposit.	Inicio	Comienzo	Fin	Bloques	Id	Sistema
/dev/sda1	1	91202	732572672	fd	Linux	raid

```
autodetect root@max-server:/home/madrid#
```

En los discos sólo se crea una partición de tipo *raid autodetect* que acapara todo el tamaño, de esta manera se simplifica y no se tiene un raid por cada punto de montaje, por tanto en nuestro caso obtenemos tres raid1:

```
root@max-server:/home/madrid# cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5]
[raid4] [raid10] md2 : active raid1 sdf1[1] sde1[0] 732572608
blocks [2/2] [UU]

md1 : active raid1 sdd1[1] sdc1[0]
732572608 blocks [2/2] [UU]

md0 : active raid1 sdb1[1] sda1[0]
732572608 blocks [2/2] [UU]

unused devices: <none> root@max-server:/home/madrid#
```

Si comprobamos los discos y las particiones asociadas a cada disco que se han detectado vemos que sólo aparece una partición por disco que corresponde a la partición de tipo *raid autodetect*:

```
root@max-server:/home/madrid# ls -l /dev/sd*
brw-rw---- 1 root disk 8, 0 2011-09-07 17:38
/dev/sda brw-rw---- 1 root disk 8, 1 2011-09-07
17:38 /dev/sda1 brw-rw---- 1 root disk 8, 16 2011-
09-07 17:38 /dev/sdb brw-rw---- 1 root disk 8, 17
2011-09-07 17:38 /dev/sdb1 brw-rw---- 1 root disk 8,
32 2011-09-07 17:38 /dev/sdc brw-rw---- 1 root disk
8, 33 2011-09-07 17:38 /dev/sdc1 brw-rw---- 1 root
disk 8, 48 2011-09-07 17:38 /dev/sdd brw-rw---- 1
root disk 8, 49 2011-09-07 17:38 /dev/sdd1 brw-rw--
-- 1 root disk 8, 64 2011-09-07 17:38 /dev/sde brw-
rw---- 1 root disk 8, 65 2011-09-07 17:38 /dev/sde1
brw-rw---- 1 root disk 8, 80 2011-09-07 17:38
/dev/sdf brw-rw---- 1 root disk 8, 81 2011-09-07
17:38 /dev/sdf1 root@max-server:/home/madrid#
```

Ahora veremos la información del LVM. Se ha creado un GV(Grupo de volúmenes) llamado *gv\_max*:

```
root@max-server:/home/madrid# vgdisplay
--- Volume group --- VG Name          gv_max
System ID
Format                lvm2
Metadata Areas        3
Metadata Sequence No  4
VG Access              read/write
VG Status              resizable
MAX LV                0
Cur LV               3
```



```
Open LV      3
Max PV       0
Cur PV      3
Act PV       3
VG Size      2,05 TiB
PE Size      4,00 MiB
Total PE     536550
Alloc PE / Size 536550 / 2,05 TiB
Free PE / Size  0 / 0
VG UUID      s0Kozi-bfRc-vgim-f9tz-xn0h-tfbi-OaKfq9
```

```
root@max-server:/home/madrid#
```

Al grupo de volúmenes se le han añadido los tres raid1, obteniendo como muestra el comando anterior 2,05 TiB de espacio efectivo. El LVM por la naturaleza de su funcionamiento nos ha permitido unir los tres raid1 sin tener que realizar un raid0.

En los tamaños vistos por los comandos vemos que se muestran los valores en TiB, GiB, MiB, etc, lo que significa que están expresados en potencia de 1024. Recordamos que elegimos para el particionamiento 50GB para la raíz, 10GB para swap y el resto para home, pero estos valores han sido tomados como potencia de 1000, si calculamos su valor en potencia de 1024 obtenemos los valores en GiB que son los valores que realmente nos van a mostrar los comandos que vamos a ver más adelante:

50GB = 50.000.000.000 bytes = 46,56612873077393 GiB

10GB = 10.000.000.000 bytes = 9,313225746154785 GiB

En la información de los PV(volúmenes físicos) podemos ver que efectivamente corresponden a los tres raid1 y pertenecen al GV llamado *gv\_max*:



```

root@max-server:/home/madrid# pvdisplay
--- Physical volume --
PV Name
/dev/md0
VG Name          gv_max
PV Size          698,64 GiB / not usable 2,94 MiB
Allocatable      yes (but full)
PE Size          4,00 MiB
Total PE         178850
Free PE          0
Allocated PE     178850
PV UUID          VICMvL-RgEf-nIED-230v-zUIW-3i9O-of7pai

--- Physical volume --
PV Name
/dev/md1
VG Name          gv_max
PV Size          698,64 GiB / not usable 2,94 MiB
Allocatable      yes (but full)
PE Size          4,00 MiB
Total PE         178850
Free PE          0
Allocated PE     178850
PV UUID          KUaxeP-sCZA-vVzl-RWtr-M1j6-pGqj-fOI07V

--- Physical volume --
PV Name
/dev/md2
VG Name          gv_max
PV Size          698,64 GiB / not usable 2,94 MiB
Allocatable      yes (but full)
PE Size          4,00 MiB
Total PE         178850
Free PE          0
Allocated PE     178850
PV UUID          yfOPUw-Kj3o-PwcM-kCgS-ocix-WkOH-txhfx3
root@max-server:/home/madrid#
  
```

En el espacio global de los 2,05Tib obtenido con el LVM es donde se han creado tres VL(volúmenes lógicos) correspondientes a nuestra estructura de particiones que son la *raíz*, *swap* y *home*:

```

root@max-server:~# lvm lvscan
ACTIVE          '/dev/gv_max/raiz' [46,56 GiB] inherit
ACTIVE          '/dev/gv_max/swap' [9,31 GiB] inherit  ACTIVE
'/dev/gv_max/home' [1,99 TiB] inherit root@max-server:~#
  
```

Al crear los tres volúmenes lógicos se crean sus tres nombres de dispositivo en la ruta */dev/gv\_max* y ahora ya podemos trabajar con ellos como si se trataran de **particiones** físicas reales. Estos tres nombres de dispositivo son realmente tres enlaces a los nombres correspondientes de la ruta */dev/mapper*.



La información de los volúmenes lógicos muestra entre otros datos, cual es el nombre de su dispositivo, el grupo de volumen al que pertenece y el tamaño de la partición:

```

root@max-server:/home/madrid# lvdisplay
--- Logical volume ---
LV Name                /dev/gv_max/raiz
VG Name                gv_max
LV UUID                o9ileA-PtHv-QNHv-XuzH-NjoP-g7iw-cHwmni
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                46,56 GiB
Current LE             11920
Segments               1
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           251:0

--- Logical volume ---
LV Name                /dev/gv_max/swap
VG Name                gv_max
LV UUID                7DmmKL-ZxyJ-oKzA-VfKD-baqy-RKrc-jnMjXy
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                9,31 GiB
Current LE             2384
Segments               1
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           251:1

--- Logical volume ---
LV Name                /dev/gv_max/home
VG Name                gv_max
LV UUID                X2HK3a-nd0J-jUuO-Hsvz-DFDA-J9QI-v3n9eB
LV Write Access        read/write
LV Status              available
# open                 1
LV Size                1,99 TiB
Current LE             522246
Segments               3
Allocation             inherit
Read ahead sectors     auto
- currently set to     256
Block device           251:2

root@max-server:/home/madrid#
  
```

Podemos obtener información detallada sobre el tamaño de las particiones y el espacio usado con el comando **df**:



```
root@max-server:/home/madrid# df

S.ficheros      Bloques de 1K  Usado   Dispon Uso% Montado en
/dev/mapper/gv_max-raiz
48057224 2240860 43375148 5% /
none          1939372    272 1939100 1%
/dev none      1944352     0 1944352 0%
/dev/shm none   1944352    956
1943396 1% /var/run none      1944352
0 1944352 0% /var/lock
none          1944352     0 1944352 0% /lib/init/rw
/dev/mapper/gv_max-home
2105553320 210980 1998386360 1% /home root@max-
server:/home/madrid#
```

El comando *mount* nos mostrará donde se ha montado cada partición:

```
root@max-server:/home/madrid# mount
/dev/mapper/gv_max-raiz on / type ext4
(rw,errors=remount-ro) proc on /proc type proc
(rw,noexec,nosuid,nodev) none on /sys type sysfs
(rw,noexec,nosuid,nodev) none on /sys/fs/fuse/connections
type fusectl (rw) none on /sys/kernel/debug type debugfs
(rw) none on /sys/kernel/security type securityfs (rw) none
on /dev type devtmpfs (rw,mode=0755)
none on /dev/pts type devpts
(rw,noexec,nosuid,gid=5,mode=0620) none on /dev/shm type
tmpfs (rw,nosuid,nodev) none on /var/run type tmpfs
(rw,nosuid,mode=0755) none on /var/lock type tmpfs
(rw,noexec,nosuid,nodev) none on /lib/init/rw type tmpfs
(rw,nosuid,mode=0755)
/dev/mapper/gv_max-home on /home type ext4 (rw,usrquota,grpquota,acl)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc
(rw,noexec,nosuid,nodev) root@max-server:/home/madrid#
```

El comando *df* y *mount* no muestran información sobre la swap, para ello podemos utilizar el comando “*swapon -s*”:

```
root@max-server:~# swapon -s

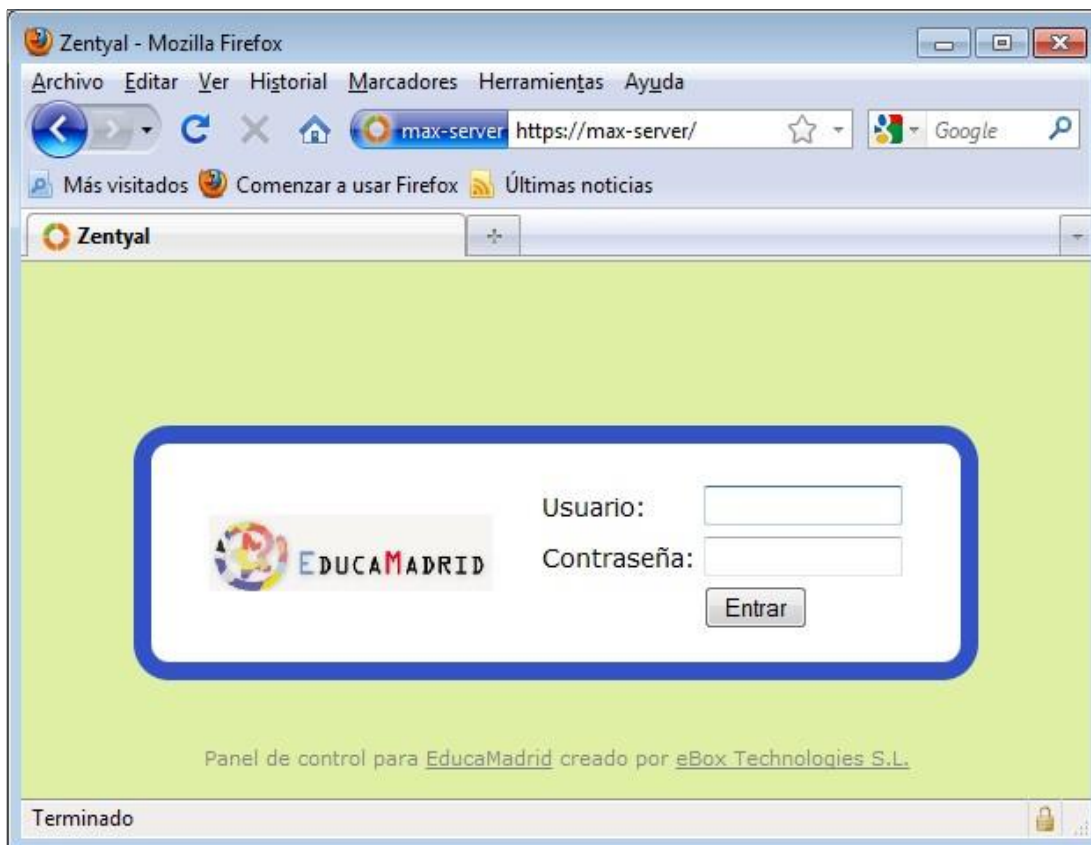
Filename      Type      Size  Used  Priority
/dev/mapper/gv_max-swap      partition 9764856 0      -1
root@max-server:~#
```

## 8. ACCESO AL PANEL DE ADMINISTRACIÓN WEB

Desde un navegador *Firefox* (Evitar *Internet Explorer* ya que no es compatible al 100% con el panel web) acceder a la dirección <https://max-server> o directamente por IP si la conocemos, generalmente <https://192.168.10.1>. Aparecerá una pantalla en la que se solicita usuario y contraseña, por defecto es “madrid” y “cmadrid” respectivamente:







El panel de administración es una aplicación web que ayuda a configurar de forma remota los servicios principales del servidor. Siempre habrá configuraciones que no se puedan realizar por medio del panel, siendo necesario ir por consola a los ficheros de configuración correspondientes, el problema es que cualquier modificación realizada directamente en los ficheros, es sobrescrita si luego se realiza algún cambio por medio del panel, ya que este se basa en unas plantillas a las que añade la configuración realizada en el panel y no tiene en cuenta los cambios manuales que se realicen en la configuración de los propios ficheros de los servicios.

En estos casos, para poder realizar configuraciones que no contempla el panel, toca modificar directamente las plantillas en las que este se basa. Las plantillas se ubican en la ruta “/usr/share/zentyal/stubs”:

```
root@max-server:~# ls /usr/share/zentyal/stubs/
antivirus  core dns  network printers remoteservices squid
ca         css      ftp      ntp      quagga  samba    trafficshaping
captiveportal dhcp     monitor  openvpn  radius   software
usercorner root@max-server:~#
```

La pantalla inicial que aparece al iniciar sesión es el “dashboard”, contiene un resumen del estado del servidor:



EDUCAMADRID

Cerrar sesión
Guardar cambios

Dashboard

[Configurar widgets](#)

**Información general**

Hora	lun oct 3 14:32:08 CEST 2011
Nombre de máquina	max-server
Versión de la plataforma	2.1.29
Software	<b>2 actualizaciones de seguridad</b>
Carga del sistema	0.02, 0.06, 0.05
Tiempo de funcionamiento sin interrupciones	25 days, 20:53
Usuarios	2

**Recursos y Servicios**

<b>Recursos de la comunidad</b> <a href="#">Suscripción Básica GRATIS</a> <a href="#">Documentación</a> <a href="#">Foro</a> <a href="#">Reportar un bug</a> <a href="#">Cómo contribuir</a>	<b>Suscripciones &amp; Servicios</b> <a href="#">Suscripciones Comerciales</a> <a href="#">Soporte Comercial</a> <a href="#">Zentyal Cloud</a> <a href="#">Formación Certificada</a> <a href="#">Tienda Online</a>
---	---

**Zentyal Cloud**

Nombre del Servidor	Ninguno
Estado de la conexión	No suscrito - <a href="#">¡Suscríbete ahora!</a>
Suscripción del Servidor	Ninguna - <a href="#">Consigue una Suscripción Básica gratuita</a>
Soporte Técnico	Deshabilitado - <a href="#">Habilitar</a>
Actualizaciones de Seguridad Avanzadas	Deshabilitado - <a href="#">Habilitar</a>
Recuperación de Desastres	Desactivado - <a href="#">Activar</a>

**Estado de los Módulos**

Red	Ejecutándose	
Cortafuegos	Ejecutándose	
Antivirus	Ejecutándose sin ser gestionado	
Apache	Ejecutándose	
Autoridad de certificación	No creada	
Portal Cautivo	Ejecutándose	<a href="#">Reiniciar</a>
DHCP	Ejecutándose	<a href="#">Reiniciar</a>
DNS	Ejecutándose	<a href="#">Reiniciar</a>
Copia de seguridad	Deshabilitado	
Eventos	Deshabilitado	
FTP	Deshabilitado	
Registros	Deshabilitado	
Monitorización	Deshabilitado	
NTP	Ejecutándose	<a href="#">Reiniciar</a>
VPN	Deshabilitado	
Compartir Impresoras	Ejecutándose sin ser gestionado	
RADIUS	Deshabilitado	
Cliente de Zentyal Cloud	No suscrito	
Compartir ficheros	Ejecutándose	<a href="#">Reiniciar</a>
Proxy HTTP	Deshabilitado	
Moldeado de tráfico	Ejecutándose	<a href="#">Reiniciar</a>
Rincón del Usuario	Ejecutándose	<a href="#">Reiniciar</a>
Usuarios y Grupos	Ejecutándose	
Servidor Web	Ejecutándose sin ser gestionado	

**Usuarios por directorio compartido**

**Interfases de Red**

▼ eth0

Estado	activado, externo, enlace ok
Dirección MAC	e0:cb:4e:42:dc:07
Dirección IP	10.111.20.5

Bytes Tx

Bytes Rx

▼ eth1

Estado	activado, interno, enlace ok
Dirección MAC	00:27:19:b1:7b:d5
Dirección IP	192.168.10.1

Bytes Tx

Bytes Rx

**IPs asignadas con DHCP**

Dirección IP	Dirección MAC	Nombre de máquina
192.168.10.201	40:61:86:93:01:0e	

**Directorios compartidos por usuario**

**Demonios OpenVPN**

Panel de control para EducaMadrid creado por eBox Technologies S.L.

Desde esta pantalla podemos conocer información interesante como el tiempo que lleva el servidor encendido, los usuarios conectados, las IPs asignadas por el servicio DHCP, el estado de las interfaces de red, etc.

## 9. ESTADO DE LOS MÓDULOS

El nombre de esta pantalla puede dar a confusión ya que realmente no es para ver si el servicio ó módulo esta ejecutándose. Para lo que sirve es para activar/desactivar los módulos que se desean utilizar, ya que por ejemplo podemos habilitar el módulo DNS, pero si ocurre



algún fallo puede que este no se inicie. Para ver entonces realmente el estado del servicio se utilizaría la pantalla del “dashboard” o mediante comandos a través de una consola:

Configuración del estado de los módulos			
	Módulo	Depende	Estado
Core			
Dashboard			
Estado del módulo	Red		<input checked="" type="checkbox"/>
Sistema	Cortafuegos	Red	<input checked="" type="checkbox"/>
Red	DHCP	Red	<input checked="" type="checkbox"/>
Objetos	DNS		<input checked="" type="checkbox"/>
Servicios	Eventos		<input type="checkbox"/>
Registros	Registros		<input type="checkbox"/>
Eventos	NTP		<input checked="" type="checkbox"/>
Gateway	VPN	Red	<input type="checkbox"/>
Proxy HTTP	Moldeado de tráfico	Red, Cortafuegos	<input type="checkbox"/>
Moldeado de tráfico	Usuarios y Grupos		<input checked="" type="checkbox"/>
UTM	Backharddi NG	DHCP	<input checked="" type="checkbox"/>
Cortafuegos	Compartir ficheros	Red, Usuarios y Grupos	<input checked="" type="checkbox"/>
VPN	Proxy HTTP	Cortafuegos, Usuarios y Grupos	<input type="checkbox"/>
Infrastructure	Rincón del Usuario	Usuarios y Grupos	<input type="checkbox"/>
DHCP	MAX Control	Red, DHCP, Compartir ficheros, Usuarios y Grupos	<input checked="" type="checkbox"/>
DNS	Compartir Impresoras	Compartir ficheros	<input type="checkbox"/>
Autoridad de certificación			
Backharddi NG			
MAX Control			
Office			
Usuarios y Grupos			
Rincón del Usuario			
Compartir ficheros			
Compartir Impresoras			

Podemos acceder de antemano a la configuración de un módulo en su sección correspondiente pero el módulo no funcionará hasta que esté habilitado en este panel.

## 10. CONFIGURACIÓN GENERAL

En esta ficha se puede configurar la contraseña del usuario(madrid), el idioma de la interfaz, zona horaria, puerto de administración y el nombre del servidor.



The screenshot shows the 'Configuración General' (General Configuration) page. The left sidebar has a menu with categories: Core, Red, Mantenimiento, Gestión de software, Suscripción, Gateway, UTM, and Infrastructure. Under 'Core', the 'General' option is highlighted with a red circle. The main content area is titled 'Configuración General' with a link '(mostrar ayuda)'. It contains several sections: 'Cambiar contraseña' (Change password) with fields for 'Usuario', 'Contraseña actual', 'Nueva contraseña', and 'Confirmar contraseña', and a 'Cambiar' button; 'Selección de idioma' (Language selection) with a dropdown set to 'Español' and a 'Cambiar' button; 'Zona Horaria' (Time zone) with dropdowns for 'Europe' and 'Madrid', and a 'Cambiar' button; 'Fecha y Hora' (Date and Time) with dropdowns for 'Fecha' (17 / Enero / 2012) and 'Hora' (12 / 48 / 39), and a 'Cambiar' button; 'Puerto TCP de la interfaz de administración' (TCP port of the administration interface) with a text box containing '443' and a 'Cambiar' button; and 'Cambiar nombre de la máquina' (Change machine name) with a text box containing 'max-server' and a 'Cambiar' button.

NOTA: Si se intenta modificar la hora desde el panel de EBOX, al pulsar el botón [Cambiar] se muestra una página en blanco sin ninguna información, pero la hora queda correctamente cambiada. Desde la consola se puede cambiar la hora con el siguiente comando: `date --set "2012-12-30 16:25"`

## 11. CONFIGURACIÓN DE RED

La IP de la interface eth0 es distinta en cada centro. Es la que se ha utilizado para dar salida a internet por lo que físicamente estará conectada al router ADSL o en una MACROLAN a una toma perteneciente a la VLAN100:





Interfaces de Red (mostrar ayuda)

eth0 eth1

Nombre: eth0

Método: Estático

Externo (WAN): ☒ Marque aquí si está usando Zentyal como gateway y este interfaz está conectado a su router a Internet

Dirección IP: 10.111.20.5

Máscara de red: 255.255.255.0

Cambiar

Interfaces Virtuales

Nombre	Dirección IP	Máscara de red	Acción
		255.255.255.0	+

NOTA: Si se tiene problemas para cambiar la IP de la interface eth0, eliminar la puerta de enlace, guardar cambios y volver a intentarlo. Después volver a añadir la puerta de enlace.

