

## PLIEGO DE PRESCRIPCIONES TÉCNICAS

### SOPORTE TÉCNICO Y FUNCIONAL DE SISTEMAS INFORMÁTICOS DE CENTROS EDUCATIVOS DE LA COMUNIDAD DE MADRID

#### 1. INTRODUCCIÓN.

El objeto del presente contrato es el soporte técnico y funcional de las aulas digitales y sistemas informáticos de los Institutos de Innovación Tecnológica, así como de otros dispositivos informáticos (portátiles y tabletas) suministrados por la Comunidad de Madrid a otros centros educativos de la Comunidad de Madrid.

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 centros, si bien más reducidas.

Además, durante los años 2020 y 2021, como consecuencia de las medidas puestas en marcha por la Comunidad de Madrid para paliar los efectos negativos de la pandemia producida por el Covid-19 y favorecer la continuidad de la enseñanza en entornos semipresenciales, se han realizado importantes dotaciones informáticas de dispositivos informáticos: tabletas y portátiles destinados a los centros y especialmente al uso de los alumnos más desfavorecidos. Estas dotaciones, compuesta por equipamientos de distintos fabricantes, requieren de un servicio de soporte que facilite una adecuada atención a los centros educativos y contribuya al mantenimiento y utilización de los equipos de manera eficaz.

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 dotación, y en su caso de la instalación y mantenimiento de las referidas infraestructuras, desde su entrega 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



La autenticidad de este documento se puede comprobar en [www.madrid.org/csv](http://www.madrid.org/csv) mediante el siguiente código seguro de verificación: 0908660397382264577913

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, así como facilitar soporte a las dotaciones informáticas (portátiles y tabletas), realizadas por la Comunidad de Madrid a distintos centros de la Comunidad de Madrid con el alcance que se establece a lo largo de este documento.

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.

En Anexo 3, 'LISTADO DE EQUIPAMIENTO INFORMÁTICO: PORTÁTILES Y TABLETAS', se detallan las dotaciones realizadas y las características del equipamiento y la configuración del mismo.

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 para los centros e instalaciones del Anexo 1 y 2. 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.

Soporte de gestión y resolución de incidencias de primer nivel a través de atención a distancia utilizando medios telemáticos de conexión remota con los dispositivos incluidos en el Anexo 3, objeto del mantenimiento, de forma que los usuarios puedan recibir atención para resolver problemas de los dispositivos, especialmente relacionados con la utilización, configuración e instalación de software. Para ello el adjudicatario dispondrá de un modelo de cada dotación.

## 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 1, 2 y 3 que recogen todas las infraestructuras incluidas inicialmente en el contrato y su ubicación en centros en caso de las instalaciones del Anexo 1.



### 3.1. Equipamiento incluido en Anexos 1 y 2

Con las actuaciones que se realicen en el marco de este contrato debe asegurarse el mantenimiento integral del equipamiento incluido en los Anexos 1 y 2, de forma que se asegure que continúe operativo y en perfecto grado de funcionamiento, para ello se realizarán las siguientes actuaciones:

#### 3.1.1. 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.

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.

#### 3.1.2. 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.



### 3.1.3. 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.

### 3.1.4. 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.

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.

### 3.1.5. 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.



### 3.2. Equipamiento incluido en Anexo 3

Con las actuaciones que se realicen en el marco de este contrato, para el equipamiento incluido en el Anexo 3 debe asegurarse la atención a los centros que utilizan el equipamiento mediante la recepción y resolución de incidencias de forma remota de forma que se asegure que este equipamiento continúa operativo resolviéndose problemas de configuración e instalación de software.

Para ello se facilitará soporte de gestión y resolución de incidencias de primer nivel a través de atención a distancia utilizando medios telemáticos de conexión remota a los dispositivos y se facilitarán instrucciones a los usuarios para resolver las incidencias que puedan plantear. Para posibilitar estas actuaciones el adjudicatario dispondrá de un modelo de cada dotación que deberá conocer haciéndose responsable de la definición y la comunicación a usuarios de las acciones necesarias para asegurar el adecuado funcionamiento de los dispositivos.

No se incluye en el alcance del contrato la reposición o sustitución de elementos de los dispositivos incluidos en el Anexo 3.

## 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 si fuera necesario para acceder a los equipos objeto de mantenimiento.

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 tres personas:

- Jefe de Proyecto: Que ejercerá funciones de coordinación del servicio y tendrá dedicación parcial.
- 1 Técnico: Con dedicación exclusiva al proyecto.
- 1 Técnico con dedicación parcial al proyecto (50%)

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:



- 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 para el técnico principal a jornada completa y en 20 horas semanales para el segundo técnico.

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 periodos 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 para al menos el técnico principal del proyecto a tiempo completo, debido a que el mismo deberá 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:

- 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	TIEMPO DE
Alta	2 horas	12 horas
Media	4 horas	36 horas
Baja	8 horas	60 horas

Para los equipos incluidos en el Anexo 3, 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	TIEMPO DE
Alta	4 horas	24 horas
Media	8 horas	48 horas
Baja	12 horas	72 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, en su caso, 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, 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

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.

Firmado digitalmente.