La interface eth1, es la que se conecta a la red de trabajo de alumnos y profesores, físicamente va conectada una toma de la VLAN110. A esta red se le asigna el rango de IPs 192.168.10.X, siendo la puerta de enlace el propio servidor al cual se le asigna la IP 192.168.10.1:



Network Interfaces (mostrar ayuda)

eth0 eth1 eth2

Nombre: eth1

Método: Estático

External (WAN): ☐ Check this if you are using eBox as a gateway and this interface is connected to your Internet router.

Dirección IP: 192.168.10.1

Máscara de red: 255.255.255.0

Cambiar

Interfaces Virtuales

Nombre	Dirección IP	Máscara de red	Acción
		255.255.255.0	+

La configuración de los interfaces se puede comprobar por consola visualizando el fichero “/etc/network/interfaces”:

```
madrid@max-server:~$ cat /etc/network/interfaces auto lo eth0 eth1
```

```
iface lo inet loopback
iface eth0 inet static
address 10.111.20.5
netmask
255.255.255.0
broadcast
10.111.20.255
gateway 10.111.20.1
```

```
iface eth1 inet static
address 192.168.10.1
netmask 255.255.255.0
broadcast
```

```
192.168.10.255  
madrid@max-server:~$
```

NOTA: Cualquier configuración realizada en este fichero se perderá cuando se actualice la configuración a través del panel de administración web.

En la siguiente fotografía se indica que etiqueta corresponde a la interface física del equipo:

Realmente el orden de asignación puede ser cualquier otro siempre que el cable de red vaya a la interfaz correcta, pero para unificar la configuración todos los servidores se configuran con el orden mostrado en la foto.

Para ver como asignar una etiqueta a una interfaz concreta se puede consultar el apartado “[Cambio de una interfaz de red](#)”.

## 12. CONFIGURACIÓN DE DNS

En el apartado DNS se especifican los servidores para la resolución de nombres. En la imagen se observa que tiene como servidor primario a sí mismo y el de la macrolan:





Traductor de Servidores de Nombres de Dominio [\(mostrar ayuda\)](#)

Lista de traductores de servidores de nombres de dominio

+ Añadir nuevo/a

Buscar

Servidor de nombres de dominio	Acción
127.0.0.1	
213.0.88.85	

10 Página 1

Dominio de búsqueda

Dominio:   
 Opcional

Cambiar

### 13. CONFIGURACIÓN DE LA PUERTA DE ENLACE

Hay que añadir la puerta de enlace que nos da salida a internet. Debe estar en concordancia con la IP de la interface *eth0*:

Configuración de Puertas de Enlace [\(mostrar ayuda\)](#)

[Puertas de enlace y Proxy](#)
[Balanceo de tráfico](#)
[WAN failover](#)

Lista de Puertas de Enlace

+ Añadir nuevo/a

Buscar

Habilitado	Nombre	Dirección IP	Interfaz	Peso	Predeterminado	Acción
<input checked="" type="checkbox"/>	macrolan	10.111.20.1	eth0	1		

10 Página 1

Proxy

Usuario:   
 Opcional

Contraseña:   
 Opcional

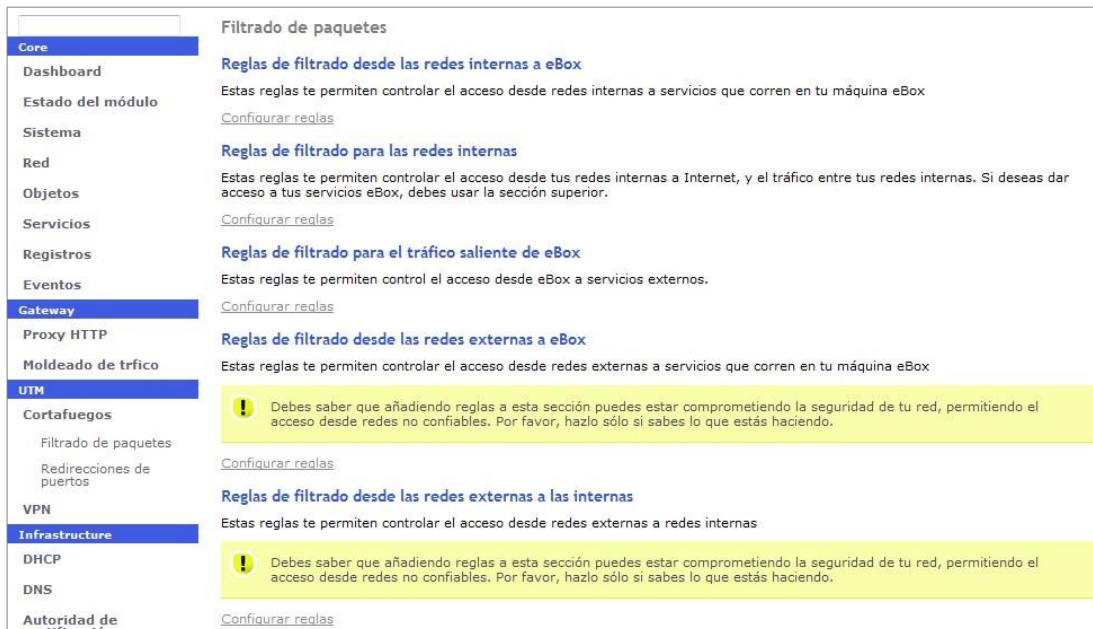
Servidor proxy:   
 Opcional

Puerto del proxy:

Cambiar

## 14. CORTAFUEGOS

El “Cortafuegos” dispone de distintas secciones para crear reglas según la dirección del tráfico entre redes:



**Filtrado de paquetes**

**Reglas de filtrado desde las redes internas a eBox**  
Estas reglas te permiten controlar el acceso desde redes internas a servicios que corren en tu máquina eBox.  
[Configurar reglas](#)

**Reglas de filtrado para las redes internas**  
Estas reglas te permiten controlar el acceso desde tus redes internas a Internet, y el tráfico entre tus redes internas. Si deseas dar acceso a tus servicios eBox, debes usar la sección superior.  
[Configurar reglas](#)

**Reglas de filtrado para el tráfico saliente de eBox**  
Estas reglas te permiten control el acceso desde eBox a servicios externos.  
[Configurar reglas](#)

**Reglas de filtrado desde las redes externas a eBox**  
Estas reglas te permiten controlar el acceso desde redes externas a servicios que corren en tu máquina eBox.

**Reglas de filtrado desde las redes externas a las internas**  
Estas reglas te permiten controlar el acceso desde redes externas a redes internas.  
[Configurar reglas](#)

**UTM**

**Cortafuegos**

Filtrado de paquetes

Redirecciones de puertos

**VPN**

**Infrastructure**

DHCP

DNS

Autoridad de certificación

Estas son las “Reglas de filtrado desde las redes internas a eBox”:

**Filtrado de paquetes** > Desde redes internas hacia Zentyal

**Configure Rules**

[+ Añadir nuevo/a](#)

Decisión	Origen	Servicio	Descripción	Acción
↑	Cualquiera	ssh	ssh	
↑	Cualquiera	Administración de Zentyal	Administracion zentyal	
↑	Cualquiera	http	--	
↑	Cualquiera	ldap	--	
↑	Cualquiera	usercorner	--	
↑	Cualquiera	samba	--	
↑	Cualquiera	RADIUS	--	
↑	Cualquiera	ipp	--	
↑	Cualquiera	ntp	--	
↑	Cualquiera	FTP	--	
↑	Cualquiera	dns	--	
↑	Cualquiera	dhcp	--	
↑	Cualquiera	tftp	--	

15



En la sección “Desde redes externas hacia eBOX”, se crearán como mínimo las dos reglas que permiten el acceso al servidor para su administración, que son acceso por “ssh” y el acceso al panel de administración EBOX, esta sería su configuración:

Filtrado de paquetes ▶ Desde redes externas hacia eBox	Filtrado de paquetes ▶ Desde redes externas hacia eBox
<p><b>Añadiendo una nueva regla</b></p> <p>Decisión: <input type="button" value="ACCEPT"/></p> <p>Origen: <input type="button" value="IP origen"/> 10.111.20.0 / 24</p> <p>Servicio: <input type="button" value="ssh"/> Inverse match: <input type="checkbox"/></p> <p><small>Si la selección inversa está marcada, la regla será aplicada</small></p> <p>Descripción: <input type="text" value="Permitir SSH"/> <i>Opcional</i></p> <p><input type="button" value="Añadir"/> <input type="button" value="Cancelar"/></p>	<p><b>Añadiendo una nueva regla</b></p> <p>Decisión: <input type="button" value="ACCEPT"/></p> <p>Origen: <input type="button" value="IP origen"/> 10.111.20.0 / 24</p> <p>Servicio: <input type="button" value="eBox administration"/> Inverse match: <input type="checkbox"/></p> <p><small>Si la selección inversa está marcada, la regla será aplicada</small></p> <p>Descripción: <input type="text" value="Permitir administr"/> <i>Opcional</i></p> <p><input type="button" value="Añadir"/> <input type="button" value="Cancelar"/></p>

Opcionalmente también crearemos las siguientes reglas:

- Acceso al panel de max-control, corresponde al Servicio “http”.

Filtrado de paquetes ▶ Desde redes externas hacia Zentyal

**Editando regla**

Decisión:

Origen:  10.111.20.0 / 24

Servicio:  Coincidencia inversa: ☐

Si la selección inversa está marcada, la regla será aplicada cualquier

Descripción:  *Opcional*



- Permitir la respuesta al ping desde el exterior. Por defecto el servidor no responde a un ping realizado a la interfaz WAN, para permitir este tráfico primero hay que crear el servicio “ping-icmp” en “Red > Servicios” y configurarlo con el protocolo ICMP, luego ya podemos añadir la regla para este servicio:

**Servicios > ping-icmp**

**Editando servicio**

Protocolo:

Puerto origen:   
La opción más común para este campo es "cualquiera"

Puerto destino:

**Filtrado de paquetes > Desde redes externas hacia Zentyal**

**Editando regla**

Decisión:

Origen:

Servicio:  Coincidencia inversa: ☐

Si la selección inversa está marcada, la regla será aplicada c

Descripción:

Opcional

En resumen se verían las siguientes reglas:

**Filtrado de paquetes > Desde redes externas hacia Zentyal**

**Configure Rules**

[+ Añadir nuevo/a](#)

Decisión	Origen	Servicio	Descripción	Acción
↑	10.5.0.1/32	any TCP	FRA OpenVPN	
↑	Cualquiera	ping-icmp	Para permitir ping desde el exterior	
↑	10.111.20.0/24	http	Permitir max-control	
↑	10.111.20.0/24	Administración de Zentyal	Permitir administración zentyal	
↑	10.111.20.0/24	ssh	Permitir ssh	
×	Cualquiera	RADIUS	--	

10 Página 1

En “Reglas de filtrado para redes internas” se permite todo el tráfico:

**Filtrado de paquetes > Redes internas**

**Configure Rules**

[+ Añadir nuevo/a](#)

Decisión	Origen	Destino	Servicio	Descripción	Acción
↑	Cualquiera	Cualquiera	cualquiera	Que entre todo	

10 Página 1

En “Reglas de filtrado desde las redes externas a las internas” no existe ninguna regla.

En “Reglas de filtrado para el tráfico saliente de Zentyal” se permite todo:



Filtrado de paquetes > Tráfico saliente de Zentyal

Configure Rules

+ Añadir nuevo/a

Buscar

Decisión	Destino	Servicio	Descripción	Acción
	Cualquiera	cualquiera	Que salta todo	

10 Página 1

Por último están las reglas añadidas por los servicios de Zentyal que dependerán de los módulos o servicios que tengamos activados. Estas reglas no se pueden eliminar ni modificar pero sí se pueden desactivar.

## 15. CONFIGURACIÓN DEL SERVICIO DHCP

La configuración DHCP se realiza sólo para la interface eth1, que es la que da servicio a la red de alumnos y profesores:

Salir de sesión Guardar cambios

Core

Dashboard

Estado del módulo

Sistema

Red

Objetos

Servicios

Registros

Eventos

Gateway

Proxy HTTP

Moldeado de tráfico

UTM

Cortafuegos

VPN

Infraestructure

**DHCP**

DNS

Autoridad de certificación

Backharddi NG

MAX Control

Office

Usuarios y Grupos

Rincón del Usuario

Compartir ficheros

Compartir Impresoras

DHCP (mostrar ayuda)

Configuración del servicio

Elije un interfaz estático para configurar: **Interfaz eth1**

Opciones personalizadas Opciones de DNS dinámico Advanced options

Puerta de enlace predeterminada: eBox  
Configurando "eBox" como router por defecto establecerá la dirección IP del interfaz como router

Dominio de búsqueda: Personalizado madrid  
El dominio seleccionado completará en tus clientes aquellas peticiones DNS que no están completamente cualificadas

Servidor de nombres primario: eBox DNS local  
Si "eBox DNS" está presente y seleccionado, el servidor eBox actuará como servidor DNS caché

Servidor de nombres secundario: Opcional

Servidor NTP: eBox NTP local  
Si "eBox NTP" está presente y es seleccionado, eBox será el servidor NTP para los clientes DHCP

Servidor WINS: eBox local  
Si "eBox Samba" está presente y está seleccionado, eBox será el servidor WINS para los clientes DHCP

Change

Rangos DHCP

Dirección IP del interfaz: 192.168.10.1  
Subred: 192.168.10.0/24  
Rango disponible: 192.168.10.1 - 192.168.10.254

Rangos

+ Añade nuevo

Buscar

Nombre	Desde	Hasta	Action
multiports	192.168.10.200	192.168.10.254	

10 Página 1

El servicio está configurado para dar IP en el rango 192.168.10.200 a la 192.168.10.254. Este servicio es imprescindible sobre todo para los equipos que arrancan por red, de forma que





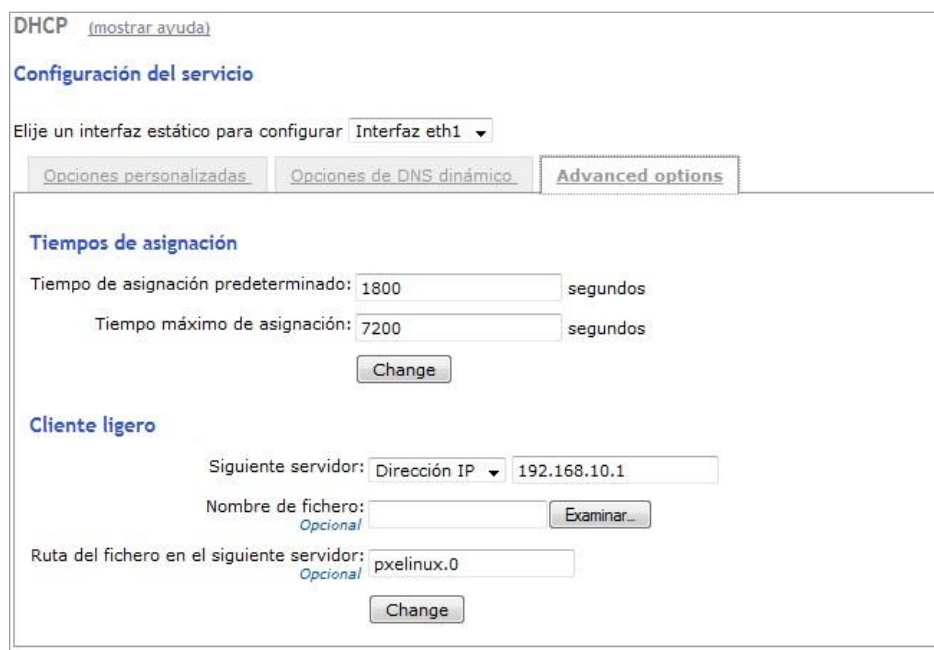
puedan recibir una IP automática y mediante PXE reciban el menú del servidor con el que se controla en qué sistema operativo iniciar.

En la ficha “Opciones de DNS dinámico” no se configura nada:



The screenshot shows the DHCP configuration interface with the 'Opciones de DNS dinámico' tab selected. At the top, it says 'DHCP (mostrar ayuda)' and 'Configuración del servicio'. Below this, there's a dropdown for 'Interfaz eth1'. Three tabs are visible: 'Opciones personalizadas', 'Opciones de DNS dinámico' (active), and 'Advanced options'. A blue banner states: 'Domains will be added/set automatically in DNS section in read-only mode.' Below this, there's a 'Habilitado:' checkbox which is unchecked. A 'Dominio dinámico:' text field is empty, with a note: 'El nombre de dominio se añade al nombre de máquina de aquellos clientes cuyo dirección IP ofrecida desde un rango'. Below that, a 'Dominio estático:' dropdown is set to 'Mismo que el dominio dinámico', with a note: 'Nombre de dominio añadido al nombre de máquina de aquellos clientes con una asignación estática'. A 'Cambiar' button is at the bottom.

La ficha “Advanced options” contiene la configuración del arranque por PXE, denominada aquí como “Cliente ligero”:



The screenshot shows the DHCP configuration interface with the 'Advanced options' tab selected. It has the same header as the previous screenshot. Below the tabs, the 'Tiempo de asignación' section has two text fields: 'Tiempo de asignación predeterminado: 1800 segundos' and 'Tiempo máximo de asignación: 7200 segundos', with a 'Change' button below them. The 'Cliente ligero' section has a 'Siguiendo servidor:' dropdown set to 'Dirección IP' with the value '192.168.10.1'. Below it, 'Nombre de fichero:' is an empty text field with a note 'Opcional' and an 'Examinar...' button. Below that, 'Ruta del fichero en el siguiente servidor:' is a text field with the value 'pxelinux.0' and a note 'Opcional', with a 'Change' button below it.

## 16. CONFIGURACIÓN DEL SERVICIO DNS

En el servicio DNS se añadirá el dominio “madrid”, no es necesario ponerle IP al dominio:





**Infrastructure**

DHCP

**DNS**

Autoridad de certificación

Backharddi NG

MAX Control

DNS [\(mostrar ayuda\)](#)

**Añadiendo una nueva dominio**

Dominio:

Dirección IP: 
Opcional

Una vez añadido el dominio pulsaremos en el icono de la columna “Nombres de máquinas”:

**Lista de Dominios**

Dominio	Nombres de máquinas	Intercambiadores de correo	Servidores de nombres	Dirección IP	Dinámico	Action
madrid				--		 


10 ▼ Página 1 

Se añadirán los nombres de máquinas que se encuentren en la red interna (la 192.168.10.0 que corresponde al eth1) imprescindible añadir el servidor “max-server” con su IP, 192.168.10.1:

DNS > madrid [\(mostrar ayuda\)](#)

**Nombres de máquinas**

 [Añade nuevo](#)

Nombre de la máquina	Dirección IP	Alias	Action
max-server	192.168.10.1		 
profesor10	192.168.10.10		 

10 ▼ Página 1 

## 17. CONFIGURACIÓN DEL SERVICIO NTP.

En “Estado de los Módulos” activaremos el servicio NTP. Sólo por el hecho de activar este módulo el servidor se convierte en un servidor de tiempo, lo que significa que podemos configurar los equipos de la red para que se conecten a él para actualizar la hora.

Si lo que queremos además es que el servidor actualice su propia hora de forma automática iremos a la configuración del módulo NTP y añadiremos los servidores de tiempo deseados:





Podemos añadir los servidores que queramos pero hasta que no marquemos la casilla de verificación “Activar sincronización con servidores NTP externos”, estos no serán usados. Hay que pulsar el botón de “Cambiar” y “Guardar cambios” para que la configuración se haga efectiva.

NOTA: En la macrolan no se tiene acceso a los servidores de hora de internet por lo que esta configuración no funciona y se puede desactivar, pero el módulo NTP debe seguir activado para que el servidor de centro actúe como servidor de hora a los equipos locales de la red.

## 18. USUARIOS Y GRUPOS

### 1. Usuarios

En esta sección podemos ver los usuarios del LDAP. Estos usuarios se han creado por medio del panel de “max-control”.



Core

Dashboard

Estado del módulo

Sistema

Red

Objetos

Servicios

Registros

Eventos

Gateway

Proxy HTTP

Moldeado de tráfico

UTM

Cortafuegos

VPN

Infrastructure

DHCP

DNS

Autoridad de certificación

Backharddi NG

MAX Control

Office

Usuarios y Grupos

Usuarios

Grupos

Plantilla de Usuario por Defecto

Datos LDAP

Estado de Esclavo

Users

Añadir usuario

Nombre de usuario:

Nombre:

Apellido:

Comentario:

Contraseña:

Confirme contraseña:

Grupo:

Añadir

Añadir y Editar

Usuarios

Buscar

Nombre	Nombre completo	Editar
Agonzalezvargas1	Agonzalezvargas1 González	
aacebesgarcia	aacebesgarcia Acebes	
aamosanchez	aamosanchez AMO SÁNCHEZ	
aapilanezgarcia	aapilanezgarcia Apilánez García	
aarandalopez	aarandalopez Aranda López	
aarnaizabad	aarnaizabad ARNÁIZ ABAD	
aazevedodeoliveira	aazevedodeoliveira AZEVEDO DE OLIVEIRA	
abecerrafernandez	abecerrafernandez BECERRA FERNÁNDEZ	
abizefont	abizefont BIZE FONT	
ablazquezdieguez	ablazquezdieguez BLAZQUEZ DIÉGUEZ	

10 Página 1 de 50

No se debe utilizar esta página para administrar los usuarios o grupos, para ello está el panel de max-control que realiza operaciones adicionales que este panel ya no contempla.

## 2. Grupos

En el apartado de grupos vemos los grupos del sistema, con la peculiaridad de que también se observan los grupos que el panel de max-control oculta, como es el de “CoordinadorTIC”, “Instaladores” y “Teachers”. Igualmente no se debe de administrar ningún grupo desde esta página siempre que se pueda hacer desde el max-control:

Registros

Eventos

Gateway

Proxy HTTP

Moldeado de tráfico

UTM

Cortafuegos

VPN

Infrastructure

DHCP

DNS

Autoridad de certificación

Backharddi NG

MAX Control

Office

Usuarios y Grupos

Usuarios

Grupos

Plantilla de Usuario por Defecto

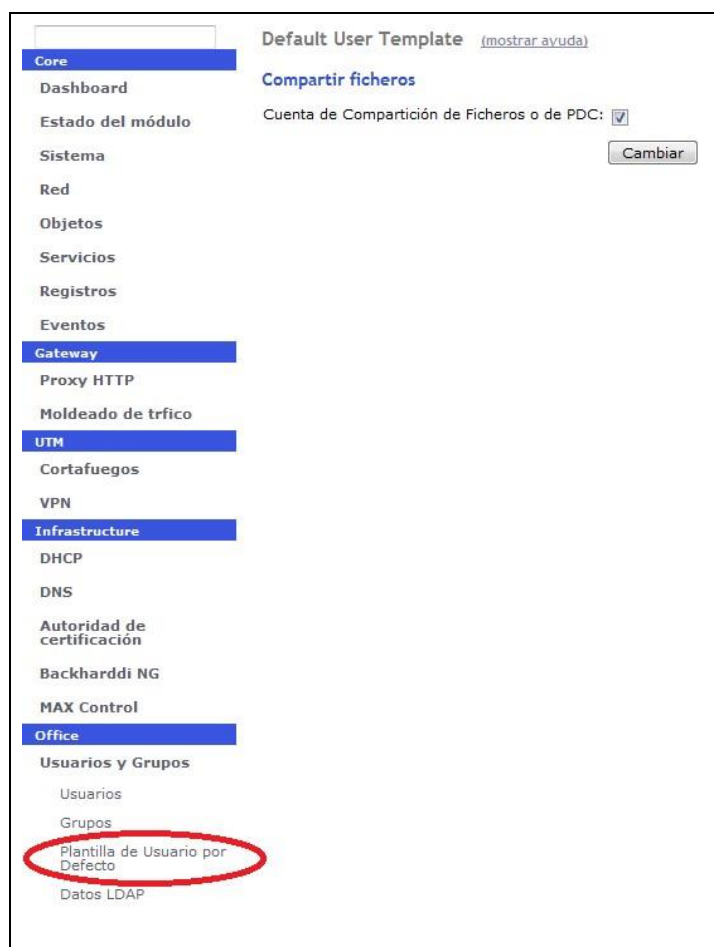
Buscar

Nombre	Descripción	Editar
Aula10		
Aula20		
Aula30		
CoordinadoresTIC	Coordinadores TIC no-borrar	
Instaladores	Instaladores no-borrar	
Teachers	Profesores no-borrar	
bachilleratmate		
consejeria		
d de et ew		
historiadelarte		

10 Página 1 de 3



A continuación de los grupos aparece la “Plantilla de Usuario por Defecto” que contiene la opción “Cuenta de compartición de ficheros o de PDC” que deberá estar marcada.



En el apartado “Datos LDAP” podemos ver a modo de información, la configuración del LDAP, debemos tener algo como lo siguiente:



En la sección de “Compartir ficheros” encontraremos la configuración relacionada con SAMBA, debemos configurarla tal como se muestra en las siguientes imágenes:



Compartir ficheros [\(mostrar ayuda\)](#)

[Configuración general](#) [PDC](#) [Directorios compartidos](#) [Papelera de Reciclaje](#)

Habilitar PDC: ☒

Nombre del dominio:

Nombre de Netbios:

Descripción:

Límite de cuota: Limitada a  Mb

Habilitar perfiles móviles: ☒

Letra de unidad:

Grupo Samba:   
Sólo los usuarios que pertenecen a este grupo tendrán una cuenta de Samba. Sincronización ocurre cada hora.

Compartir ficheros [\(mostrar ayuda\)](#)

[Configuración general](#) [PDC](#) [Directorios compartidos](#) [Papelera de Reciclaje](#)

Longitud mínima de contraseña: Limitada a  caracteres

Caducidad de la contraseña:

Forzar historial de contraseñas:

Compartir ficheros [\(mostrar ayuda\)](#)

[Configuración general](#) [PDC](#) [Directorios compartidos](#) [Papelera de Reciclaje](#)

[+ Añade nuevo](#)

Compartir ficheros [\(mostrar ayuda\)](#)

[Configuración general](#) [PDC](#) [Directorios compartidos](#) [Papelera de Reciclaje](#)

Opciones por defecto de la Papelera [\(mostrar ayuda\)](#)

Opciones por defecto de la Papelera de Reciclaje

Habilitar Papelera de Reciclaje: ☐

Recursos excluidos de la Papelera de Reciclaje

[+ Añade nuevo](#)



## 19. CONFIGURACIÓN DE LA VPN

Comprobaremos que existen los siguientes certificados:

Core

Dashboard

Estado del módulo

Sistema

Red

Objetos

Servicios

Registros

Eventos

Gateway

Proxy HTTP

Moldeado de tráfico

UTM

Cortafuegos

VPN

Infrastructure

DHCP

DNS

Autoridad de certificación

General

Certificados para los servicios

Certification Authority [\(mostrar ayuda\)](#)

Expedir un nuevo certificado

Nombre común:

Días para expirar:

Expedir

Lista de Certificados actual

Name	Estado	Fecha	Acciones
Certification Authority Certificate desde MAX	Válido	2020-06-15 10:13:52	
vpn-max-server	Válido	2020-06-15 10:13:52	
vpn-clientes	Válido	2020-06-15 10:13:52	

Revocar
 Descargar clave(s) y certificado
 Renovar

Ahora vamos a “Estado del módulo” y activamos el módulo VPN. Si es la primera vez que activamos el módulo, tendremos que confirmar el siguiente mensaje para que se creen los ficheros de configuración necesarios:

Configurar módulo: openvpn

Habilitar este módulo causaría que eBox realizase las acciones y las modificaciones en los ficheros listados debajo. Debes aceptar explícitamente estos cambios para habilitar el módulo.

**Ficheros a modificar por eBox**

**File:** /etc/quagga/daemons  
**Reason:** To configure Quagga to run ripd and zebra

**File:** /etc/quagga/debian.conf  
**Reason:** To configure Quagga to listen on the given interfaces

**File:** /etc/quagga/zebra.conf  
**Reason:** Main zebra configuration file

**File:** /etc/quagga/ripd.conf  
**Reason:** To configure ripd to exchange routes with client to client connections

Aceptar

Una vez aceptado el mensaje guardaremos los cambios en el panel para que se active el módulo.

Ahora iremos a la sección VPN > Servidores, donde añadiremos un nuevo servidor de VPN al que pondremos el nombre del centro todo en minúsculas, utilizando guiones bajos en vez de espacios y no pondremos acentos ni caracteres especiales:





**Core**  
 Dashboard  
 Estado del módulo  
 Sistema  
 Red  
 Objetos  
 Servicios  
 Registros  
 Eventos  
**Gateway**  
 Proxy HTTP  
 Moldeado de tráfico  
**UTM**  
 Cortafuegos  
**VPN**  
**Servidores**  
 Clientes

Servidores VPN [\(mostrar ayuda\)](#)  
**Añadiendo una nueva Servidor**  
 Activado: ☒  
 Nombre:

Al pulsar el botón “Añadir” aparecerá la lista de servidores VPN con el nuevo servidor:


 Servidor actualizada

Servidores VPN [\(mostrar ayuda\)](#)  
**Lista de servidores**  
[+ Añade nuevo](#)

Activado	Nombre	Configuración	Redes anunciadas	Descargar paquete de configuración de cliente	Action
<input checked="" type="checkbox"/>	gran_capitan				 

10

↓

Página 1






Pulsaremos el icono de la columna “Configuración”, nos aparecerá la siguiente página que configuraremos como se muestra:



**Servidores VPN ▶ gran\_capitan**

**Configuración del servidor**

Puerto del servidor: UDP puerto 1194

Dirección VPN: 192.168.160.0 / 24  
Use una dirección de red que no esté en uso por esta máquina

Certificado de servidor: vpn-gran\_capitan

Autorizar al cliente por su nombre común: disabled  
Si se deshabilita todos los clientes con un certificado generado por eBox se pueden conectar

Traducción de dirección de red (NAT): ☐  
Habilítelo si sólo dispone de una interfaz de red

Permitir conexiones cliente-cliente: ☒  
Habilite esto para permitir que máquinas clientes de esta VPN puedan verse unas a otras

Permitir túneles eBox a eBox: ☐  
Habilite esto si esta VPN se usa para conectar con otra eBox

Contraseña de túneles eBox a eBox:   
Opcional

Interfaz en la que escuchar: eth0

**Cambiar**

Pulsamos el botón “Cambiar” para que acepte la configuración y luego hacemos clic en el enlace “Servidores VPN” de la esquina superior izquierda para volver a la lista de servidores VPN y ahora pulsamos sobre el botón de “Redes anunciadas”.

Veremos que aparecen dos redes, 192.168.10.0/24 y 192.168.11.0/24. Borraremos la red 192.168.11.0/24:

**Servidores VPN ▶ gran\_capitan** [\(mostrar ayuda\)](#)

**Lista de redes anunciadas**

+ [Añade nuevo](#)

**Buscar**













Red anunciada	Action
192.168.10.0/24	




10 **Página 1**

Ahora ya podemos pulsar el botón “Guardar cambios” y confirmar para que se graben todas las configuraciones y se active la VPN.

## 20. COMPROBACIONES DE LA VPN

Cuando se crea una VPN se crea automáticamente un certificado digital con su nombre, comprobamos que aparece dicho certificado:

Lista de Certificados actual			
Name	Estado	Fecha	Acciones
Certification Authority Certificate desde MAX	Válido	2020-06-15 10:13:52	  
vpn-max-server	Válido	2020-06-15 10:13:52	  
vnp-clientes	Válido	2020-06-15 10:13:52	  
vpn-gran_capitan	Válido	2020-06-15 10:13:52	  

 Revocar
  Descargar clave(s) y certificado
  Renovar

En el “Dashboard” comprobaremos que aparece un nuevo “widget” con el estado de la VPN. Además de ver la configuración nos fijaremos sobre todo que el estado del demonio es “Corriendo”:

Demonios OpenVPN	
▼ Servidor gran_capitan	
Servicio	Activado
Estado del demonio	Corriendo
Dirección local	192.168.1.5
Puerto	1194/UDP
Subred VPN	192.168.160.0/255.255.255.0
Interfaz de red de la VPN	tap0
Dirección de la interfaz de la VPN	192.168.160.1/24

En el ejemplo vemos que la dirección local es la de la interface eth0(192.168.1.5) que es la que sale a internet, en una macrolan veremos la dirección del tipo 10.111.XX.X. Desde la consola podemos comprobar que ahora aparece un nuevo interfaz virtual de red llamado “tap0”:

```

madrid@max-server:~$ ifconfig
eth0    Link encap:Ethernet direcciónHW 54:e6:fc:80:40:7a
        Direc. inet:192.168.1.5  Difus.:192.168.1.255  Másc:255.255.255.0
        Dirección inet6: fe80::56e6:fcff:fe80:407a/64 Alcance:Enlace
        ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
        Paquetes RX:4358 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:3541 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1000
        Bytes RX:3668082 (3.6 MB) TX bytes:1099774 (1.0 MB)
        Interrupción:28 Dirección base: 0x2000
eth1    Link encap:Ethernet direcciónHW 54:e6:fc:80:30:eb
        Direc. inet:192.168.10.1 Difus.:192.168.10.255 Másc:255.255.255.0
        Dirección inet6: fe80::56e6:fcff:fe80:30eb/64 Alcance:Enlace
        ACTIVO DIFUSIÓN MULTICAST MTU:1500 Métrica:1
        Paquetes RX:1926 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:2941 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1000
        Bytes RX:213409 (213.4 KB) TX bytes:3535403 (3.5 MB)
        Interrupción:29 Dirección base: 0xc000
eth2    Link encap:Ethernet direcciónHW 00:1e:8c:68:71:bd
        Direc. inet:192.168.11.1 Difus.:192.168.11.255 Másc:255.255.255.0
        ACTIVO DIFUSIÓN MULTICAST MTU:1500 Métrica:1
        Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:0 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1000
        Bytes RX:0 (0.0 B) TX bytes:0 (0.0 B)
        Interrupción:30
lo      Link encap:Bucle local
        Direc. inet:127.0.0.1 Másc:255.0.0.0
        Dirección inet6: ::1/128 Alcance:Anfitrión
        ACTIVO BUCLE FUNCIONANDO MTU:16436 Métrica:1
        Paquetes RX:1422 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:1422 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:0
        Bytes RX:307726 (307.7 KB) TX bytes:307726 (307.7 KB)
tap0    Link encap:Ethernet direcciónHW 0e:da:50:fa:03:07
        Direc. inet:192.168.160.1 Difus.:192.168.160.255 Másc:255.255.255.0
        Dirección inet6: fe80::cda:50ff:fefa:307/64 Alcance:Enlace
        ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
        Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:22 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:100
        Bytes RX:0 (0.0 B) TX bytes:3723 (3.7 KB) madrid@max-
server:~$
  
```

El fichero de configuración de la VPN los podemos encontrar en “/etc/openvpn”:

```

madrid@max-server:~$ ls -l /etc/openvpn/ total 12
-rw-r--r-- 1 root root 245 2010-05-13 15:19 ebox-dh1024.pem
-r----- 1 root root 3338 2011-05-14 21:20 gran_capitan.conf -rwxr-xr-x 1 root root 1352
2009-10-13 10:01 update-resolv-conf madrid@max-server:~$
  
```

Y si editamos el fichero “.conf” veremos que esta configurado para que se guarden dos log en /var/log/ebbox/openvpn que podemos consultar para detectar errores:



```
madrid@max-server:~$ ls -l /var/log/ebox/openvpn/ total 8
-rw-r----- 1 root ebox 1437 2011-05-14 21:20 gran_capitan.log
-rw-r----- 1 root ebox 232 2011-05-14 21:55 status-gran_capitan.log madrid@max-server:~
```

## 21. CONECTARSE A LA VPN DESDE MAX

MAX ya tiene instalado por defecto el paquete “openvpn” el cual es necesario para realizar la conexión. Necesitaremos también los certificados y la configuración de la VPN que nos lo suministra el propio panel de administración de la VPN:

Hacemos clic en el botón “Descargar paquete de configuración de cliente” y nos aparecerá la siguiente página:

Configuramos el “Tipo de cliente” para Linux, como certificado dejamos el “vnp-clientes” y ponemos el nombre o la IP pública del servidor. En la macrolan tenemos acceso directo a la IP por lo que ponemos su IP.



Al pulsar el botón “Cambiar” nos descargaremos un fichero de extensión “.tar.gz” el cual descomprimiremos en una carpeta.

Accederemos por consola a la carpeta, en nuestro ejemplo este sería el contenido:

```
madrid@pc00:~/vpns/gran_capitan$ ls -l
total 16
-rw-r--r-- 1 madrid madrid 1151 2011-05-14 22:20 cacert.pem
-rw-r--r-- 1 madrid madrid 3126 2011-05-14 22:20
F45F057682A11181.pem
-rw-rw-rw- 1 madrid madrid 3698 2011-05-14 22:20 gran_capitan-
client.conf
-rw-r--r-- 1 madrid madrid 887 2011-05-14 22:20 vnp-clientes.pem
madrid@pc00:~/vpns/gran_capitan$
```

Ahora desde la carpeta donde hemos descomprimido los archivos ejecutaremos con permisos de administrador el comando “openvpn <fichero.conf>” donde “fichero.conf es el correspondiente a la VPN, “gran\_capitan-client.conf” en nuestro ejemplo.

IMPORTANTE: Si no ejecutamos como root el comando “openvpn” no se podrá crear el interface virtual “tap0” y la conexión dará error.

```
madrid@pc00:~/vpns/gran_capitan$ sudo openvpn gran_capitan-
client.conf [sudo] password for madrid:
Sat May 14 22:42:58 2011 OpenVPN 2.1.3 i486-pc-linux-gnu [SSL] [LZO2] [EPOLL] [PKCS11] [MH] [PF_INET6] [eurephia]
built on Mar
29 2011
Sat May 14 22:42:58 2011 WARNING: Make sure you understand the semantics of --tls-remote before using it (see
the man page).
Sat May 14 22:42:58 2011 NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-defined scripts or
executables
Sat May 14 22:42:58 2011 WARNING: file 'vnp-clientes.pem' is group or others accessible
Sat May 14 22:42:58 2011 /usr/bin/openssl-vulnkey -q -b 1024 -m <modulus omitted>
Sat May 14 22:42:58 2011 LZO compression initialized
Sat May 14 22:42:58 2011 Control Channel MTU parms [ L:1574 D:138 EF:38 EB:0 ET:0 EL:0 ]
Sat May 14 22:42:58 2011 Socket Buffers: R=[112640->131072] S=[112640->131072]
Sat May 14 22:42:58 2011 Data Channel MTU parms [ L:1574 D:1450 EF:42 EB:135 ET:32 EL:0 AF:3/1 ]
Sat May 14 22:42:58 2011 Local Options hash (VER=V4): 'd79ca330'
Sat May 14 22:42:58 2011 Expected Remote Options hash (VER=V4): 'f7df56b8'
Sat May 14 22:42:58 2011 UDPv4 link local: [undef]
Sat May 14 22:42:58 2011 UDPv4 link remote: [AF_INET]192.168.1.5:1194
Sat May 14 22:42:58 2011 TLS: Initial packet from [AF_INET]192.168.1.5:1194, sid=aade44 e6e1e338
Sat May 14 22:42:58 2011 VERIFY OK: depth=1,
/C=ES/ST=Madrid/L=Madrid/O=MAX/CN=Certification_Authority_Certificate
Sat May 14 22:42:58 2011 VERIFY X509NAME OK: /C=ES/ST=Madrid/L=Madrid/O=MAX/CN=vpn-gran_capitan
Sat May 14 22:42:58 2011 VERIFY OK: depth=0, /C=ES/ST=Madrid/L=Madrid/O=MAX/CN=vpn-gran_capitan
Sat May 14 22:42:59 2011 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sat May 14 22:42:59 2011 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Sat May 14 22:42:59 2011 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Sat May 14 22:42:59 2011 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Sat May 14 22:42:59 2011 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Sat May 14 22:42:59 2011 [vpn-gran_capitan] Peer Connection Initiated with [AF_INET]192.168.1.5:1194
Sat May 14 22:43:01 2011 SENT CONTROL [vpn-gran_capitan]: 'PUSH_REQUEST' (status=1)
Sat May 14 22:43:01 2011 PUSH: Received control message: 'PUSH_REPLY,route 192.168.10.0 255.255.255.0,route-
gateway
192.168.160.1,ping 10,ping-restart 120,ifconfig 192.168.160.2 255.255.255.0'
Sat May 14 22:43:01 2011 OPTIONS IMPORT: timers and/or timeouts modified
Sat May 14 22:43:01 2011 OPTIONS IMPORT: --ifconfig/up options modified
Sat May 14 22:43:01 2011 OPTIONS IMPORT: route options modified
Sat May 14 22:43:01 2011 OPTIONS IMPORT: route-related options modified
Sat May 14 22:43:01 2011 ROUTE default_gateway=192.168.1.1
Sat May 14 22:43:01 2011 TUN/TAP device tap0 opened
Sat May 14 22:43:01 2011 TUN/TAP TX queue length set to 100
```



```
Sat May 14 22:43:01 2011 /sbin/ifconfig tap0 192.168.160.2 netmask 255.255.255.0 mtu 1500 broadcast  
192.168.160.255 Sat May 14 22:43:01 2011 /sbin/route add -net 192.168.10.0 netmask 255.255.255.0 gw  
192.168.160.1  
Sat May 14 22:43:01 2011 Initialization Sequence Completed
```

Al ejecutar el comando “openvpn” si la conexión tiene éxito no se devuelve el control a la consola por lo que sin cerrar esa consola abriremos otra desde la que ejecutaremos un “ifconfig” para comprobar que se ha creado el interfaz virtual “tap0” con una IP correspondiente a la de la VPN, la 192.168.160.2:



```
madrid@pc00:~/vpns/gran_capitan$ ifconfig
eth0    Link encap:Ethernet direcciónHW 00:01:80:40:2f:e7
        Direc. inet:192.168.1.10 Difus.:192.168.1.255 Másc:255.255.255.0
        Dirección inet6: fe80::201:80ff:fe40:2fe7/64 Alcance:Enlace
        ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
        Paquetes RX:315117 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:230683 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1000
        Bytes RX:403182461 (403.1 MB) TX bytes:16998444 (16.9 MB)
        Interrupción:17 Dirección base: 0xe000

lo       Link encap:Bucle local
        Direc. inet:127.0.0.1 Másc:255.0.0.0
        Dirección inet6: ::1/128 Alcance:Anfitrión
        ACTIVO BUCLE FUNCIONANDO MTU:16436 Métrica:1
        Paquetes RX:985 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:985 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:0
        Bytes RX:66992 (66.9 KB) TX bytes:66992 (66.9 KB)

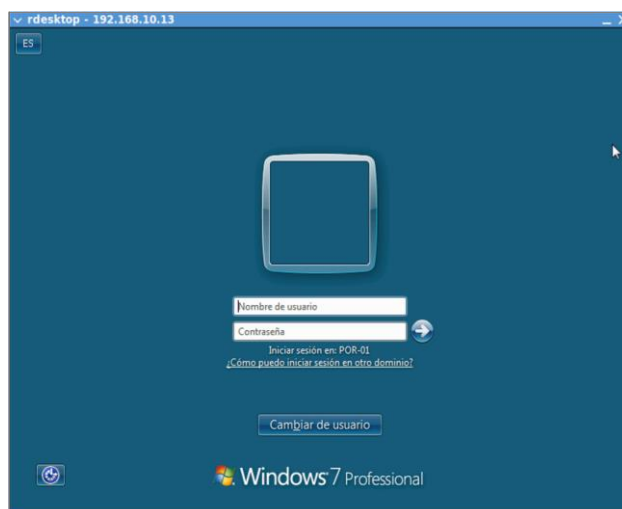
tap0     Link encap:Ethernet direcciónHW e2:29:4f:f2:90:75
        Direc. inet:192.168.160.2 Difus.:192.168.160.255 Másc:255.255.255.0
        Dirección inet6: fe80::e029:4fff:fef2:9075/64 Alcance:Enlace
        ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
        Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:50 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:100
        Bytes RX:0 (0.0 B) TX bytes:6840 (6.8 KB) madrid@pc00:~/vpns/gran_capitan$
```

Ahora ya podemos hacer un ping a cualquier equipo de la red para ver si está disponible y por ejemplo conectarnos a Windows con el comando “rdesktop”:

Para terminar la conexión VPN basta con pulsar CTRL+C desde el terminal que iniciamos la conexión con “openvpn”. Podemos comprobar entonces con “ifconfig” que el interfaz “tap0” ha desaparecido.