DIRECTOR GENERAL DE INFRAESTRUCTURAS Y SERVICIOS



La autenticidad de este documento se puede comprobar en [www.madrid.org/csn](http://www.madrid.org/csn)  
mediante el siguiente código seguro de verificación: **0908660397382264577913**

## ANEXO 1

### LISTADO DE EQUIPAMIENTO INFORMÁTICO DE INSTITUTOS DE INNOVACIÓN TECNOLÓGICA Y CENTROS SIMILARES

		DOTACIONES				Total		Total	Total
	Centro	DOT 1	DOT 2	DOT 3	DOT 4	Aulas	Servidores	PC-ISLA Ó PROFESOR	Terminales (NL300-MC)
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

La autenticidad de este documento se puede comprobar en [www.madrid.org/csv](http://www.madrid.org/csv) mediante el siguiente código de verificación: 090600059736220437913

		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	0	4	30
	HOTEL ESCUELA	0	0	0	2	2N	0	4+5	34+36
	JUAN DE LA CIERVA(Tablets)	0	0	0	1	1N	0	4	30
	MUNDIAL86(piscina)	0	0	0	1	1N	0	4	30
	CEIPS Maria Moliner(Villanueva de la Cañada)	0	0	1	0	1N	0	4	30
	CEIP Angel Gonzalez(Leganés)	0	0	1	0	1N	0	4	30
	<b>TOTALES SOLO IIT</b>	45	35	44	46	171	15	712	5270
	<b>TOTALES</b>	50	36	47	46	188	16	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

### 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





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

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.

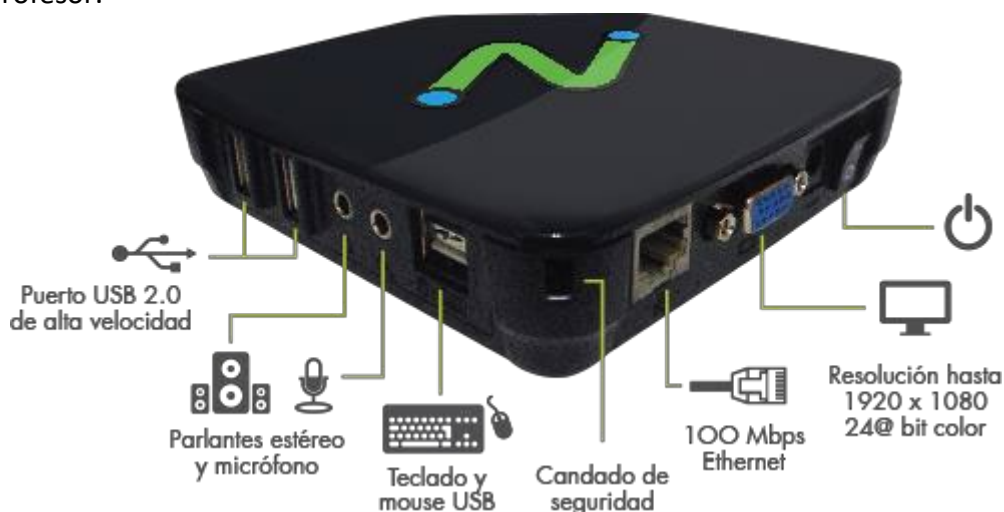


Imagen 2: Conexiones de un terminal NComputing L300

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:

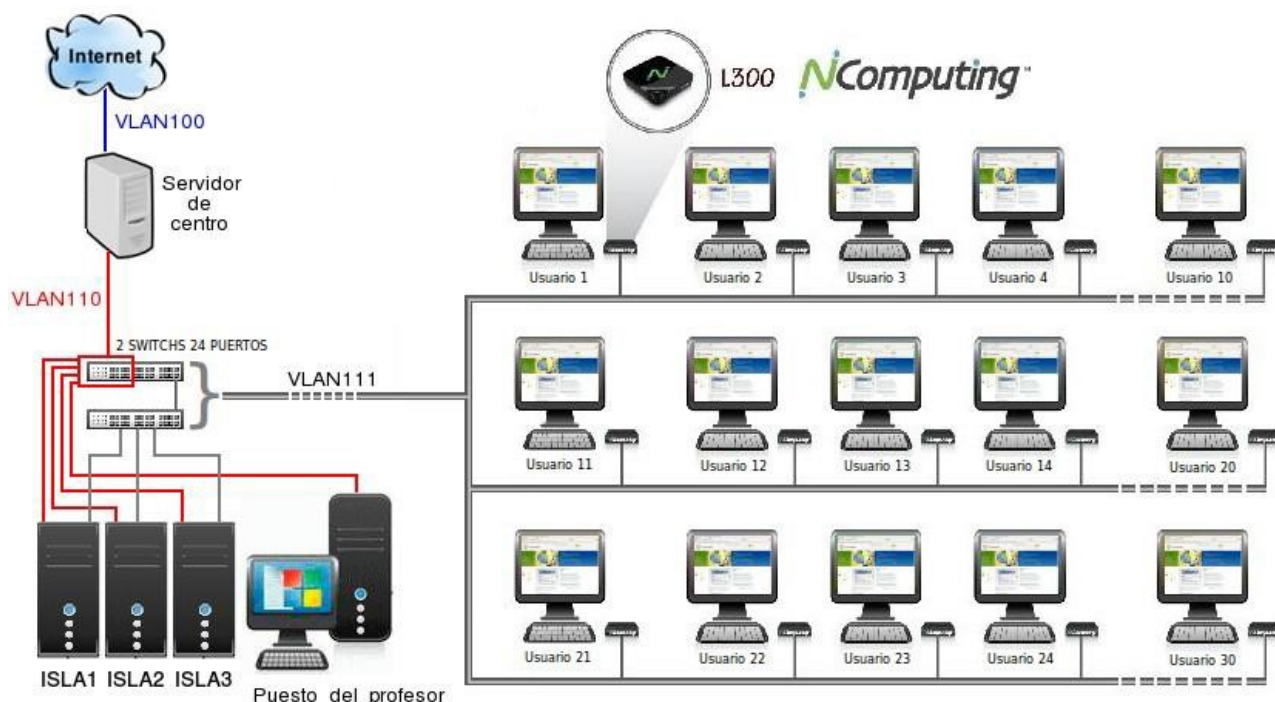
- El reconocimiento de dispositivos conectados por USB al terminal ligero es limitado, no se recomienda por ejemplo conectar pizarras digitales ya que no tienen buen soporte. Por eso no recomendamos el uso para el puesto del profesor.
- El uso de Arduino o dispositivos similares es factible pero se vuelve 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.