## 22. CONECTARSE A LA VPN DESDE WINDOWS

Necesitamos descargar los certificados y el programa OpenVPN para Windows. Todo esto nos lo suministra el propio panel de administración de la VPN. Pulsamos en el icono de la columna “Descargar paquete de configuración de cliente” y aparecerá la siguiente pantalla de configuración:



Servidores VPN ▸ gran\_capitan (mostrar ayuda)

Descargar paquete de configuración de cliente

Tipo de cliente: Windows

Certificado del cliente: vnp-clientes

Añadir instalador de OpenVPN al paquete de configuración del cliente: ☒

Instalador de OpenVPN para Microsoft Windows

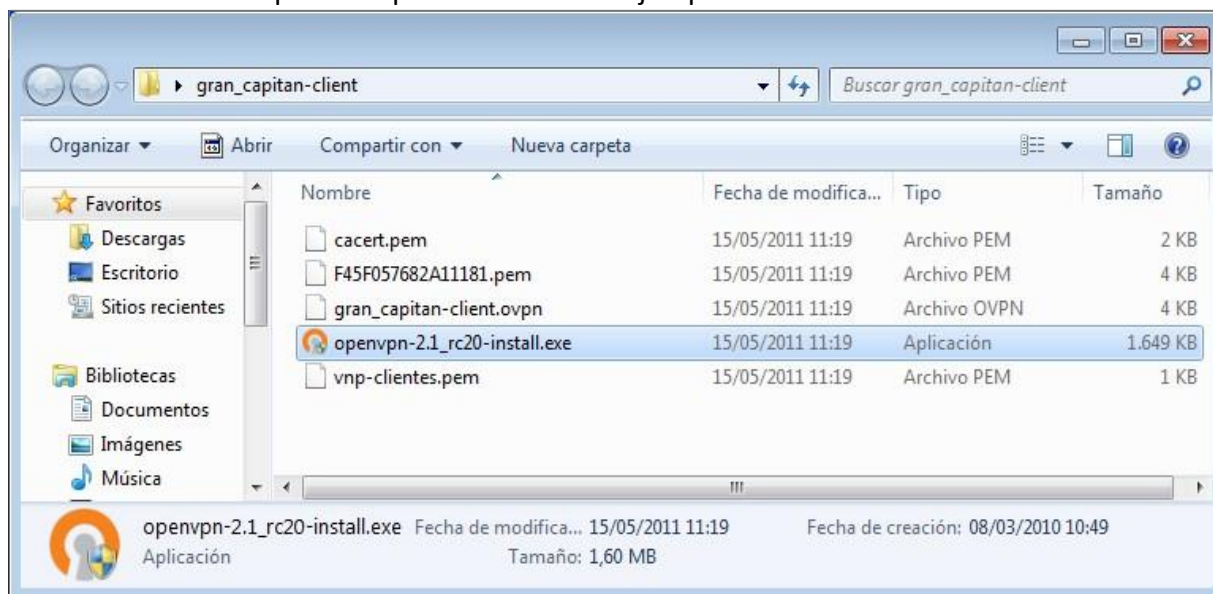
Dirección del servidor: 10.111.18.5  
 Esta es la dirección que usarán sus clientes para conectarse al servidor. Normalmente, ésta será una IP pública o un nombre de host

Dirección adicional del servidor (opcional):

Dirección adicional del servidor (opcional):

Si no tenemos instalado OpenVPN en Windows, marcaremos la opción de “Añadir instalador de OpenVPN”, de esta manera se añade al paquete un pequeño fichero ejecutable para su instalación. En la dirección del servidor pondremos la correspondiente a la interfaz eth0 que es la que está conectada a internet y que varía dependiendo de cada centro.

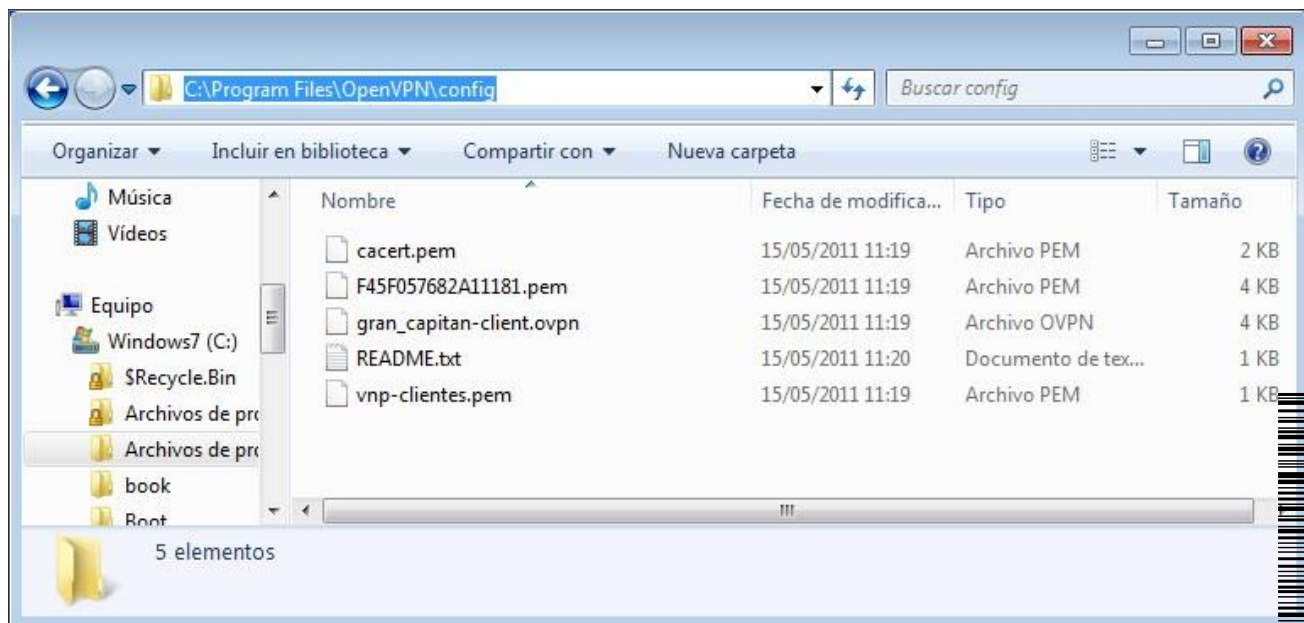
Al pulsar el botón “Cambiar” nos descargaremos un fichero “.zip” que descomprimiremos en Windows en una carpeta temporal. En nuestro ejemplo este es el contenido:



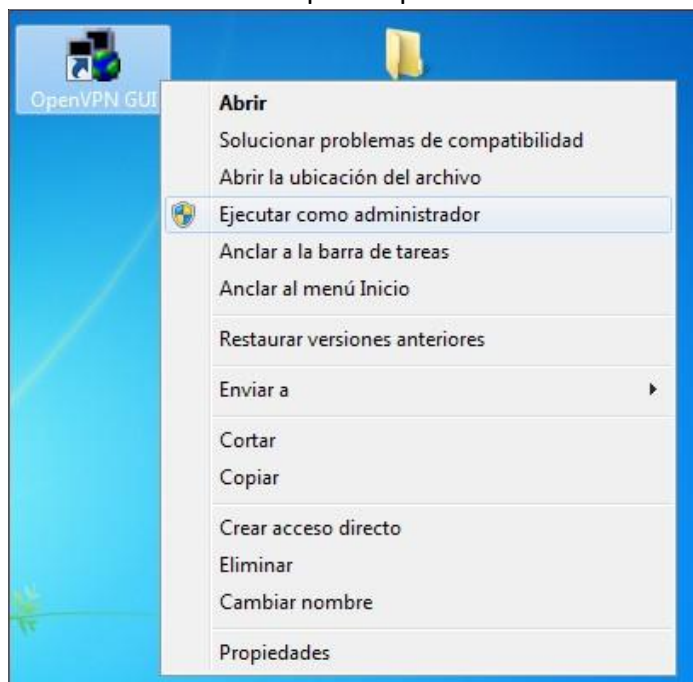
En la carpeta encontraremos el instalador de “openvpn” el cual instalaremos dejando todas las opciones de instalación por defecto. Una vez instalado encontraremos un icono en el escritorio llamado “OpenVPN GUI”.

Antes de iniciar la conexión hay que copiar los certificados “.pem” y el fichero de configuración “.ovpn” a la carpeta de configuración de OpenVPN que se encuentra en “C:\Archivos de programa\OpenVPN\config\”:

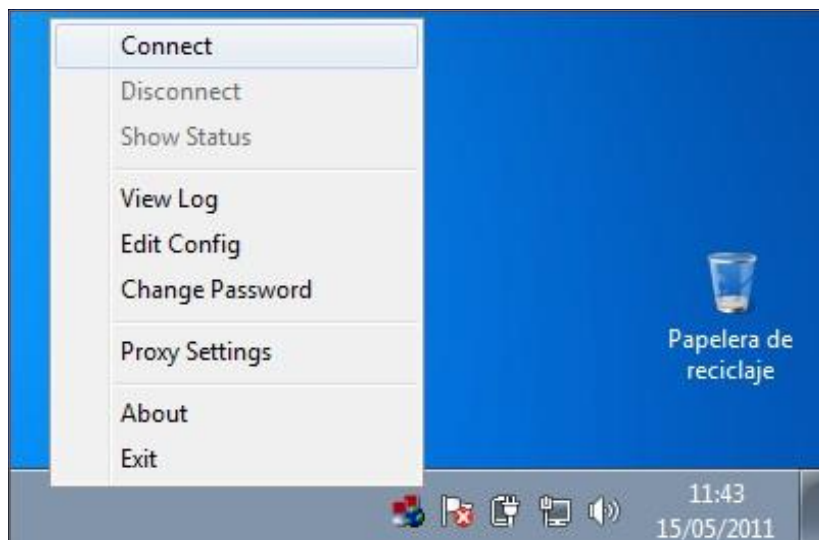




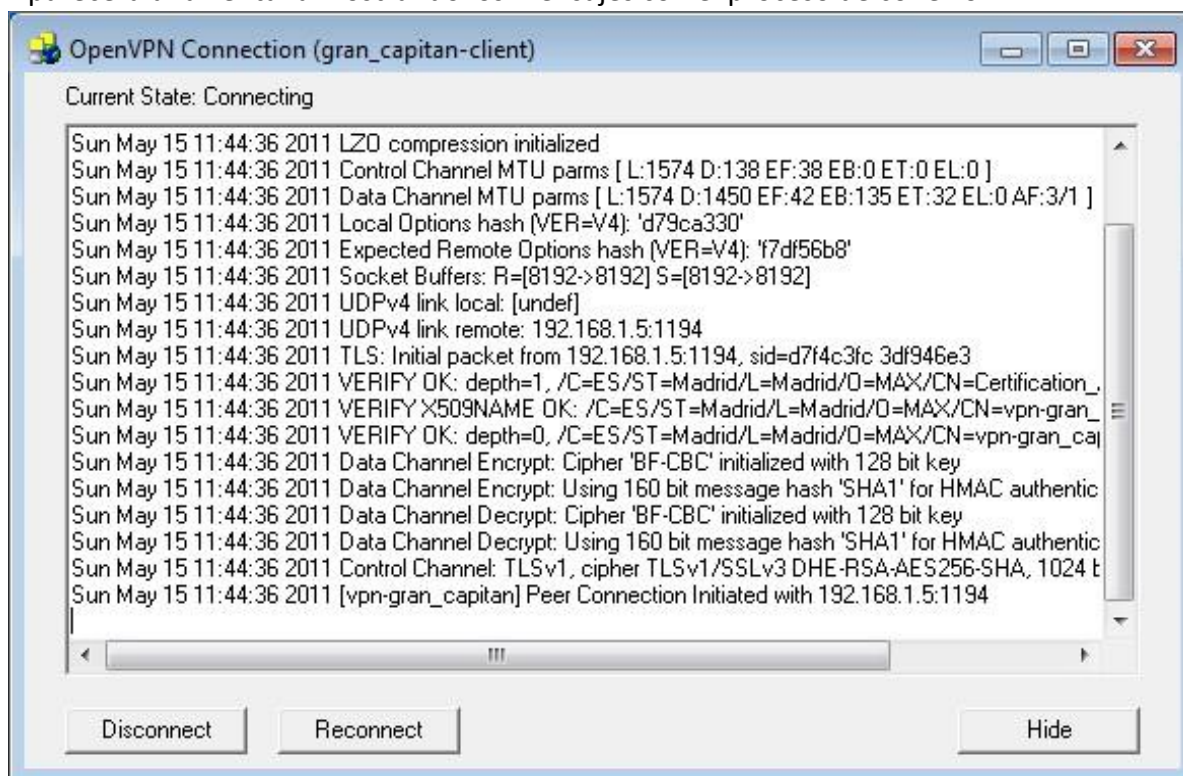
Si no estamos trabajando con la cuenta de “Administrador” deberemos ejecutar el icono de “OpenVPN GUI” haciendo clic derecho sobre él y seleccionado “Ejecutar como administrador”, de lo contrario conectaremos a la VPN pero no se crearán las rutas en Windows hacia la VPN por lo que no tendremos acceso a ella:



Al ejecutar “OpenVPN GUI” aparecerá su icono en el área de notificación pero todavía no se habrá iniciado la conexión. Para iniciar la conexión haremos clic derecho sobre el icono y en el menú que aparece seleccionaremos “Connect”:



Aparecerá una ventana mostrando los mensajes con el proceso de conexión:

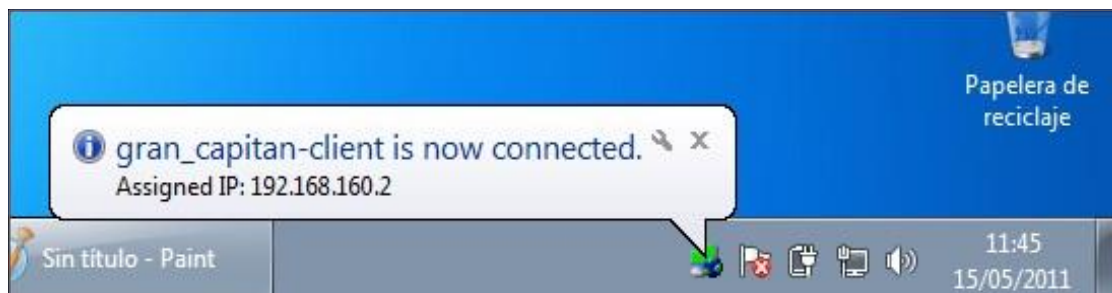


Esta ventana sólo la veremos unos segundos pues se cerrará automáticamente cuando la conexión se realice. Si queremos ver los detalles de conexión podemos abrir esta ventana en la opción "Show Status" del menú anterior.

Una vez que la conexión ha tenido éxito veremos que el icono de OpenVPN cambia al color verde y aparece durante unos segundos un globo de notificación:







Ahora ya podemos hacer un “ping” para comprobar si un equipo está disponible o conectarnos mediante “Escritorio Remoto”.

### **23. CREAR UN BACKUP DEL LDAP**

1º Comprobar que el servicio slapd está en

marcha: `ps u -C slapd`

2º Parar el servicio slapd:

`stop ebox.slapd`

3º Comprobar que el servicio slapd ya no

existe: `ps u -C slapd`

4º Crear el backup del ldap:

`tar czpvf <nombre_fichero>.gz /var/lib/ldap`

5º Iniciar el servicio slapd:

`start ebox.slapd`

6º Comprobar que el servicio slapd está en

marcha: `ps u -C slapd`

### **24. RESTAURAR EL BACKUP DEL LDAP**

1º Comprobar que el servicio slapd está en marcha: `ps u -C slapd`

2º Parar el servicio slapd:

`stop ebox.service slapd`

3º Comprobar que el servicio slapd está parado:

`ps u -C slapd`

4º Descomprimir la copia del ldap:

`tar -xzipvf <nombre_fichero>.gz -C /`

5º Iniciar el servicio slapd:

`start ebox.slapd`

6º Comprobar que el servicio slapd está en marcha:

`ps u -C slapd`





NOTA: Ahora incluso la contraseña del coordinadortic es la que tuviera el centro en el momento de crear la copia del ldap.

Además hay que copiar el fichero “/etc/samba/max-control.conf”. Después de restaurar hay que crear los grupos que hubiera en “/home/samba/groups” y en general la estructura de directorios que tenga “/home/samba”.

Para hacer una copia de los ficheros de SAMBA(no es necesario para restaurar un servidor) se siguen los mismos pasos cambiando el proceso “slapd” por “smbd” y la ruta “/var/lib/ldap” por “/var/lib/samba”.

## 25. CAMBIAR UN DISCO AVERIADO

El servidor de centro dispone de 6 discos emparejados en raid1 por lo que obtenemos 3 parejas de discos cada una perteneciente a un raid1. Un servidor con los raid estables muestra la siguiente información donde podemos ver la correspondencia de los raid *mdX* con los dos discos *sdX* de los que se compone:

```
madrid@max-server:~$ cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md2 : active raid1 sdf1[1] sde1[0]
      732572608 blocks [2/2] [UU]

md0 : active raid1 sda1[0] sdb1[1]
      732572608 blocks [2/2] [UU]

md1 : active raid1 sdc1[0] sdd1[1]
      732572608 blocks [2/2] [UU]

unused devices: <none>
madrid@max-server:~$
```

Para estar seguros del disco a retirar hay que averiguar el número de serie al que está asociado el nombre de dispositivo(sda, sdb, etc). Ejecutaremos el siguiente comando anotando la información que muestra pues será útil cuando extraigamos el disco averiado para comprobar que coincide el número de serie con el que viene anotado en la etiqueta del disco:

```
root@max-server:/home/madrid# lshw -C disk | grep -e serial -e /dev/sd
/dev/sd      logical name: /dev/sda      serial: S13UJDWZ406032
logical name: /dev/sdb      serial: S13UJDWZ406034      logical name:
/dev/sdc      serial: S13UJDWZ406024      logical name: /dev/sdd
serial: S13UJDWZ406030      logical name: /dev/sde      serial:
S13UJDWZ405905      logical name: /dev/sdf      serial: S13UJDWZ405906
root@max-server:/home/madrid#
```

Si el disco ha tenido una avería tal que ni siquiera es accesible, por descarte de los discos que están funcionando se puede averiguar cuál es el que hay que retirar. Otro dato a tener en cuenta es el puerto SATA al que está conectado cada disco, por lo general tal como se ha comprobado en un equipo encontramos la siguiente relación:



sda = SATA1  
sdb = SATA3  
sdc = SATA2  
sdd = SATA4  
sde = SATA5  
sdf = SATA6

Hay que fijarse en el listado anterior que el disco sdb y sdc no sigue el orden esperado (lo lógico es que estuvieran al revés). En la secuencia arranque se busca en orden secuencial (SATA1, SATA2, SATA3, etc.) el primer SATA que tenga un disco conectado, y no continúa mirando en los demás SATA aunque el disco no sea el correcto para iniciar el sistema. Debido a esta secuencia de arranque y la rara asignación que se produce entre los puertos SATA2 y SATA3, esto provoca que en caso de que quitemos el disco sda, el equipo no pueda arrancar desde el disco sdb ya que está conectado al SATA3. Recordamos que sólo los discos sda y sdb pertenecientes al raid md0, están preparados para poder iniciar el sistema, es decir, son los que tienen instalado el cargador de arranque *grub*. Como el SATA2 tiene un disco que no está preparado para arrancar(sdc) el sistema no puede iniciar. Esta situación se soluciona conectando el disco sdb al SATA1 o al SATA2, lo ideal es conectarlo al SATA1 ya que cuando conectemos el disco nuevo al SATA1 no encontramos nuevamente en que el sistema no arranca ya que ese disco no está preparado para iniciar el sistema operativo.

1st Drive	[SATA:PM-SAMSUNG HD] =
SATA 1	
2nd Drive	[SATA:PS-SAMSUNG HD] =
SATA 3	
3rd Drive	[SATA:SM-SAMSUNG HD] =
SATA 2	

Otra opción en vez de cambiar los cables, es asignar el orden de arranque en la BIOS en la sección "Boot > Hard Disk Drivers" sabiendo que la relación de los puertos SATA con los identificadores que se muestran(PM, PS, SM, etc.) es la que se muestra en la tabla, por ello los discos con 4th Drive [SATA:SS-SAMSUNG HD] = la etiqueta "PM" y "PS" que corresponden al SATA1(sda) y SATA3(sdb) están puestos los dos primeros.

Este extraño orden de asignación del puerto SATA3 con *sdb* sólo se entiende al comprobar que durante la secuencia de arranque vemos el siguiente orden en el que los discos son detectados:

				Mode	Mode	Info	Mode	Mode	Mode
SATA 1	:	Hard Disk	750.2GB	LBA	16Sec	Good	On	UDMA5	4
SATA 3	:	Hard Disk	750.2GB	LBA	16Sec	Good	On	UDMA5	4
SATA 2	:	Hard Disk	750.2GB	LBA	16Sec	Good	On	UDMA5	4
SATA 4	:	Hard Disk	750.2GB	LBA	16Sec	Good	On	UDMA5	4
SATA 5	:	Hard Disk	750.2GB	LBA	16Sec	Good	On	UDMA5	4
SATA 6	:	Hard Disk	750.2GB	LBA	16Sec	Good	On	UDMA5	4

Como vemos en la secuencia de detección de discos, la BIOS enumera el disco SATA3 antes que el SATA2(por eso suponemos que linux asigna *sdb* al SATA3). Sin embargo en la



secuencia de buscar el primer disco disponible para arrancar el sistema, la BIOS sí sigue la secuencia SATA1, SATA2, SATA3, etc.

En resumen, los discos que indique el raid md0(normalmente está formado por sda y sdb) independientemente del puerto SATA al que estén conectados, en la secuencia de arranque en la BIOS tienen que estar asignados al “1st Drive” y “2nd Drive”. El resto de los discos es indiferente al SATA donde se conecten y no existe problema en cambiarlos de puerto SATA en cualquier momento, ya que a la hora de asociar los RAID no se hace por el puerto SATA si no por un identificador que lleva cada disco.

Otro problema que podemos encontrar al iniciar el sistema con un disco fallido o desconectado es que este no consiga iniciar, mostrando el siguiente mensaje:

```
fscck desde util-linux-ng 2.17.2
/dev/mapper/gv_max-raiz: limpio, 56562/186944 ficheros, 266800/749568 bloques
El controlador de disco para /home no está listo o presente
Continúe esperando o pulse S para omitir o M para recuperar manualmente
```

En estos casos pulsamos la tecla M y saldremos a una consola de comandos donde ejecutaremos el comando “**cat /proc/mdstat**” para comprobar cuál de los raid no se ha puesto en marcha:

```
Filesystem check or mount failed.
A maintenance shell will now be started.
CONTROL-D will terminate this shell and continue booting after re-trying
filesystems. Any further errors will be ignored
root@max-server:~# cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md1 : inactive sdc1[0](S)
      2095040 blocks

md0 : active raid1 sda1[0] sdb1[1]
      2095040 blocks [2/2] [UU]

md2 : active raid1 sde1[1] sdd1[0]
      2096384 blocks [2/2] [UU]

unused devices: <none>
root@max-server:~#
```

En el ejemplo vemos que el raid *md1* está inactivo así que lo activamos ejecutando el comando



```
"mdadm --run /dev/md1:
root@max-server:~# mdadm --run /dev/md1
mdadm: started /dev/md1
root@max-server:~# cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md1 : active raid1 sdc1[0]
      2095040 blocks [2/1] [U_]

md0 : active raid1 sda1[0] sdb1[1]
      2095040 blocks [2/2] [UU]

md2 : active raid1 sde1[1] sdd1[0]
      2096384 blocks [2/2] [UU]

unused devices: <none>
root@max-server:~#
```

Si ejecutamos ahora **"cat /proc/mdstat"** podemos comprobar que ahora el raid ya aparece como activo. Ahora salimos de la consola pulsando "CTRL+D" o ejecutando **"exit"** y el equipo continuará la carga del sistema. Una vez arrancado el servidor hay que reiniciarlo para comprobar que ya inicia directamente con el raid en modo degradado y sin realizar ninguna pausa.

#### a) Cambio del disco

El proceso de cambio de un disco nuevo es igual para todos los discos con la excepción de que en los dos discos formados por el raid md0(los que tienen soporte para el arranque del sistema) se realiza un paso más para instalar *grub*. Los pasos son los siguientes, suponemos que ya hemos conectado el disco nuevo y arrancado el sistema:

Primero con el comando **"cat /proc/mdstat"** comprobaremos qué raid es el que está incompleto y cuál es el disco que falta en el raid:

```
root@max-server:/home/madrid# cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md1 : active raid1 sdc1[0] sdd1[1]
      732572608 blocks [2/2] [UU]

md0 : active raid1 sda1[0]
      732572608 blocks [2/1] [U_]

md2 : active raid1 sde1[0] sdf1[1]
      732572608 blocks [2/2] [UU]

unused devices: <none> root@max-server:/home/madrid#
```

En el ejemplo vemos que el raid incompleto es el *md0* y mirando todos los *sdX* que aparecen vemos que el disco que falta es el *sdb*. En el raid incompleto hay que copiar el primer sector del disco que está funcionando(*sda*) al disco nuevo que es el *sdb*, para ellos ejecutamos:

```
dd if=/dev/sda of=/dev/sdb bs=512 count=2048
```



Ahora hay que refrescar las tablas de particiones del kernel de linux del nuevo disco, para ello ejecutamos el comando: **`sfdisk -R /dev/sdb`**

Esto lo que hace es que se cree el dispositivo “/dev/sdb1” que antes no existía pues el disco al ser nuevo no tenía ninguna partición. Entonces ya podemos añadir la partición al raid incompleto ejecutando:

**`mdadm --manage /dev/md0 --add /dev/sdb1`**

Este commando anade la partición al raid y comienza su sincronización, la cual puede tardar hasta 4 horas. Por último, como el disco pertenece al raid *md0*, hay que instalarle el *grub*(si pertenece a otro raid no hay que instalarlo), ejecutamos:

**`grub-install --no-floppy /dev/sdb`**

**IMPORTANTE: Hay que tener cuidado con el comando grub-install para utilizar el nombre de dispositivo adecuado y NO añadir el número 1 al nombre del dispositivo(/dev/sdb).**

Se muestra un resumen de los comandos que se ejecutarían con su resultado:



```
root@max-server:/home/madrid# cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4]
[raid10] md0 : active raid1 sda1[1] 2095040 blocks [2/1] [_U]

md2 : active raid1 sdf1[1] sde1[0]
2096384 blocks [2/2] [UU]

md1 : active raid1 sdd1[1] sdc1[0]
2095040 blocks [2/2] [UU]

unused devices: <none>
root@max-server:/home/madrid# dd if=/dev/sda of=/dev/sdb bs=512
count=1 1+0 registros de entrada
1+0 registros de salida
512 bytes (512 B) copiados, 0,0264186 s, 19,4 kB/s root@max-
server:/home/madrid# sfdisk -R /dev/sdb
root@max-server:/home/madrid# mdadm --manage /dev/md0 --add /dev/sdb1
mdadm: added /dev/sdb1
root@max-server:/home/madrid# cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4]
[raid10] md0 : active raid1 sdb1[2] sda1[1] 2095040 blocks [2/1]
[_U]
[=>.....] recovery = 7.6% (161536/2095040) finish=0.7min
speed=40384K/sec

md2 : active raid1 sdf1[1] sde1[0]
2096384 blocks [2/2] [UU]

md1 : active raid1 sdd1[1] sdc1[0]
2095040 blocks [2/2] [UU]

unused devices: <none>
root@max-server:/home/madrid# grub-install --no-floppy /dev/sdb
Installation finished. No error reported.
root@max-server:/home/madrid#
```

## 26. EL DIRECTORIO /HOME/SAMBA/NETLOGON

Este directorio contiene los ficheros de configuración que se utilizan en la configuración y en el inicio de cada sesión de un usuario. Si accedemos desde Windows a [\\max-server](#), este permanece oculto, pero es accesible por todos los usuarios si se pone su ruta directa([\\maxserver\netlogon](#)) por ello no se debe de poner en él información confidencial sin los permisos adecuados:





```

root@max-server:/home/samba/netlogon# ls -l total 3312
-rw-r--r-- 1 root root 703 2011-03-21 09:25
Add_GroupPolicy_ControlPanel.zip
-rw-r--r-- 1 root root 16173 2011-03-21 09:25 AulaVirtual.zip
-rw-r--r-- 1 root root 129302 2011-03-21 09:25
Configuracion_Firefox_213.0.88.85.zip
-rw-r--r-- 1 root root 133534 2011-03-21 09:25
Configuracion_Firefox_sin_proxy.zip
-rw-r--r-- 1 root root 133534 2011-03-21 09:25 Configuracion_Firefox.zip
-rw-r--r-- 1 root root 6 2011-03-21 09:25 domain.txt
drw-r--r-- 2 root root 4096 2010-07-19 09:29 Fix-Windows7-server2008
-rw-r--r-- 1 root root 120628 2011-03-21 09:25 fondos-iconos.zip
-rw-r--r-- 1 root root 3271 2011-03-24 13:07
GroupPolicy_213.0.88.85.zip
-rw-r--r-- 1 root root 1963 2011-03-24 13:07 GroupPolicy_sin_proxy.zip
-rw-r--r-- 1 root root 3271 2011-03-24 13:07 GroupPolicy.zip
-rw-r--r-- 1 root root 315392 2011-03-21 09:25 kix32.exe
-rw-r--r-- 1 root root 483328 2011-03-21 09:25 KiXtart.dll
-rw-r--r-- 1 root root 209 2011-03-21 09:25 logon.bat
-rw-r--r-- 1 root root 7002 2011-03-21 09:25 logon.kix
-rw-r--r-- 1 root root 660 2011-03-21 09:25 mount.bat
-rw-r--r-- 1 root root 262144 2011-03-21 09:25 ntconfig.pol
-rw-r--r-- 1 root root 2605 2011-03-21 09:25 prepara_dominio_paso1.bat
-rw-r--r-- 1 root root 5092 2011-03-21 09:25 prepara_dominio_paso2.bat
-rw-r--r-- 1 root root 1414 2011-03-21 09:25 README.txt
-rw-r--r-- 1 root root 409 2011-03-21 09:25
Remove_GroupPolicy_ControlPanel.zip
-rw-r--r-- 1 root root 1435 2011-03-21 09:25 shares.kix
-rw-r--r-- 1 root root 290304 2011-03-21 09:25 subinacl.exe
-rw-r--r-- 1 root root 164864 2011-03-21 09:25 unzip.exe
-rw-r--r-- 1 root root 1168 2011-03-21 09:25
winvista.win7.win2008.registry.fix.bat
-rw-r--r-- 1 root root 319488 2011-03-21 09:25 wkix32.exe root@max-
server:/home/samba/netlogon#
  
```

Hay que distinguir el directorio “/home/samba” que tiene el propio servidor de centro, del “/home/samba” que se monta cuando se conecta al servidor de almacenamiento. No hay que trabajar nunca con “/home/samba” local del servidor de centro ya que cuando se conecta con el servidor de almacenamiento se sustituye el “/home/samba” local con el del servidor de almacenamiento. Podemos comprobar con el comando “mount” que estamos conectados al servidor de almacenamiento, visualizaremos una línea como esta:

```

/dev/nbd0 on /home/samba type ext4
(rw,usrquota,grpquota,acl,user_xattr)
  
```

## 27. COMO ACTUALIZAR EL FICHERO "CONFIGURACION FIREFOX.ZIP"

Este fichero contiene la configuración del firefox para Windows que se aplica la primera vez que el usuario inicia sesión o cuando se borra la carpeta “Programas” del escritorio.

La versión de Firefox en Windows instalada tanto en los servidores multipoint como en el equipo del profesor es la 3.6. En MAX la versión de Firefox es la 3.6.3. pero esta configuración



sólo es válida para Windows, en MAX el fichero que se toma como plantilla para todos los usuarios se encuentra en “/etc/firefox/profile/pref.js”.

Para actualizar el fichero “/home/samba/netlogon/Configuracion\_Firefox.zip” hay seguir los siguientes pasos:

- Entrar con un usuario con perfil de alumno, por ejemplo “alumno01”.
- Configurar el firefox con las preferencias que se quieran.
- Hacer limpieza en el firefox para que no quede basura(borrar historial, etc).
- Cerrar la sesión del usuario.
- Desde el servidor de centro como root ejecutar:
  - `cd/home/samba/profiles/alumno01.V2/AppData/`
  - `Roaming/Mozilla/`
  - `zip -r Configuracion_Firefox.zip Firefox/`
  - `mv Configuracion_Firefox.zip`
  - `/home/samba/netlogon/`

NOTA: sustituir en el primer comando “alumno01” por el nombre de la cuenta del usuario que se haya utilizado para configurar el firefox.

## 28. CREAR COPIA DE SEGURIDAD DE /HOME/SAMBA / CON 'TAR '

Debe tener en cuenta que el dispositivo de destino donde va a guardar la copia tenga suficiente espacio para que entre el fichero que se genere con “tar”. El siguiente comando le dará el tamaño en Megabytes del directorio “/home/samba”:

```
root@max-server:~# du -hs /home/samba
18M    /home/samba root@max-
server:~#
```

Tenga en cuenta que la copia generada con 'tar' es comprimida con “gzip” por lo que fácilmente el tamaño obtenido con el comando anterior, puede ser reducido a menos de la mitad.




El siguiente comando crea una copia comprimida con “gzip” del directorio “/home/samba” en un disco externo montado en “/mnt/usb”:

```
root@max-server:~# tar -czf /mnt/usb/home_samba_2010-10-12.gz /home/samba/
tar: Eliminando la '/' inicial de los nombres root@max-server:~#
```

Si queremos listar el contenido del archivo creado: `tar -tvf <nombre_del_archivo.gz>`

## 29. RESTAURAR COPIA DE SEGURIDAD DE /HOME/SAMBA CON 'TAR '

A la hora de restaurar tenga en cuenta el siguiente comportamiento:

-  La restauración mantendrá los permisos y propietarios originales que había en el momento de la copia.
-  Si ya existe un fichero este será eliminado y sustituido por el de la copia.
-  Los ficheros que ya existan en el destino pero no en la copia se mantendrán intactos.



Si no quiere mantener ningún resto antiguo de “/home/samba” elimine antes el directorio (rm -R /home/samba), no se recomienda al no ser que sepa lo que hace.

Para restaurar la copia ejecutamos el siguiente comando, sustituyendo el “<nombre de archivo>” por el correspondiente:

```
root@max-server:~# tar -xpvf <nombre del archivo> -C /
```

Cuando se hizo la copia se guardó con ruta relativa a “/”, es decir “home/samba”(sin el primer “/”), por lo que para restaurarla se pasa el parámetro “-C /” para que la ruta coincida con “/home/samba”.

Una vez restaurada la copia se pueden hacer ciertas comprobaciones. Mirar que los permisos y los propietarios de las carpetas son los correctos:

```
madrid@max-server:/home$ ls -l total 8
drwxr-xr-x 3 madrid madrid 4096 2010-10-05 23:21 madrid drwxr-xr-x 7 root
root 4096 2010-09-12 00:03 samba madrid@max-server:/home$ ls -l samba/ total
20
drwxr-xr-x 2 root root 4096 2010-09-12 00:03 groups drwxr-xr-x 2 root root
4096 2010-10-11 20:19 netlogon drwxr-xr-x 15 root root 4096 2010-10-11 01:16
profiles -rw-r--r-- 1 root root 0 2010-09-11 23:46 quota.group -rw-r--r-
- 1 root root 0 2010-09-11 23:46 quota.user drwxr-xr-x 5 root root 4096
2010-09-11 23:46 shares drwxr-xr-x 9 root root 4096 2010-10-11 01:16 users
madrid@max-server:/home$ ls -l samba/profiles/ total 52
drwx-----x 2 Alumno01 Domain Users 4096 2010-10-10 20:45 Alumno01 drwx-
----x 8 Alumno01 Domain Users 4096 2010-10-11 21:02 Alumno01.V2 drwx-
----x 2 coordinadortic Domain Users 4096 2010-09-12 00:03 coordinadortic
drwx-----x 8 coordinadortic Domain Users 4096 2010-10-11 19:59
coordinadortic.V2 drwx-----x 2 max-control Domain Users 4096 2010-09-12
00:41 max-control drwx-----x 2 max-control Domain Users 4096 2010-09-12
00:41 max-control.V2 drwx-----x 2 Profesor01 Domain Users 4096 2010-10-
10 16:44 Profesor01 drwx-----x 8 Profesor01 Domain Users 4096 2010-10-
11 20:50 Profesor01.V2 madrid@max-server:/home$ ls -l samba/users total 28
drwx-----x 9 Alumno01 Domain Users 4096 2010-10-10 23:07 Alumno01 drwx-
----x 9 coordinadortic Domain Users 4096 2010-10-11 01:18 coordinadortic drwx-
----x 2 max-control Domain Users 4096 2010-09-12 00:41 max-control drwx-
----x 9 Profesor01 Domain Users 4096 2010-10-10 16:47 Profesor01 madrid@max-
server:/home$
```

Dentro del perfil de un usuario, este tiene que tener como propietario a él mismo y como grupo a “\_\_USERS\_\_”:

```
root@max-server:/home# ls -l
samba/profiles/Alumno01.V2/ total 544
drwx----- 3 Alumno01 __USERS__ 4096 2010-10-10
23:07 AppData drwx----- 2 Alumno01 __USERS__ 4096
2010-10-10 23:07 Contacts drwx----- 7 Alumno01
__USERS__ 4096 2010-10-10 23:07 Favorites drwx-----
2 Alumno01 __USERS__ 4096 2010-10-10 23:07 Links -
rw----- 1 Alumno01 __USERS__ 524288 2010-10-11 21:02
NTUSER.DAT
-rw----- 1 Alumno01 __USERS__ 160 2010-10-11
21:02 ntuser.ini -r----- 1 Alumno01 __USERS__
```



```
3054 2010-10-11 20:00 ntuser.pol drwx----- 2 Alumno01
__USERS__ 4096 2010-10-10 23:07 Saved Games drwx----
-- 2 Alumno01 __USERS__ 4096 2010-10-10 23:07
Searches root@max-server:/home# ls -l
samba/users/Alumno01/ total 28
drwxr-xr-x 3 Alumno01 __USERS__ 4096 2010-10-10 23:07
Descargas drwxr-xr-x 3 Alumno01 __USERS__ 4096 2010-
10-10 23:07 Documentos drwxr-xr-x 5 Alumno01 __USERS__
4096 2010-10-11 21:01 Escritorio drwxr-xr-x 3 Alumno01
__USERS__ 4096 2010-10-10 23:07 Imagenes drwxr-xr-x 3
Alumno01 __USERS__ 4096 2010-10-10 23:07 Musica drwxr-
xr-x 3 Alumno01 __USERS__ 4096 2010-10-10 23:07
Plantillas drwxr-xr-x 3 Alumno01 __USERS__ 4096 2010-
10-10 23:07 Videos root@max-server:/home#
```

### 30. APAGADO / REINICIO DEL SERVIDOR

Para apagar o reiniciar el servidos se pueden utilizar los típicos comandos de apagado “poweroff” o “shutdown” los cuales necesitan privilegios de root.

El personal del centro puede apagar el servidor del centro sin necesidad de privilegios pulsando el botón de encendido/apagado del mismo. Cuando se hace de esta manera se lanza el script “/etc/acpi/powerbtn.sh”.

### 31. CONFIGURAR EL BOTÓN DE ENCENDIDO/APAGADO

Para que funcione el apagado mediante el botón del equipo hay que instalar el paquete **acpid**(**aptget install acpid**). En el servidor de almacenamiento funcionará inmediatamente después de la instalación pero el servidor de centro necesita ser reiniciado.

Una vez instalado este paquete, cuando se pulsa el botón de encendido/apagado se ejecutará el script “/etc/acpi/powerbtn.sh”, este es su contenido:

```
#!/bin/sh
# /etc/acpi/powerbtn.sh
# Initiates a shutdown when the power putton has
been # pressed.

# Skip if we just in the middle of resuming.
test -f /var/lock/acpisleep && exit 0

# If gnome-power-manager, kded4, dalston-power-applet or xfce4-power-manager
# are running, let them handle policy This is effectively the same as
# 'acpi-support's '/usr/share/acpi-support/policy-funcs' file.

if pidof gnome-power-manager kded4 dalston-power-applet xfce4-power-manager >
/dev/null;
then      exit
fi

# If all else failed, just initiate a plain shutdown.
/sbin/shutdown -h now "Power button pressed"
```



## 32. RESOLUCIÓN DE PROBLEMAS

### a) Reparar ficheros de cuotas

Síntoma: No aparecen las cuotas en el panel de max-control.

```
...
...
*   Add group MA.1AB
*   Add group RMT-1C
*   Disabling quotas on /home/samba
*   Enabling quotas on /home/samba
quotaon: No se puede encontrar el archivo de cuota en /home/samba
[/dev/nbd0] pa ra encender/apagar las cuotas.
quotaon: No se puede encontrar el archivo de cuota en /home/samba
[/dev/nbd0] pa ra encender/apagar las cuotas. group quota en /home/samba
(/dev/nbd0) es apagado user quota en /home/samba (/dev/nbd0) es apagado
setquota: El archivo de Cuota no fue encontrado o tiene un formato
incorrecto.
*   Set quota for user acabanillas (teacher) 4000 MB
*   Set quota for user acamaraesclapez (teacher) 4000 MB
*   Set quota for user adriana.tirado 2000 MB
*   Set quota for user agonzalezmartinez (teacher) 4000 MB
*   Set quota for user agustin.devesa (teacher) 4000 MB ...
...
```

Si hacemos un “dpkg-reconfigure max-control” se observan los siguientes errores:

Usando el comando “quotacheck” también se puede comprobar que devuelve un mensaje de error. Una posible causa de estos errores es que los ficheros de cuota se hayan corrompido.

Existen los dos siguientes ficheros de cuota:

/home/samba/quota.user  
/home/samba/quota.group

Para crear de nuevo estos dos ficheros ejecutar como “root” el script “reset-quota”. Otra forma de hacerlo manualmente sería ejecutando los siguientes comandos:

```
cd
/home/samba
quotaoff
/home/samba/
rm
quota.user
rm
quota.group
quotacheck -u -c --format=vfsold
/home/samba/ quotacheck -g -c --
format=vfsold /home/samba/
```



```
quotaon dpkg-  
reconfigure max-  
control
```

NOTA: Si sólo se desea restaurar uno de los ficheros de cuota, omitir el comando “rm” y el “quotacheck” correspondiente al fichero que deseamos conservar. Si el comando “quotacheck” da algún error comprobar que no hay usuarios usando el servidor(smbstatus).