## 6. Perfiles de usuario

- a) ¿Que es el perfil del usuario?
- b) ¿Que significa que sea móvil?
- c) Borrado de perfil en Windows

## B. CONSIDERACIONES 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

## C. EL 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 'F1' 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:





GNU GRUB version 1.98-1ubuntu12

**Iniciar System Rescue CD**

Restaurar servidor  
Generar nueva imagen  
Chequeo de Memoria  
Cargar /boot/grub/grub.cfg del servidor  
MaX-Servidor, con Linux 2.6.32-33-server  
MaX-Servidor, con Linux 2.6.32-33-server (modo recuperacion)

Use the ↑ and ↓ keys to select which entry is highlighted.  
Press enter to boot the selected OS, 'e' to edit the commands before  
booting or 'c' for a command-line.

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 remaquetará 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. 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. 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-QNHY-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*”:

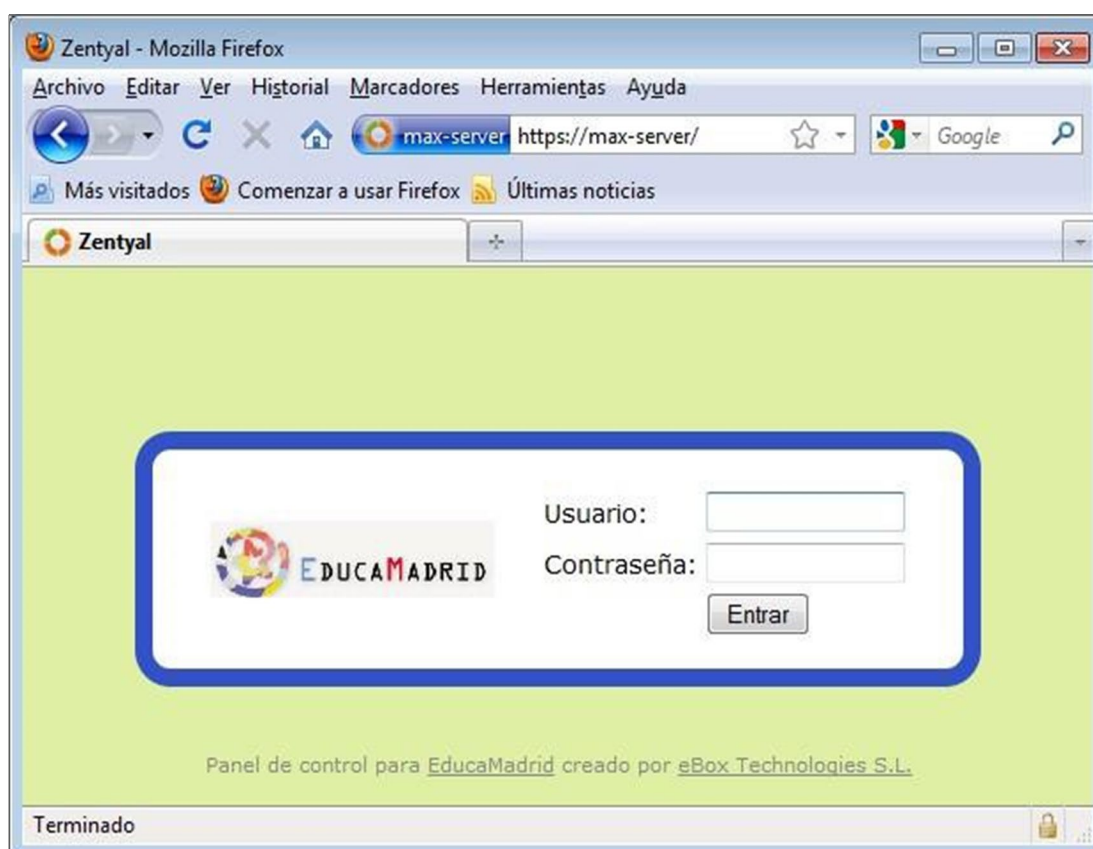
```

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

## 6. 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](#)

**Core**  
Dashboard  
Estado de los Módulos  
Sistema  
Red  
Mantenimiento  
Gestión de software  
Suscripción  
**Gateway**  
Proxy HTTP  
Moldeado de tráfico  
RADIUS  
Portal Cautivo  
**UTM**  
Cortafuegos  
VPN  
Antivirus  
**Infraestructure**  
DHCP  
DNS  
Servidor Web  
FTP  
Autoridad de certificación  
NTP  
**Office**  
Usuarios y Grupos  
Compartir ficheros  
Compartir Impresoras

**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="#">¡Suscríbese 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**

**Interfaces de Red**  

**eth0**  
Estado: activado, externo, enlace ok  
Dirección MAC: e0:cb:4e:42:dc:07  
Dirección IP: 10.111.20.5  

Bytes Tx: 0 B  
Bytes Rx: 0 B

**eth1**  
Estado: activado, interno, enlace ok  
Dirección MAC: 00:27:19:b1:7b:d5  
Dirección IP: 192.168.10.1  

Bytes Tx: 0 B  
Bytes Rx: 0 B

**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.

## 7. 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	
Red		<input checked="" type="checkbox"/>	
Cortafuegos	Red	<input checked="" type="checkbox"/>	
DHCP	Red	<input checked="" type="checkbox"/>	
DNS		<input checked="" type="checkbox"/>	
Eventos		<input type="checkbox"/>	
Registros		<input type="checkbox"/>	
NTP		<input checked="" type="checkbox"/>	
VPN	Red	<input type="checkbox"/>	
Moldeado de tráfico	Red, Cortafuegos	<input type="checkbox"/>	
Usuarios y Grupos		<input checked="" type="checkbox"/>	
Backharddi NG	DHCP	<input checked="" type="checkbox"/>	
Compartir ficheros	Red, Usuarios y Grupos	<input checked="" type="checkbox"/>	
Proxy HTTP	Cortafuegos, Usuarios y Grupos	<input type="checkbox"/>	
Rincón del Usuario	Usuarios y Grupos	<input type="checkbox"/>	
MAX Control	Red, DHCP, Compartir ficheros, Usuarios y Grupos	<input checked="" type="checkbox"/>	