### Unir una partición perdida al RAID

Visualizamos el estado de los discos:

```
root@almacen:~# cat /proc/mdstat  
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4]  
[raid10] md3 : active raid10 sda4[0] sde4[4] sdc4[2] sdf4[5] sdd4[3]  
2132683584 blocks 64K chunks 2 near-copies [6/6] [U_UUUU]  
  
md2 : active raid10 sda3[0] sdb3[1] sdd3[3] sdc3[2] sde3[4] sdf3[5]  
58592064 blocks 64K chunks 2 near-copies [6/6] [UUUUUU]  
  
md1 : active raid10 sdc2[2] sdd2[3] sda2[0] sdf2[5] sde2[4]  
5858112 blocks 64K chunks 2 near-copies [6/6] [U_UUUU]  
  
md0 : active raid1 sdd1[3] sdc1[2] sdb1[4] sdf1[5] sde1[1]  
194496 blocks [6/6] [UUUU_U]  
  
unused devices: <none>  
root@almacen:~#
```

En el ejemplo vemos que los RAID md0, md1 y md3 han perdido una partición. Si observamos que se ha perdido la misma partición en todos los RAID, puede ser debido a que el disco completo ha dejado de estar reconocido por el sistema. Una causa típica es por una mala conexión del cableado, se debería entonces comprobar en la BIOS si vemos todos los discos o no. Antes podemos comprobar si todos los discos y sus particiones han sido detectadas, deberemos ver un listado como este:

```
root@almacen:~# ls -l /dev/sd*  
brw-rw---- 1 root disk 8, 0 2010-10-16 16:22 /dev/sda brw-rw---- 1 root disk  
8, 1 2010-10-16 16:22 /dev/sda1 brw-rw---- 1 root disk 8, 2 2010-10-16 16:22  
/dev/sda2 brw-rw---- 1 root disk 8, 3 2010-10-16 16:22 /dev/sda3 brw-rw---- 1  
root disk 8, 4 2010-10-16 16:22 /dev/sda4 brw-rw---- 1 root disk 8, 16 2010-  
10-16 16:22 /dev/sdb brw-rw---- 1 root disk 8, 17 2010-10-16 16:22 /dev/sdb1  
brw-rw---- 1 root disk 8, 18 2010-10-16 16:22 /dev/sdb2 brw-rw---- 1 root disk  
8, 19 2010-10-16 16:22 /dev/sdb3 brw-rw---- 1 root disk 8, 20 2010-10-16 16:22  
/dev/sdb4 brw-rw---- 1 root disk 8, 32 2010-10-16 16:22 /dev/sdc brw-rw---- 1  
root disk 8, 33 2010-10-16 16:22 /dev/sdc1 brw-rw---- 1 root disk 8, 34 2010-  
10-16 16:22 /dev/sdc2 brw-rw---- 1 root disk 8, 35 2010-10-16 16:22 /dev/sdc3  
brw-rw---- 1 root disk 8, 36 2010-10-16 16:22 /dev/sdc4 brw-rw---- 1 root disk  
8, 48 2010-10-16 16:22 /dev/sdd brw-rw---- 1 root disk 8, 49 2010-10-16 16:22  
/dev/sdd1 brw-rw---- 1 root disk 8, 50 2010-10-16 16:22 /dev/sdd2 brw-rw---- 1  
root disk 8, 51 2010-10-16 16:22 /dev/sdd3 brw-rw---- 1 root disk 8, 52 2010-  
10-16 16:22 /dev/sdd4 brw-rw---- 1 root disk 8, 64 2010-10-16 16:22 /dev/sde  
brw-rw---- 1 root disk 8, 65 2010-10-16 16:22 /dev/sde1 brw-rw---- 1 root disk  
8, 66 2010-10-16 16:22 /dev/sde2 brw-rw---- 1 root disk 8, 67 2010-10-16 16:22  
/dev/sde3 brw-rw---- 1 root disk 8, 68 2010-10-16 16:22 /dev/sde4 brw-rw---- 1  
root disk 8, 80 2010-10-16 16:22 /dev/sdf brw-rw---- 1 root disk 8, 81 2010-  
10-16 16:22 /dev/sdf1 brw-rw---- 1 root disk 8, 82 2010-10-16 16:22 /dev/sdf2  
brw-rw---- 1 root disk 8, 83 2010-10-16 16:22 /dev/sdf3 brw-rw---- 1 root disk  
8, 84 2010-10-16 16:22 /dev/sdf4  
root@almacen:~#
```





Comprobamos que en el listado aparecen 6 discos: sda, sdb, sdc, sdd, sde y sdf y cada uno tiene 4 particiones. Si vemos que todo está correcto podemos añadir la partición perdida al raid.

Continuando con el ejemplo, al RAID “md3” le faltaba la partición “sdb4”:

```
md3 : active raid10 sda4[0] sde4[4] sdc4[2] sdf4[5] sdd4[3]
2132683584 blocks 64K chunks 2 near-copies [6/6] [U_UUUU]
```

Dentro de un RAID el número de todas las particiones es el mismo, el 4 en este caso, no equivocarse en este número al añadir la partición correspondiente al raid.

Para añadir dicha partición ejecutamos:

```
mdadm --manage /dev/md3 --add /dev/sdb4
```

Al raid “md1” le falta la partición “sdb2”, ejecutamos:

```
mdadm --manage /dev/md2 --add /dev/sdb2
```

Al raid “md0” le falta la partición “sda1”, ejecutamos:

```
mdadm --manage /dev/md0 --add /dev/sda1
```

Se pueden ejecutar las tres líneas seguidas de forma que los trabajos de sincronización se irán encolando.

### **Error al hacer login en Windows**

Existen varias causas por las que no se consiga iniciar sesión en Windows. La comentada aquí es debido a que se ha unido al dominio un equipo con Windows XP provocando que cambie el comportamiento del servicio WINS en el servidor de centro y deje de validar las sesiones de usuarios, sin embargo en MAX sí que podemos iniciar sesión.

Para saber si es debido a que está fallando el servicio WINS, se puede consultar el fichero “/var/log/samba/nmbd”, encontraremos unas líneas que están dando error:



```
[2011/04/26 14:02:50, 0] nmbd/nmbd_nameregister.c:72(register_name_response)
register_name_response: Answer name MADRID<00> differs from question name
MADRID<1e>.
[2011/04/26 14:02:50, 0] nmbd/nmbd_nameregister.c:72(register_name_response)
register_name_response: Answer name MADRID<00> differs from question name
MADRID<1c>.
[2011/04/26 14:02:52, 0]
nmbd/nmbd_workgroupdb.c:225(fail_register) fail_register: Failed to
register name MADRID<00> on subnet 192.168.10.1. [2011/04/26
14:02:52, 0] nmbd/nmbd_namelistdb.c:307(standard_fail_register)
standard_fail_register: Failed to register/refresh name MADRID<00> on subnet
192.168.10.1
[2011/04/26 14:02:52, 0]
nmbd/nmbd_workgroupdb.c:225(fail_register) fail_register: Failed to
register name MADRID<1e> on subnet 192.168.10.1. [2011/04/26
14:02:52, 0] nmbd/nmbd_namelistdb.c:307(standard_fail_register)
standard_fail_register: Failed to register/refresh name MADRID<1e> on subnet
192.168.10.1
[2011/04/26 14:02:52, 0] nmbd/nmbd_logonnames.c:62(become_logon_server_fail)
become_logon_server_fail: Failed to become a domain master for workgroup MADRID on
subnet 192.168.10.1. Couldn't register name MADRID<1c>.
[2011/04/26 14:02:52, 0] nmbd/nmbd_namelistdb.c:307(standard_fail_register)
standard_fail_register: Failed to register/refresh name MADRID<1c> on subnet
192.168.10.1 [2011/04/26 14:02:54, 0]
nmbd/nmbd_logonnames.c:121(become_logon_server_success)
become_logon_server_success: Samba is now a logon server for workgroup MADRID on
subnet 192.168.11.1
[2011/04/26 14:02:58, 0] nmbd/nmbd_become_dmb.c:110(become_domain_master_stage2)
*****

Samba server MAX-SERVER is now a domain master browser for workgroup MADRID on
subnet
192.168.10.1

*****
[2011/04/26 14:02:58, 0] nmbd/nmbd_become_dmb.c:110(become_domain_master_stage2)
*****

Samba server MAX-SERVER is now a domain master browser for workgroup MADRID on
subnet
192.168.11.1

*****
[2011/04/26 14:03:12, 0] nmbd/nmbd_become_lmb.c:395(become_local_master_stage2)
*****

Samba name server MAX-SERVER is now a local master browser for workgroup MADRID on
subnet 192.168.11.1

*****
```

De momento no se ha encontrado la configuración adecuada para que “Windows XP” no interfiera con el servidor de centro por lo que la única solución es desconectar el equipo con “Windows XP” y reiniciar el servidor.

### 33. CAMBIO DE UNA INTERFAZ DE RED

Los nombres de las interfaces de red “eth0”, “eth1”, “eth2”, etc., se asocian con la MAC de la interfaz en un momento concreto de detección de nuevo hardware durante el inicio del



equipo y no se libera. Eso quiere decir que si cambiamos por avería la tarjeta de red asociada por ejemplo con la interfaz “eth2”, la etiqueta “eth2” queda asociada a la MAC de la tarjeta averiada, por lo que a la nueva tarjeta de red le asignara la siguiente etiqueta libre, “eth3”. Como hay configuraciones que hacen referencia por la etiqueta de la interfaz, se debe de reasignar el nombre de la etiqueta para que la nueva tarjeta de red tenga la misma que antes.

Podemos ver la asignación de etiqueta/MAC en el fichero “/etc/udev/rules.d/70-persistentnet.rules”, por ejemplo este sería el de un servidor de centro:

```
madrid@max-server:/var/log/samba$ cat /etc/udev/rules.d/70-
persistentnet.rules
# This file was automatically generated by the
/lib/udev/write_net_rules # program, run by the persistent-net-
generator.rules file.
#
# You can modify it, as long as you keep each rule on
a single # line, and change only the value of the
NAME= key.

# PCI device 0x10ec:0x8168 (r8169)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*",
ATTR{address}=="00:1a:92:38:XX:XX", ATTR{dev_id}=="0x0",
ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"

# PCI device 0x10ec:0x8169 (r8169)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*",
ATTR{address}=="00:16:0a:24:XX:XX", ATTR{dev_id}=="0x0",
ATTR{type}=="1",
KERNEL=="eth*", NAME="eth2"

# PCI device 0x10ec:0x8169 (r8169)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*",
ATTR{address}=="00:16:0a:24:XX:XX", ATTR{dev_id}=="0x0",
ATTR{type}=="1",
KERNEL=="eth*", NAME="eth1" madrid@max-
server:/var/log/samba$
```

Vemos que hay tres líneas, una por cada interfaz (como no entra en una línea se ve en 2 pero realmente es una línea). Cuando se cambie alguna de las tarjetas de red, en este fichero aparecerá una nueva línea correspondiente a la nueva tarjeta de red, sabremos cual es por la MAC y por qué se le habrá asignado la siguiente etiqueta libre, “eth3”, entonces habrá que editar este fichero y borrar la línea de la tarjeta antigua y renombrar “eth3”(el atributo “NAME=” de final de la línea) y poner la etiqueta que le corresponda.

En cualquier caso, el fichero “/etc/udev/rules.d/70-persistent-net.rules” se puede eliminar sin problemas ya que al siguiente reinicio el sistema lo vuelve a crear, pero entonces tendremos que tener en cuenta si se han asignado correctamente las etiquetas con las interfaces. En caso negativo entonces podemos editarlo y reasignar los nombres de las interfaces según nuestras preferencias(es necesario reiniciar para que se apliquen los cambios del fichero).



## 34. ALGUNA DE LAS INTERFACES DE RED NO RESPONDE

Se ha detectado que en ciertas condiciones, alguna de las interfaces puede dejar de responder. El comando *ifconfig* devuelve bien la configuración pero en el *dashboard* o el comando *mii-tool* informa de que dicha interfaz no tiene link. Si miramos los led de actividad de la interfaz en la parte de atrás del equipo podemos comprobar que no hay ningún led encendido.

Para resolver este problema hay que apagar el servidor, desconectar el cable eléctrico de alimentación, esperar un minuto aproximadamente para que el equipo se descargue completamente y entonces volverlo a encender.

## 35. COMANDOS DE INTERÉS

### a) Abrir una consola(cmd) de Windows desde el servidor de centro

En el servidor de centro existe el comando “winexe” con el que podemos conectarnos a un equipo Windows y ejecutar comandos de consola. Con el siguiente comando podemos abrir un “cmd” o símbolo del sistema(cambiar los datos de usuario, contraseña e IP por los adecuados):

```
winexe -U administrador%contraseña --interactive=0 //192.168.10.14 "cmd"
```

Podemos ejecutar comandos directamente sin abrir una consola. Se muestran algunos comandos útiles:

```
Comprobar si Windows está activado: winexe -U  
administrador%contraseña --interactive=0 //192.168.10.14  
"cscript c:\windows\system32\slmgr.vbs -dli"
```

Listar las impresoras instaladas:

```
winexe -U administrador%cmadrid --interactive=0 //192.168.10.14 "wmic printer  
list brief"
```

### b) Averiguar las conexiones activas de SAMBA

Con el comando “smbstatus” se puede obtener mucha información de las conexiones activas y los usuarios que tiene abierto SAMBA. Consultar la ayuda(man smbstatus) para ver los diferentes parámetros que se pueden pasar a este comando, algunos de los más utiles son “smbstatus -b” y “smbstatus -S”.

### c) Reiniciar un equipo en Windows desde el servidor de centro

Entre las utilidades de samba se encuentra el comando “net” que sirve para muchas cosas, entre ellas podemos reiniciar un equipo que se encuentra en Windows de forma muy sencilla:



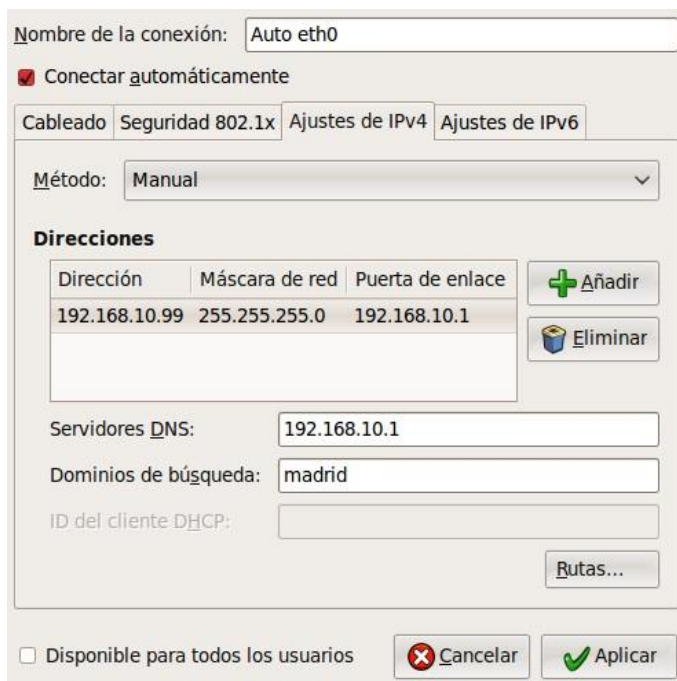
```
net rpc shutdown -r -I 192.168.10.14 -U ".\administrador%cmadrid"
```

Si queremos apagar, en vez de reiniciar cambiaríamos el parámetro “-r” por “-p”. Otra forma sería utilizar el shutdown de Windows utilizando el comando winexe visto anteriormente para conectarnos al equipo.



## F. PROCEDIMIENTO: CONFIGURACIÓN EQUIPO DE ALUMNO CON TERMINALES USB

1. *(Sólo en equipos de alumno)* Desconectar todos los terminales multipoint de los puertos USB del equipo.
2. *(Sólo en equipos de alumno)* Conectar directamente teclado, ratón y monitor al PC para remaquetarlo (en el equipo de profesor no hace falta porque ya tienen que estar conectados).
3. El proceso de instalación de la maqueta en un equipo comienza conectando el disco que contiene la maqueta en el ordenador que queremos instalar y presionando la tecla "F11" inmediatamente después de que comience el arranque de la BIOS, acción que nos permitirá acceder al menú para elegir el dispositivo de inicio de sistema, donde seleccionaremos la unidad de disco duro externo (en caso de encontrarse la maqueta en un disco duro USB), o la unidad óptica (en caso de encontrarse en un DVD). Esto nos lanzará el menú de Bakarddhi que nos permite **Restaurar la imagen** que queremos del equipo, ya se trate del equipo de Profesor o de Alumno.
4. Actualizar y Configurar [la BIOS \(ver al final de este documento\)](#)
5. Iniciar en MAX (comprobar que ya debe de aparecer el menú de arranque PXE del servidor en cada arranque). Aparecerá la pantalla de "login" de MAX en modo texto, logarse con el usuario "madrid" y ejecutar el comando "**startx**" que arranca el modo gráfico.
6. Ya en modo gráfico, abrir un terminal y ejecutar el comando "**sudo configurar\_equipo**" desde el menú "Accesorios > Terminal", es un script que primero ejecuta el comando "nmconnection-editor" desde donde configuraremos la IP (Equivale a "Botón derecho icono de red > Editar las conexiones..."):



Nombre de la conexión: Auto eth0

☒ Conectar automáticamente

Cableado Seguridad 802.1x Ajustes de IPv4 Ajustes de IPv6

Método: Manual

**Direcciones**

Dirección	Máscara de red	Puerta de enlace
192.168.10.99	255.255.255.0	192.168.10.1

+ Añadir

Eliminar

Servidores DNS: 192.168.10.1

Dominios de búsqueda: madrid

ID del cliente DHCP:

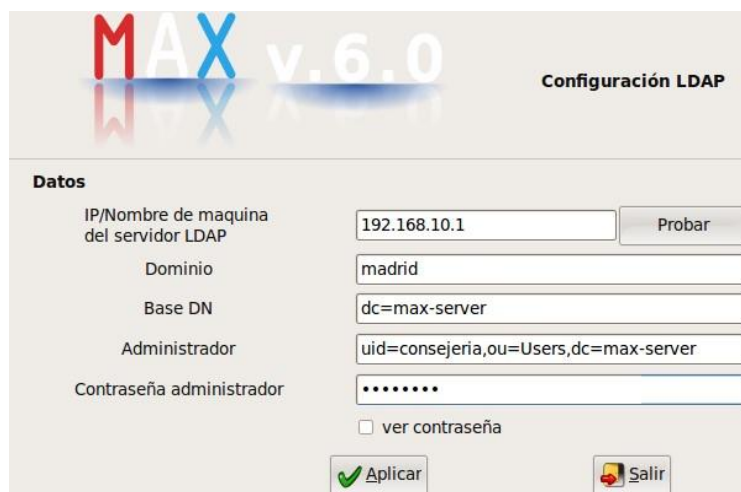
Rutas...

☐ Disponible para todos los usuarios

Cancelar Aplicar

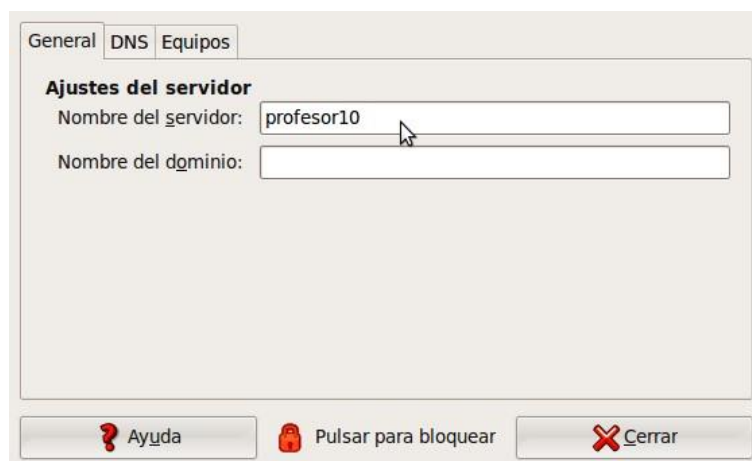






The image shows the 'MAX v.6.0 Configuración LDAP' window. It has a title bar with the MAX logo and version. The window is divided into a header and a main area. The header contains the title. The main area is titled 'Datos' and contains several input fields: 'IP/Nombre de maquina del servidor LDAP' with the value '192.168.10.1', 'Dominio' with 'madrid', 'Base DN' with 'dc=max-server', 'Administrador' with 'uid=consejeria,ou=Users,dc=max-server', and 'Contraseña administrador' with a masked password. There is a 'Probar' button next to the IP field and a 'ver contraseña' checkbox. At the bottom, there are 'Aplicar' and 'Salir' buttons.

El script luego ejecuta el comando “network-admin” desde donde cambiaremos el nombre del equipo (Equivale a “Sistema > Administración > Red”):



The image shows the 'General DNS Equipos' window. It has a title bar with the tabs 'General', 'DNS', and 'Equipos'. The 'General' tab is selected. The window is titled 'Ajustes del servidor' and contains two input fields: 'Nombre del servidor' with the value 'profesor10' and 'Nombre del dominio' which is empty. At the bottom, there are three buttons: 'Ayuda', 'Pulsar para bloquear', and 'Cerrar'.

Al cerrar este último asistente el equipo se reiniciará automáticamente. Volver a iniciar en MAX y entrar con el usuario “madrid”.

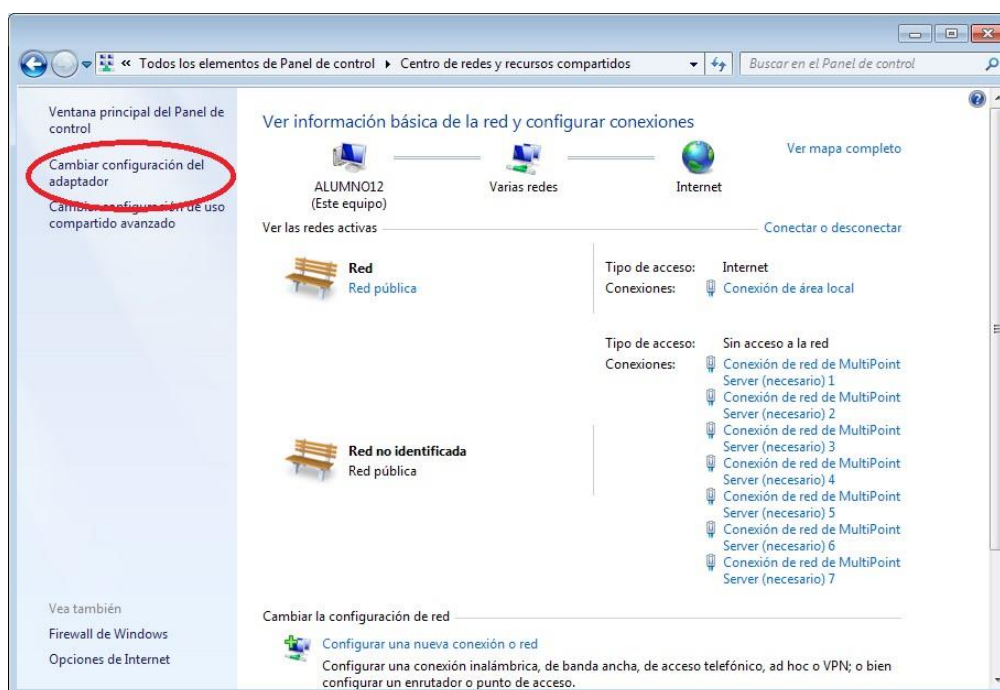
7. Instalar la impresora en MAX (existe un documento aparte llamado [“Cómo instalar la impresora en Windows y Max Linux”](#)).
8. Abrir un terminal y ejecutar el comando “**sudo apt-get update**” para actualizar los repositorios de paquetes.
9. Unirlo al servidor LDAP desde el menú “Sistema > Administración > Configurar MAX como cliente LDAP”.

En IP del servidor LDAP pondremos siempre la IP “192.168.10.1”, en el Dominio “madrid”, Base DN lo dejamos como está, en Administrador sustituimos el “uid=admin” por “uid=consejeria” y en Contraseña administrador le ponemos la clave actual del usuario “consejeria”.

10. Una vez unido al LDAP ya podemos reiniciar en Windows (con el comando de Terminal “sudo reboot”). Iniciar sesión con el usuario “Administrador”.



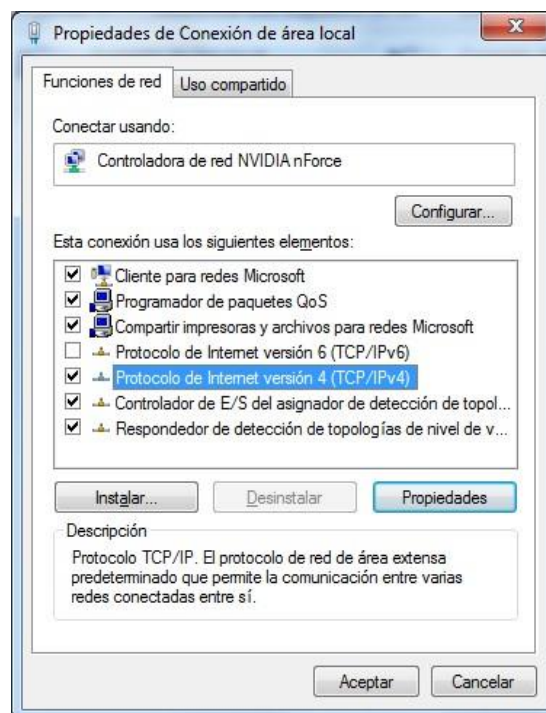
11. Cambiar la IP del equipo. Para esto vamos a “Panel de Control > Centro de Redes y recursos compartidos > Cambiar configuración del adaptador”.



Seleccionamos la interfaz de red de “Conexión de área local” y accedemos a las Propiedades de la misma con el Botón derecho del ratón. Seleccionamos el Protocolo de Internet

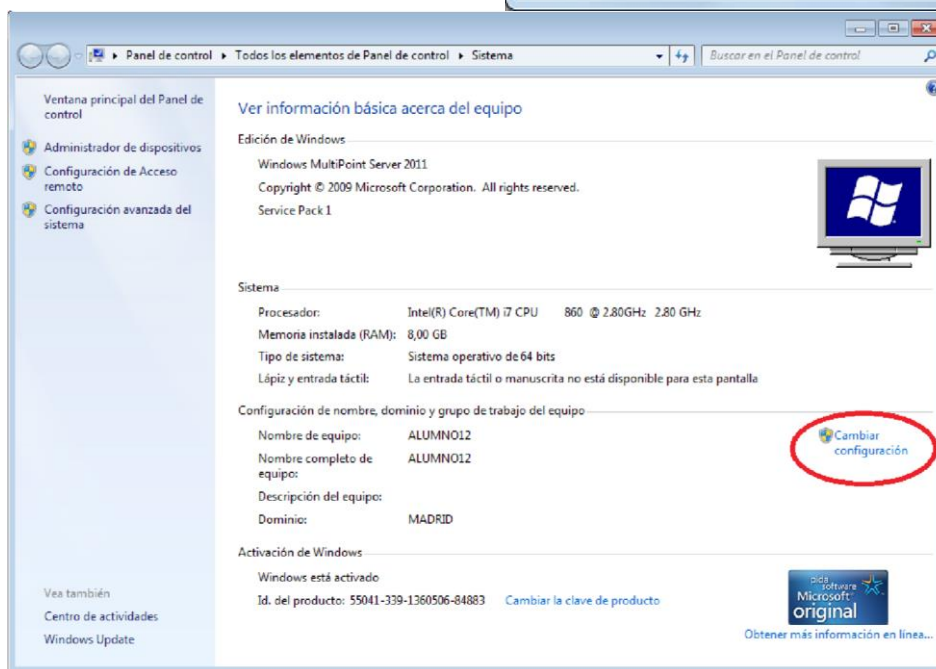
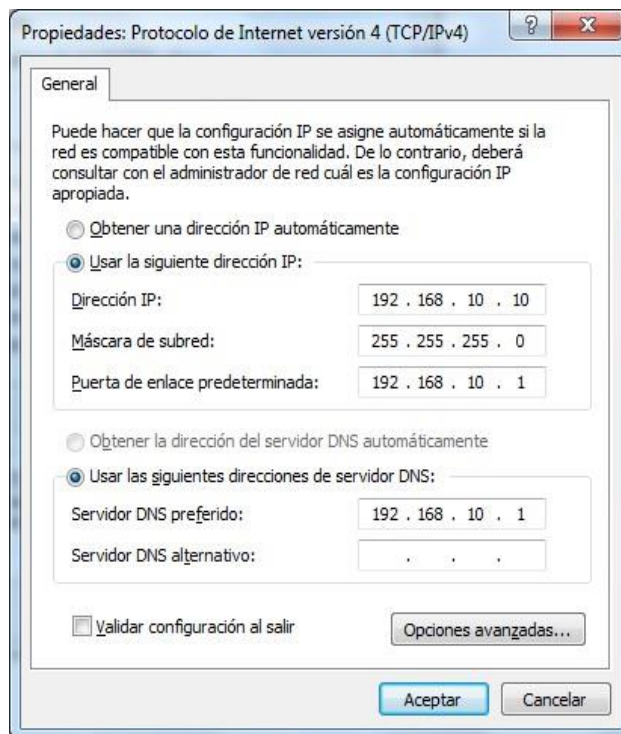
(TCP/IP v4) y le damos al botón de

“Propiedades” del mismo.



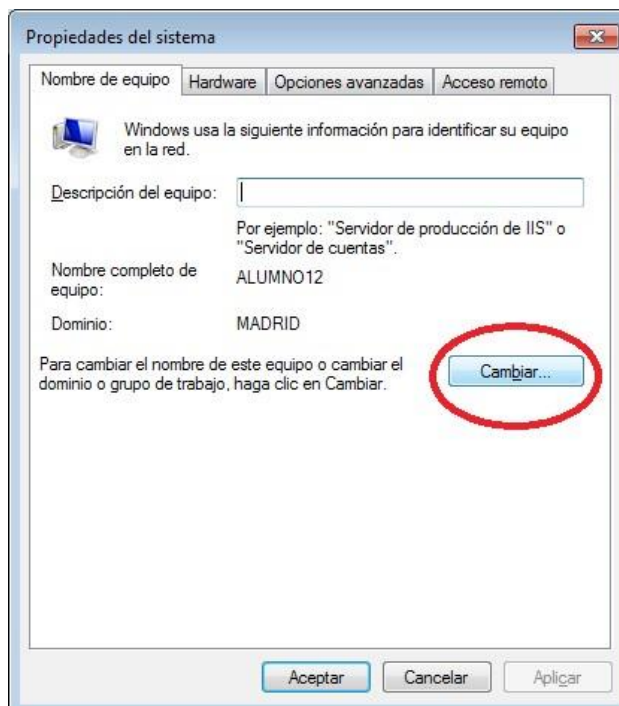
Le introducimos a mano la dirección IP que le queremos asignar a ese equipo en el campo “Dirección IP” y le damos al botón de “Aceptar”.

12. Para cambiar el nombre del equipo desplegamos el menú “Inicio” y hacemos clic derecho en el icono “Equipo”. Aparece un menú contextual donde elegimos la opción “Propiedades”. Nos aparece la siguiente pantalla donde seleccionaremos la opción “Cambiar configuración”.

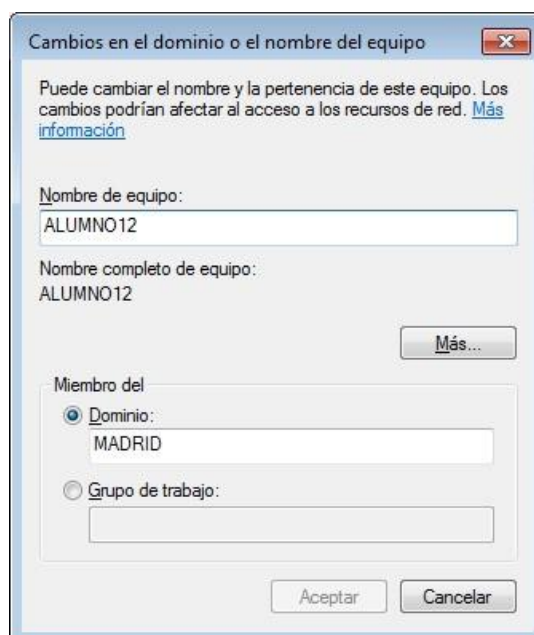


En la siguiente pantalla le damos al botón de “Cambiar”.





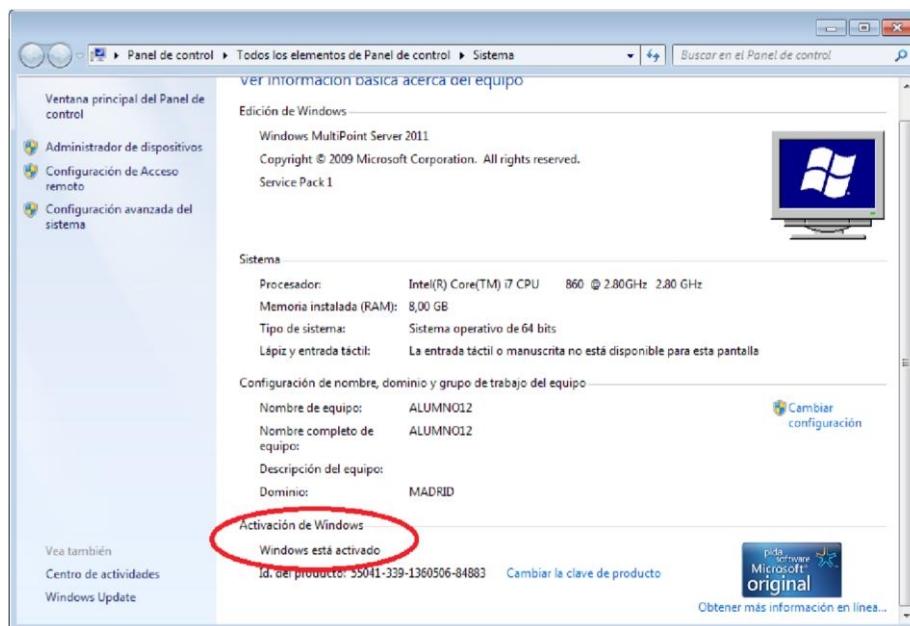
Ponemos el nombre de equipo deseado en “Nombre de equipo”



Para que los cambios realizados tengan efecto se debe realizar un reinicio del equipo, poniendo antes el login del usuario “Administrador” del equipo.

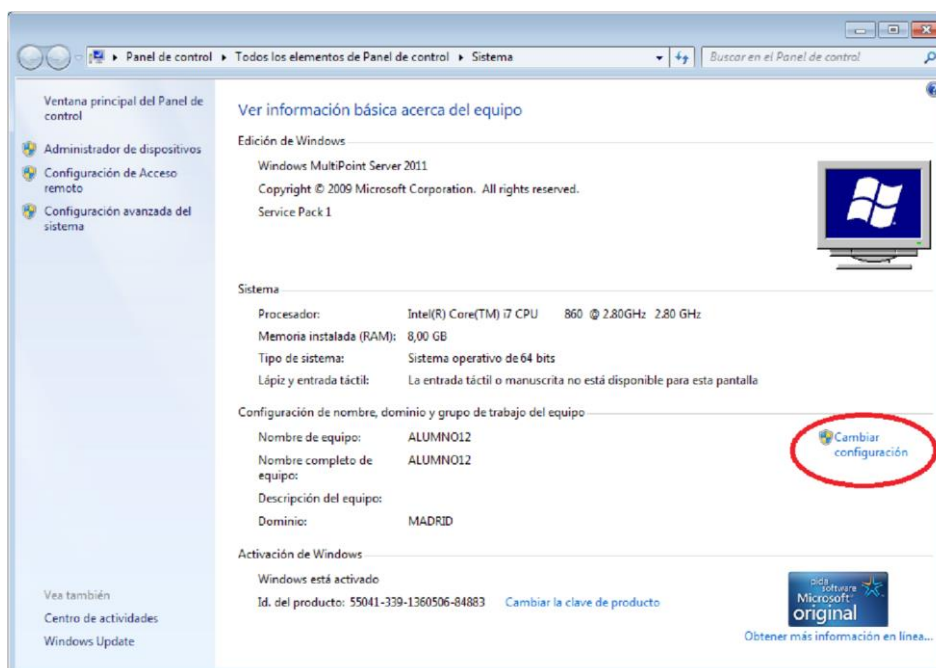
13. Activar la licencia de Windows. Vamos a la opción de menú contextual de “Equipo” en el menú Inicio de Windows, y en la sección de “Activación de Windows”, activamos la licencia dando al enlace que aparece al respecto donde indica los días que quedan para la expiración.





14. Instalar la impresora en Windows.

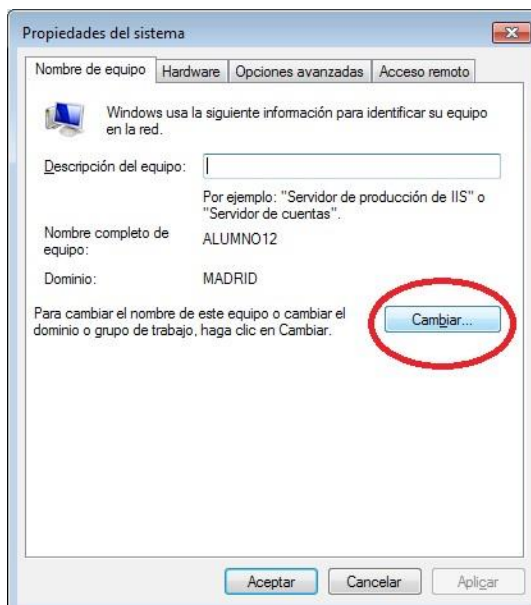
15. Para unir el equipo al dominio utilizar las credenciales del usuario “consejeria”. No reiniciar cuando lo pida. Desplegamos el menú “Inicio” y hacemos clic derecho en el icono “Equipo”. Aparece un menú contextual donde elegimos la opción “Propiedades”. Nos aparece la siguiente pantalla donde seleccionaremos la opción “Cambiar configuración”.



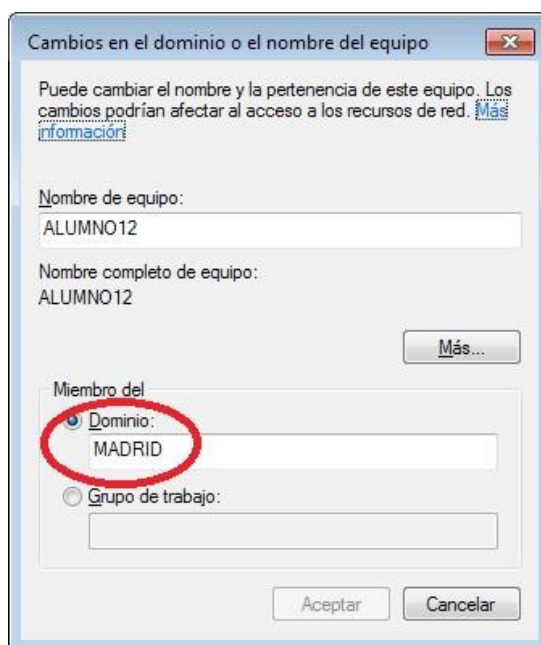
En la siguiente pantalla le damos al botón de “Cambiar”







En esta pantalla se especifica el nombre de dominio y se le da a “Aceptar”. Después de introducir las credenciales del usuario “Administrador”, el equipo necesita reiniciarse para que los cambios sean efectivos.



16. Abrir la ruta “\\max-server\netlogon” (cuando pida credenciales usar las del usuario “consejería”) y ejecutar el script “**prepara\_dominio\_paso2.bat**”. Comprobar que se ejecuta el primer paso correctamente, pulsar alguna tecla en la pantalla negra que aparece para que se ejecuten correctamente los comandos del script y repetir la misma operación en el segundo paso para que se cierre la pantalla de ejecución del script.





```
C:\Windows\system32\cmd.exe

Este script se debe ejecutar con permisos de administrador(boton
derecho "Ejecutar como administrador")

Este script prepara Windows 7 y Multipoint Server 2010/2011 para
trabajar en el dominio de las aulas tecnologicas.

Si tiene problemas para ejecutar este script, desactive el "Control
de cuentas de usuario" desde el Panel de control > Cuentas de usuario

Pulse CTRL+C si desea cancelar, otra tecla para continuar...
_
```

```
C:\Windows\system32\cmd.exe

Conectando unidad de red w:\(\max-server\netlogon)...
Se ha completado el comando correctamente.

Ya existe el subdirectorio o el archivo c:\Windows\educamadrid.
Copiando politicas de grupo a C:\Windows\System32\GroupPolicy...
C:\borrame\gpt.ini
C:\borrame\Machine\Registry.pol
C:\borrame\User\Registry.pol
C:\borrame\User\MICROSOFT\IEAK\install.ins
4 archivo(s) copiado(s)
Copiando mount.bat a C:\Windows\System32...
1 archivo(s) copiado(s).

Desconectando la unidad w:\(\max-server\netlogon)...
Hay archivos abiertos y/o búsquedas incompletas de directorios pendientes en la
conexión con w:.

w: se ha eliminado.

Fase 2 de configuracion terminada.

Presione una tecla para continuar . . .
```

17. Reiniciar en Windows. Notaremos que después de haberlo unido al dominio, automáticamente ha iniciado en modo mantenimiento (aparece la pantalla de *login* en color gris). Iniciar sesión con el usuario "Administrador".
18. (Sólo en equipos de alumno) Instalar el driver de los Multipoint. Ver la sección "INSTALACION DEL DRIVER MCT DE LOS MULTIPOINT" del documento aparte llamado ["Cómo actualizar el driver MCT"](#) donde está el procedimiento). No reiniciar cuando lo pida.
19. (Sólo en equipos de alumno) Esperar a que aparezca el panel de control "Multipoint Manager", y pulsar "Cambiar a modo normal". Esto provoca que se reinicie el equipo pero ya no dejaremos que el equipo inicie Windows. Cuando aparezcan las primeras letras en el monitor le damos un toque al botón de encendido de la torre para que se apague el equipo.
20. (Sólo en equipos de alumno) Conectar todos los terminales en los puertos USB donde estaban (si existe una numeración de los cables, respetarla) y desconectar el ratón, teclado y monitor local que se habían conectado al principio.