Compartir Impresoras	Compartir ficheros	<input type="checkbox"/>	

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.

## 8. 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.







**Configuración General** [\(mostrar ayuda\)](#)

**Cambiar contraseña**

Usuario:

Contraseña actual:

Nueva contraseña:

Confirmar contraseña:

**Selección de idioma**

Español

**Zona Horaria**

Europe  Madrid

**Fecha y Hora**

Fecha: 17 / Enero / 2012

Hora: 12 / 48 / 39

**Puerto TCP de la interfaz de administración**

443

**Cambiar nombre de la máquina**

max-server

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"`

## 9. 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

**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

Externo (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

**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/networking/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](#)”.

## 10. 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](#)

Servidor de nombres de dominio	Acción
127.0.0.1	
213.0.88.85	

10 ▼ Página 1


**Domino de búsqueda**

Domino:

Opcional

## 11. 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](#)

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:

## 12. CORTAFUEGOS

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



Core

Dashboard

Estado del módulo

Sistema

Red

Objetos

Servicios

Registros

Eventos

Gateway

Proxy HTTP

Moldeado de tráfico

UTM

Cortafuegos

Filtrado de paquetes

Redirecciones de puertos

VPN

Infraestructura

DHCP

DNS

Autoridad de certificación

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 controlar 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

!

Debes saber que añadiendo reglas a esta sección puedes estar comprometiendo la seguridad de tu red, permitiendo el acceso desde redes no confiables. Por favor, hazlo sólo si sabes lo que estás haciendo.

[Configurar reglas](#)

Reglas de filtrado desde las redes externas a las internas

Estas reglas te permiten controlar el acceso desde redes externas a redes internas

!

Debes saber que añadiendo reglas a esta sección puedes estar comprometiendo la seguridad de tu red, permitiendo el acceso desde redes no confiables. Por favor, hazlo sólo si sabes lo que estás haciendo.

[Configurar reglas](#)

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

Buscar

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

Página 1

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
<b>Añadiendo una nueva regla</b> Decisión: <b>ACCEPT</b> Origen: <b>IP origen</b> / <b>10.111.20.0</b> / <b>24</b> Servicio: <b>ssh</b> Inverse match: <input type="checkbox"/> <small>Si la selección inversa está marcada, la regla será aplic</small> Descripción: <b>Permitir SSH</b> <small>Opcional</small> <b>Añadir</b> <b>Cancelar</b>	<b>Añadiendo una nueva regla</b> Decisión: <b>ACCEPT</b> Origen: <b>IP origen</b> / <b>10.111.20.0</b> / <b>24</b> Servicio: <b>eBox administration</b> Inverse match: <input type="checkbox"/> <small>Si la selección inversa está marcada, la regla será aplico</small> Descripción: <b>Permitir administr</b> <small>Opcional</small> <b>Añadir</b> <b>Cancelar</b>