21. (Sólo en equipos de alumno) Encendemos el equipo, pero en este primer inicio no se activará ningún terminal.
22. (Sólo en equipo de profesor) Verificación y Calibración de pantalla. Verificamos que la pantalla ha sido detectada tanto en Windows como en Max Linux por la aplicación de ActiveInspire. También calibramos la pantalla con el lapiz de la pizarra tocando los puntos indicados en la pantalla cuando lo solicite el asistente de calibración de la misma.
23. (Sólo en equipo de profesor) Configuración de ABTutor.
- Si el equipo remaquetado es uno de alumno, hay que reconfigurar el ABTutor en el equipo del profesor para que vuelva a tener conexión con el equipo remaquetado.
  - Si el equipo remaquetado es el del profesor hay que volver a licenciar el ABTutor, crear el grupo de ese aula y poner la contraseña adecuada para que pueda volver a conectarse con los equipos (Si el ABTutor no detecta algún equipo, iniciar sesión en ese equipo con cualquier usuario administrador y cerrar la sesión).
24. Abrir el max-control en algún equipo y actualizar la MAC e IP del equipo remaquetado:

Panel de control de Servidor de Centro

Menú

- Mi perfil
- Usuarios y Grupos
- Aulas y Equipos
  - Ver equipos
  - Ver aulas
- Distribuir ISOS
- Apagado y reinicio
- Programar arranque equipos

Editar equipo alumno12

Dirección MAC: 40:61:86:XX:XX:XX **Averiguar MAC** (ejemplo 00:00:00:00:00:00)

Dirección IP: 192.168.10.12 **Averiguar IP** (ejemplo 192.168.1.23)

Archivo de arranque: (por defecto vacío)

Aula:

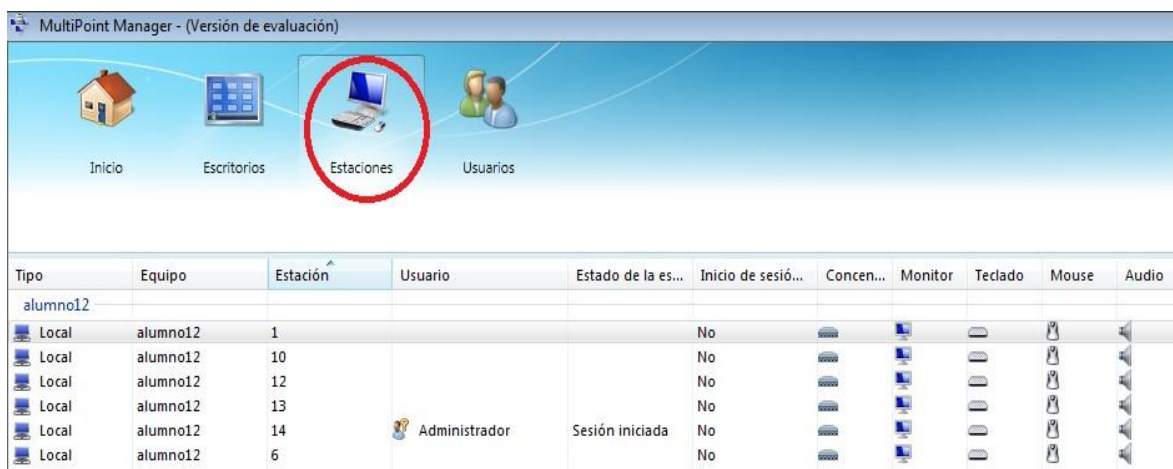
NOTA: Si no detecta la MAC o IP correcta introducir los datos a mano y pulsar el botón de “Guardar”.

25. Desde el max-control, reiniciar el equipo en Windows, ahora ya en el segundo reinicio, se activarán todos los terminales.
26. Desde el max-control, reiniciar el equipo en MAX y comprobar que todos los terminales están OK y se inicia sesión con un usuario del dominio.
27. Desde el max-control apagar el equipo. Una vez apagado encenderlo en Windows y comprobar que los terminales están OK y podemos iniciar sesión con un usuario del



dominio. Desde el “Multipoint Manager” podemos comprobar el estado de los terminales:

MultiPoint Manager - (Versión de evaluación)



Tipo	Equipo	Estación	Usuario	Estado de la es...	Inicio de sesió...	Concen...	Monitor	Teclado	Mouse	Audio
alumno12										
Local	alumno12	1			No					
Local	alumno12	10			No					
Local	alumno12	12			No					
Local	alumno12	13			No					
Local	alumno12	14	Administrador	Sesión iniciada	No					
Local	alumno12	6			No					



## 1. CÓMO ACTUALIZAR LA BIOS

1. Conectar el USB que debe de contener en la raíz, el fichero de actualización de la BIOS.
2. Encender el equipo y pulsar la tecla [Supr] para acceder a la BIOS.
3. Ir al menú “M-Flash” y poner la opción “M-Flash Function as” en [BIOS Update]. Aparecerá justo debajo una línea para seleccionar el USB:

Load BIOS Source File from [USB:<nuestro USB>]

Lo seleccionamos y en el nuevo menú elegimos la “Partición 0:” entonces ya aparecerá el nombre del fichero de la BIOS, lo seleccionamos y confirmamos para que inicie la actualización. Una vez terminada la actualización el equipo se reiniciará automáticamente y detectará que la BIOS está sin configurar, indicando que hay que pulsar F1 para acceder a la BIOS, entramos y configuramos BIOS tal como se muestra en la siguiente sección.

## 2. CONFIGURACIÓN DE LA BIOS

Pulsar la tecla [Supr] para acceder a la BIOS. Hay que configurar primero el arranque por PXE para que luego salga la red en la lista de dispositivos de arranque:

+ Integrated Peripherals

▪ LAN Option ROM [Enabled]

Pulsamos F10 y grabamos los cambios, volvemos a entrar en la BIOS pulsando [Supr] y configuramos los siguientes parámetros de la BIOS:

+ Standard CMOS Features Date(MM:DD:YY)  
Time(HH:MM:SS)

+ Advanced BIOS Features

+ Boot Sequence

1st Boot Device [Network:Realte]

2st Boot Device [SATA:3S-SAMSUN]

<el resto> [Disabled]

Boot From Other Device [No]

Full Screen Logo Display [Disabled]

+ Power Management Setup

Restore On AC Power Loss [On]

+ Wake Up Event Setup

Resume By PCI or PCI-E Device [Enabled]

Pulsamos F10 y grabamos los cambios.

## 3. POSIBLES INCIDENCIAS Y SOLUCIÓN A LAS MISMAS

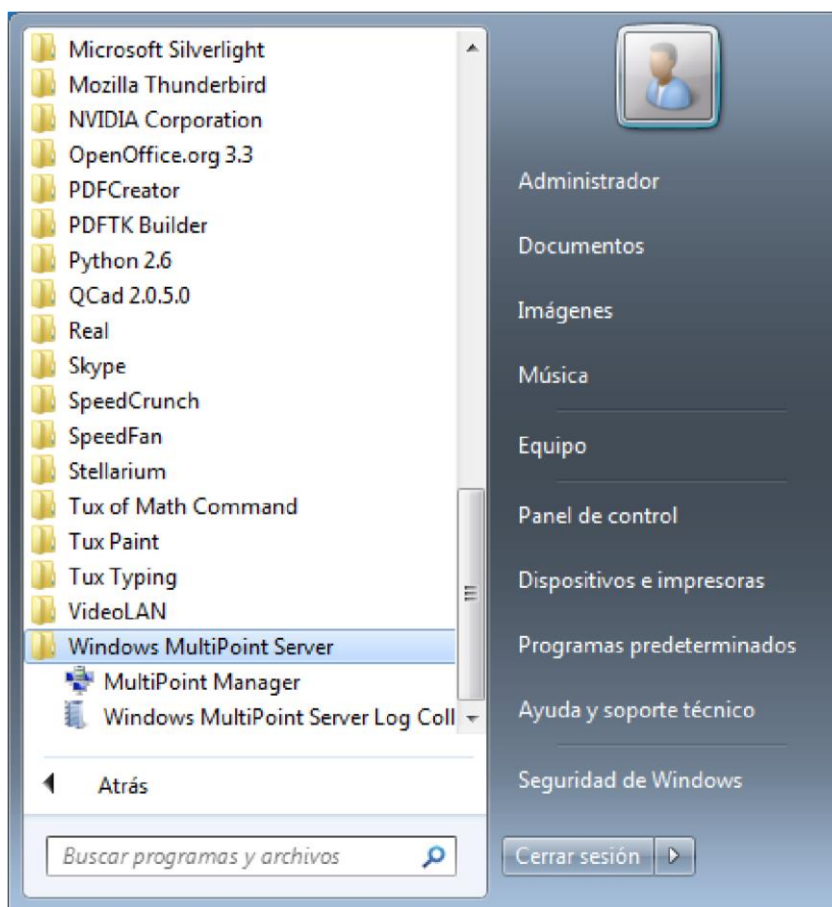
### a) Terminales en negro

Si después de haber configurado y arrancado un equipo de alumno según el procedimiento anterior, aparece algún terminal en negro de los equipos que forman



parte de una isla, haremos una serie de comprobaciones para detectar donde se encuentra el problema.

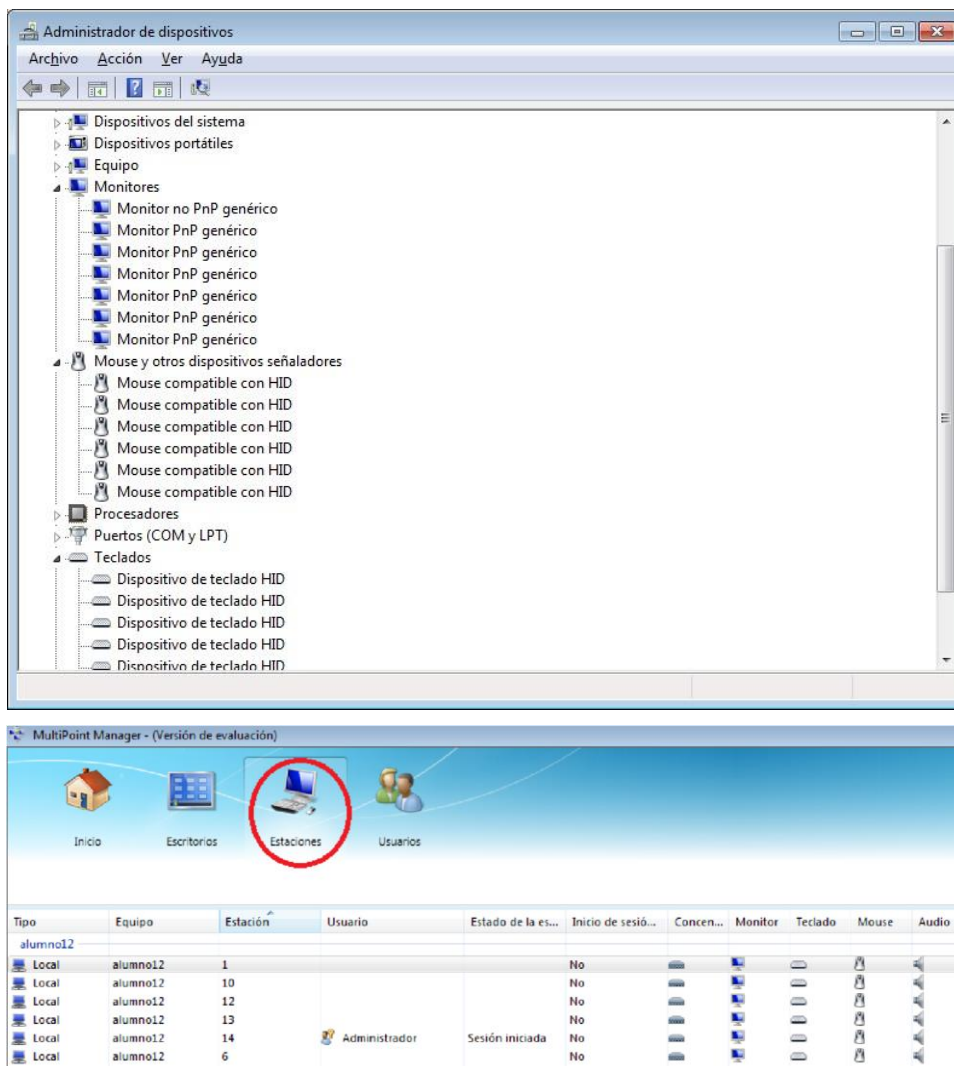
- ✚ Verificación de cables: comprobamos que todos los cables están correctamente conectados en el Multipoint, en la CPU y en el Monitor (cables de alimentación, USB, teclado y ratón, VGA).
- ✚ Verificación desde otro terminal operativo de la misma isla con la aplicación Multipoint Manager de los terminales reconocidos por el sistema. Iniciaremos sesión en este terminal con el usuario “Administrador” local.



En la pestaña “Estaciones” verificaremos también si ha reconocido todos los terminales de la isla. En caso de no ser así, podemos ver qué estación no ha sido reconocida y ver si está fallando algún cableado o componente en mal estado que haya que sustituir (teclado, ratón, monitor, audio).

Esto también lo podemos ver en Propiedades de “Equipo” > “Administrador de Dispositivos”, donde podemos ver si han sido reconocidos todos los elementos de hardware de los equipos que forman parte de la isla.



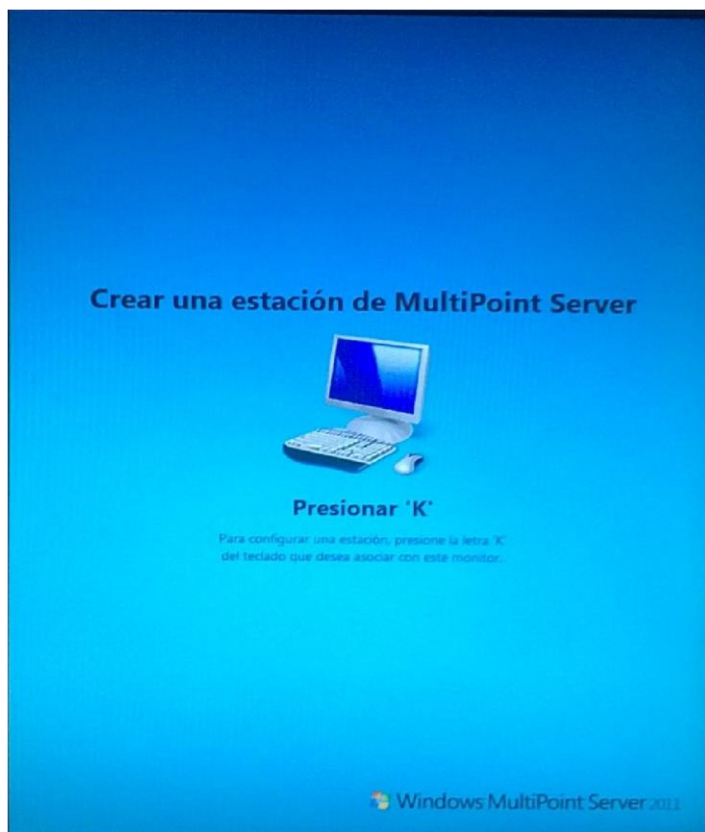


## b) Estaciones que no se asignan

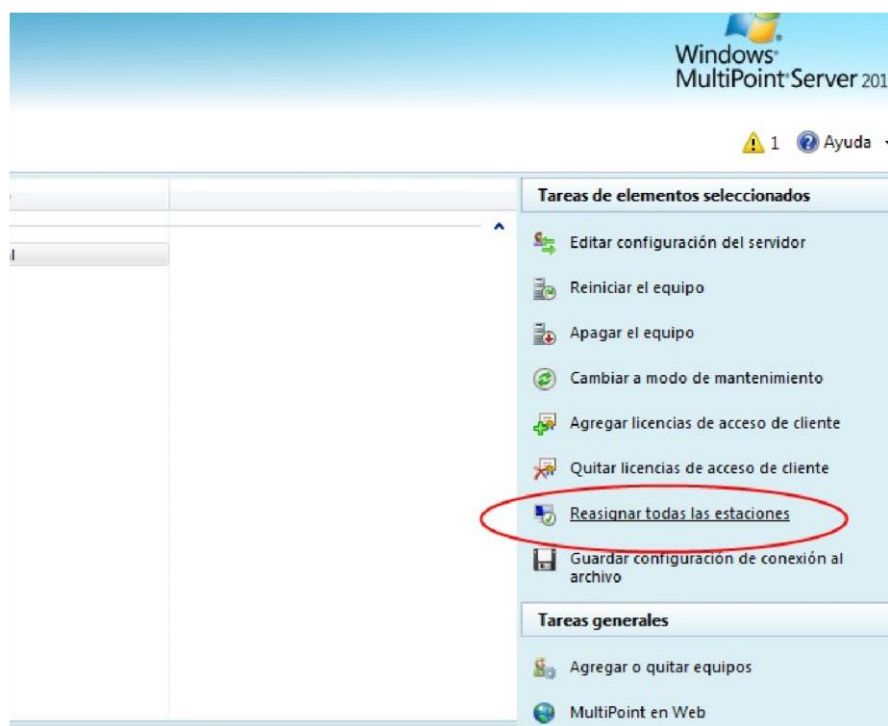
Si después de configurado un equipo, se arranca la isla y aparece un mensaje con pantalla azul en algún terminal, relativo a que alguna de las estaciones no ha podido ser asignada, primeramente presionaremos la tecla indicada en dicha pantalla para ver si se asigna correctamente la estación.





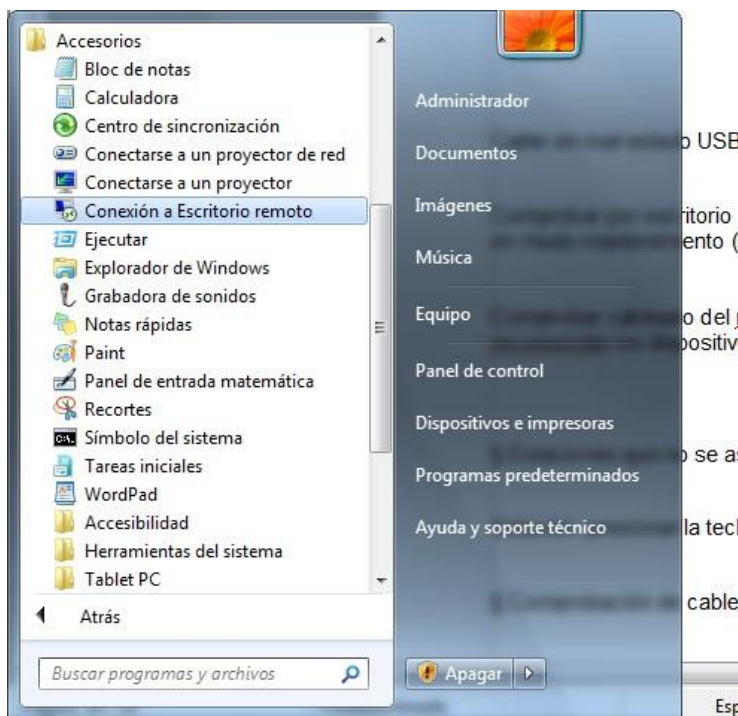


Si esto no funcionase accederemos desde otro puesto operativo de la isla a la aplicación Multipoint Manager y usaremos la opción de la pestaña “Inicio” llamada “*Reasignar todas las estaciones*”. Si hecho esto no funcionase la estación después de reiniciada la isla, se debería de reinstalar el driver de MCT según el procedimiento “Cómo actualizar el driver MCT”.



### c) Isla en negro

En caso de que no se vea ningún terminal de la isla, utilizaremos para verificar el problema la Conexión por escritorio remoto al PC de alumno. Desde el menú “Inicio de Windows > Todos los Programas > Accesorios > Conexión a Escritorio Remoto” podemos lanzar la aplicación.



Ponemos la dirección IP del equipo al que nos queremos conectar en remoto y le damos a “Conectar”. Nos pedirá las credenciales de usuario de la máquina, utilizaremos las del usuario “Administrador” local.



Una vez abierta la sesión remota, abrir la aplicación Multipoint Manager, que se puede ejecutar desde el menú “Inicio > Todos los Programas > Windows Multipoint Server > Multipoint Manager” y verificar en la pestaña “Inicio” de la misma si el equipo está en modo mantenimiento. En este caso, pasarlo a modo normal desde el enlace que aparece a la derecha (el equipo se reiniciará).



En caso de que la conexión por Escritorio Remoto no fuese satisfactoria, verificaremos que el equipo se encuentra arrancado en Windows, mandando un reinicio desde el Panel de Control de max-control en el sistema Windows.

Nombre	IP / MAC	Aula	Acciones	Encender/Reiniciar en	Estado	Múltiple
profesor10\$	192.168.10.10 / 40:61:86:93:01:0e	Aula10	[Icons]	[Icons]	✓	[Icon]
alumno13\$	192.168.10.13 / 90:e6:ba:d3:e8:2f	Aula10	[Icons]	[Icons]	✗	[Icon]
alumno11\$	192.168.10.11 / 40:61:86:93:18:8b	Aula10	[Icons]	[Icons]	✗	[Icon]
alumno12\$	192.168.10.12 / 40:61:86:93:19:2b	Aula10	[Icons]	[Icons]	✓	[Icon]
alumno14\$	192.168.10.14 / 40:61:86:ca:63:97	Aula10	[Icons]	[Icons]	✗	[Icon]
alumno15\$	192.168.10.15 / 40:61:86:ca:63:cc	Aula10	[Icons]	[Icons]	✗	[Icon]
profesor20\$	192.168.10.20 / 40:61:86:ca:5d:74		[Icons]	[Icons]	✗	[Icon]
profesor30\$	192.168.10.30 / 40:61:86:ca:63:b6		[Icons]	[Icons]	✗	[Icon]
alumno31\$	192.168.10.31 / 40:61:86:ca:63:d2	Aula30	[Icons]	[Icons]	✗	[Icon]
alumno32\$	192.168.10.32 / 40:61:86:ca:63:ca	Aula30	[Icons]	[Icons]	✗	[Icon]
alumno12 36:ca:63:7d		Aula30	[Icons]	[Icons]	✗	[Icon]

#### d) Cable USB en mal estado

Si después de verificar lo anterior detectamos que algún terminal no funciona, posiblemente se deba al mal estado del cable USB, y se tenga que sustituir por otro con la longitud adecuada. Antes de cambiarlo probaremos a conectar directamente el multipoint con la CPU de alumno con un cable USB nuevo, para ver si se activa el terminal. Si es así, lo cambiaremos y lo instalaremos correctamente canalizándolo adecuadamente por la canaleta correspondiente y poniéndole las bridas que sean necesarias para que la instalación sea lo más óptima y limpia posible.