Opcionalmente también crearemos las siguientes reglas:

- Acceso al panel de max-control, corresponde al Servicio "http".
- 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	Filtrado de paquetes ▶ Desde redes externas hacia Zentyal
<b>Editando servicio</b> Protocolo: <b>ICMP</b> Puerto origen: <b>Cualquiera</b> <small>La opción más común para este campo es "cualquiera"</small> Puerto destino: <b>Cualquiera</b>	<b>Editando regla</b> Decisión: <b>ACEPTAR</b> Origen: <b>Cualquiera</b> Servicio: <b>ping-icmp</b> Coincidencia inversa: <input checked="" type="checkbox"/> <small>Si la selección inversa está marcada, la regla será aplicada cu</small> Descripción: <b>Para permitir ping desde el exterior</b> <small>Opcional</small>

En resumen se verían las siguientes reglas:





Filtrado de paquetes ▸ Desde redes externas hacia Zentyal

Configure Rules

+ Añadir nuevo/a

Buscar

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

Buscar

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	

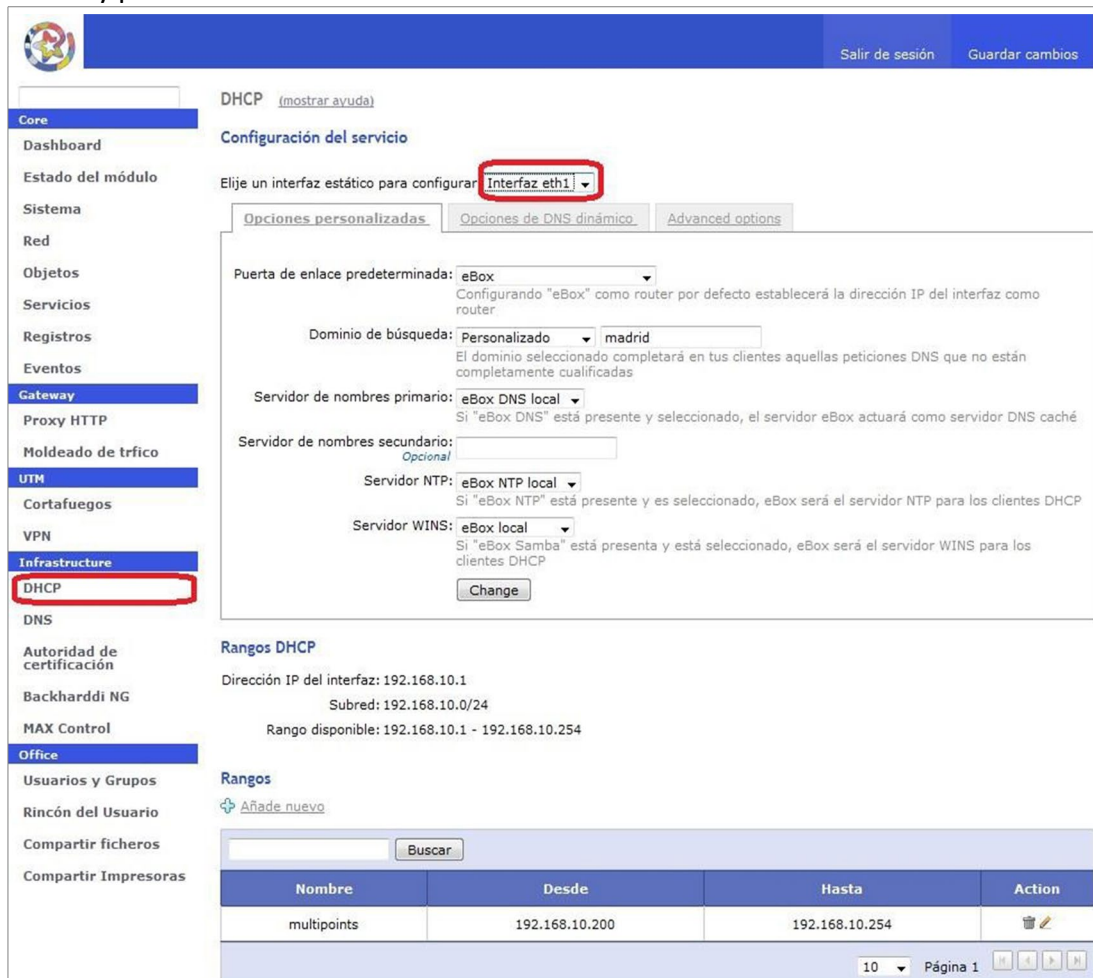
10 Página 1

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.

### 13. 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:



Core

Dashboard

Estado del módulo

Sistema

Red

Objetos

Servicios

Registros

Eventos

Gateway

Proxy HTTP

Moldeado de tráfico

UTM

Cortafuegos

VPN

Infraestructura

**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

Elige 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

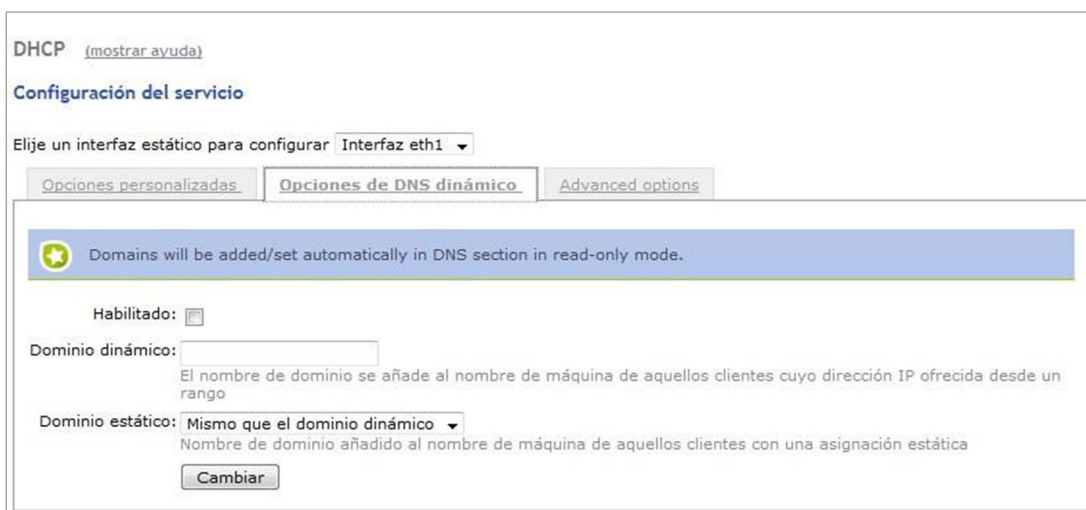
Nombre	Desde	Hasta	Action
multipoints	192.168.10.200	192.168.10.254	

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:



DHCP (mostrar ayuda)

Configuración del servicio

Elige un interfaz estático para configurar: Interfaz eth1

Opciones personalizadas Opciones de DNS dinámico Advanced options

Domains will be added/set automatically in DNS section in read-only mode.

Habilitado: ☐

Dominio dinámico:

El nombre de dominio se añade al nombre de máquina de aquellos clientes cuyo dirección IP ofrecida desde un rango

Dominio estático: Mismo que el dominio dinámico

Nombre de dominio añadido al nombre de máquina de aquellos clientes con una asignación estática

Cambiar



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

## 14. CONFIGURACIÓN DEL SERVICIO DNS

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

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

Lista de Dominios						
<input type="text"/> <input type="button" value="Buscar"/>						
Dominio	Nombres de máquinas	Intercambiadores de correo	Servidores de nombres	Dirección IP	Dinámico	Action
madrid				--		
<div>10</div> <div>Página 1</div>						

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

Buscar

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

10 Página 1

## 15. 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:

Proxy HTTP

Moldeado de tráfico

RADIUS

Portal Cautivo

UTM

Cortafuegos

VPN

Antivirus

Infraestructure

DHCP

DNS

Servidor Web

FTP

Autoridad de certificación

NTP

NTP (mostrar ayuda)

Configuración General

Activar sincronización con servidores NTP externos: ☐

Cambiar

Servidores NTP

+ Añadir nuevo/a

Buscar

Servidor	Acción
1.es.pool.ntp.org	
0.es.pool.ntp.org	
2.es.pool.ntp.org	

10 Página 1

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.

## 16. 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	
aarandaloquez	aarandaloquez 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	Buscar
Eventos	
Gateway	
Proxy HTTP	
Moldeado de tráfico	
UTM	
Cortafuegos	
VPN	
Infraestructure	
DHCP	
DNS	
Autoridad de certificación	
Backharddi NG	
MAX Control	
Office	
Usuarios y Grupos	
Usuarios	
Grupos	

Nombre	Descripción	Editar
Aula10		
Aula20		
Aula30		
CoordinadoresTIC	Coordinadores TIC no-borrar	
Instaladores	Instaladores no-borrar	
Teachers	Profesores no-borrar	
bachilleratomate		
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.

Core	Default User Template <a href="#">(mostrar ayuda)</a>
Dashboard	Compartir ficheros
Estado del módulo	Cuenta de Compartición de Ficheros o de PDC: <input checked="" type="checkbox"/>
Sistema	<input type="button" value="Cambiar"/>
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	
Usuarios	
Grupos	
Plantilla de Usuario por Defecto	
Datos LDAP	

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



**Datos de LDAP**

**Datos LDAP**

DN Base: dc=max-server

Contraseña: 4KnLOJ1AX.Pan-

DN de Usuarios: ou=Users,dc=max-server

DN de Grupos: ou=Groups,dc=max-server

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](#)





## 17. CREAR UN BACKUP DEL LDAP

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

2º Parar el servicio slapd:  
`stopebox.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:  
`startebox.slapd`

6º Comprobar que el servicio slapd está en marcha: `ps u -C slapd`

## 18. RESTAURAR EL BACKUP DEL LDAP

1º Comprobar que el servicio slapd está en marcha: `ps u -C slapd`  
 2º Parar el servicio slapd: `stopebox.service slapd`  
 3º Comprobar que el servicio slapd está parado: `ps u -C slapd`  
 4º Descomprimir la copia del ldap: `tar -xzpvf <nombre_fichero>.gz -C /`  
 5º Iniciar el servicio slapd: `startebox.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 cambiado el proceso `"slapd"` por `"smbd"` y la ruta `"/var/lib/ldap"` por `"/var/lib/samba"`.





## 19. 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)

## 20. 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>

## 21. 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 -xvpf <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”.

## 22. APAGADO / REINICIO DEL SERVIDOR

Para apagar o reiniciar el servidor 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”.

## 23. 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 button 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"
```

## 24. 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 quotas.
quotaon: No se puede encontrar el archivo de cuota en /home/samba
[/dev/nbd0] pa ra encender/apagar las quotas. 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/sa
mba/ rm
quota.us
er rm
quota.gr
oup
quotacheck -u -c --format=vfsold
/home/samba/ quotacheck -g -c --
format=vfsold /home/samba/

quotaon
dpkg-
reconfigu
```



re 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.

## 25. 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 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).

## 26. 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.

## 27. 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"
```

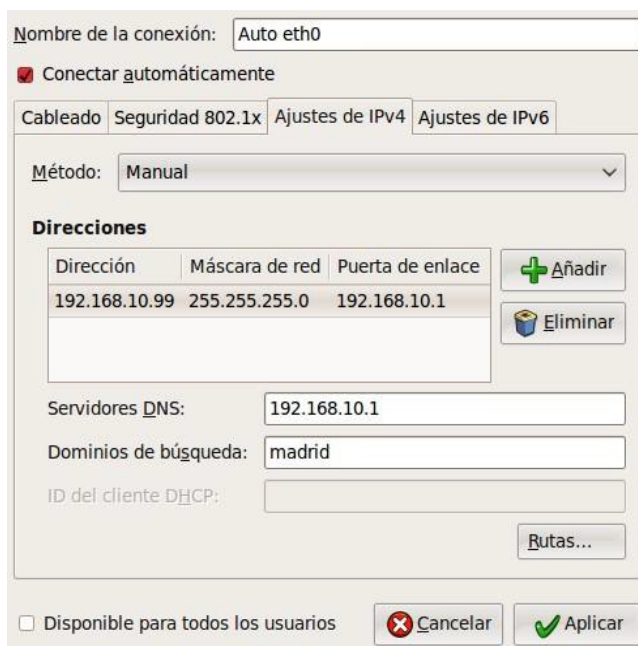
Si queremos apagar, en vez de reiniciar cambiaríamos el parámetro “-r” por “-p”. Otra forma sería utilizar el shutdown de Windows utilizando el comando winexe visto anteriormente para conectarnos al equipo.

## D. 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**

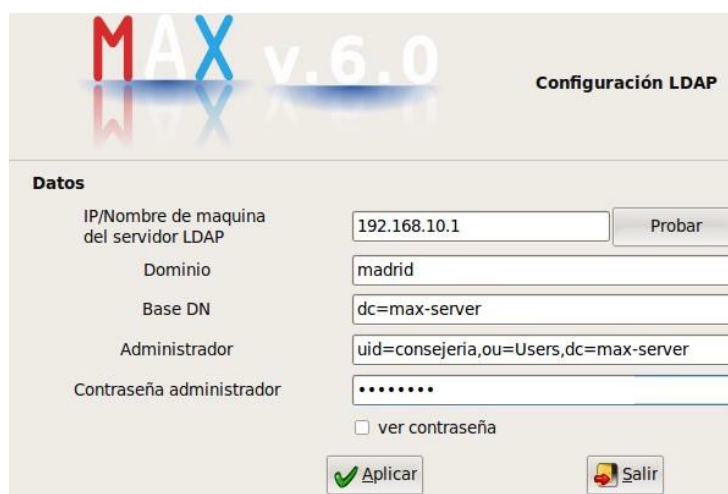
Dirección	Máscara de red	Puerta de enlace
192.168.10.99	255.255.255.0	192.168.10.1

Servidores DNS: 192.168.10.1

Domínios de búsqueda: madrid

ID del cliente DHCP:

☐ Disponible para todos los usuarios



**MAX v.6.0** Configuración LDAP

**Datos**

IP/Nombre de maquina del servidor LDAP: 192.168.10.1

Dominio: madrid

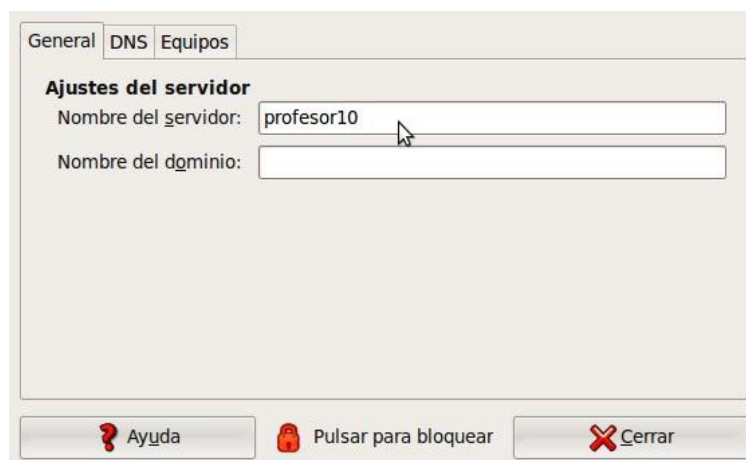
Base DN: dc=max-server

Administrador: uid=consejeria,ou=Users,dc=max-server

Contraseña administrador: ..... ☐ ver contraseña

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





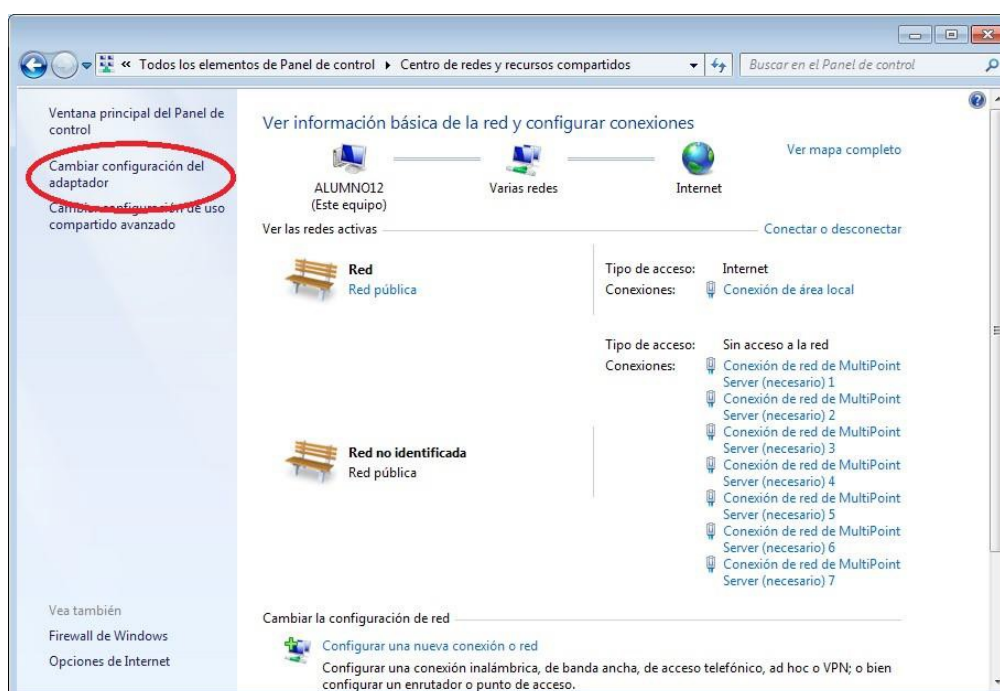
Al cerrar este último asistente el equipo se reiniciará automáticamente. Volver a iniciar en MAX y entrar con el usuario “madrid”.

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”.





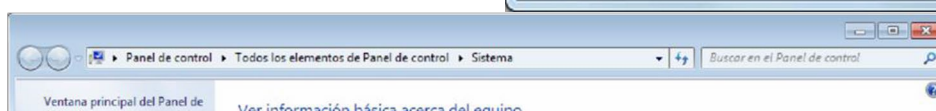
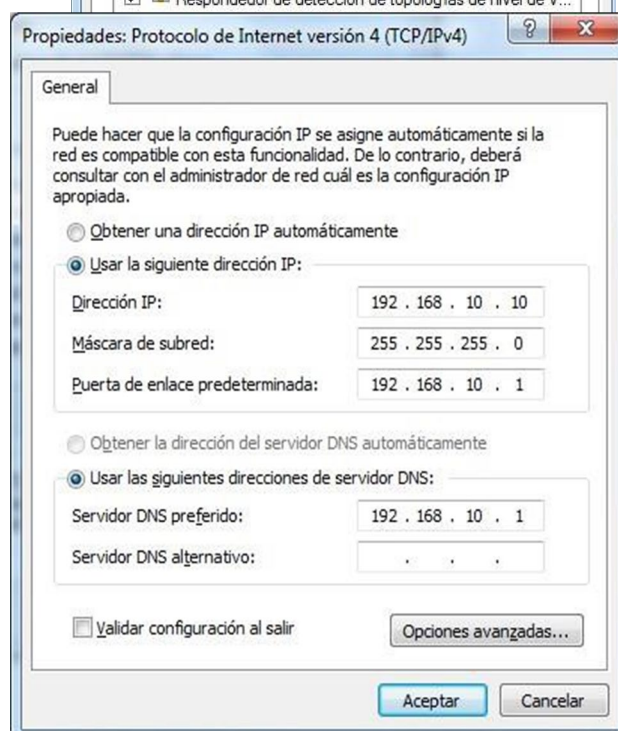
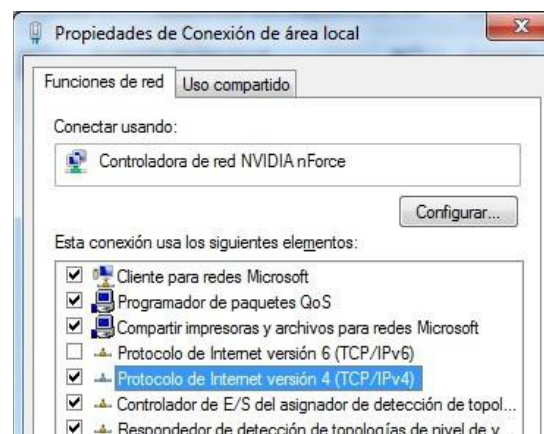
Seleccionamos la interfaz de red de “Conexión de área local” y accedemos a las Propiedades de la misma con el Botón derecho del ratón. Seleccionamos el Protocolo de Internet

(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”.

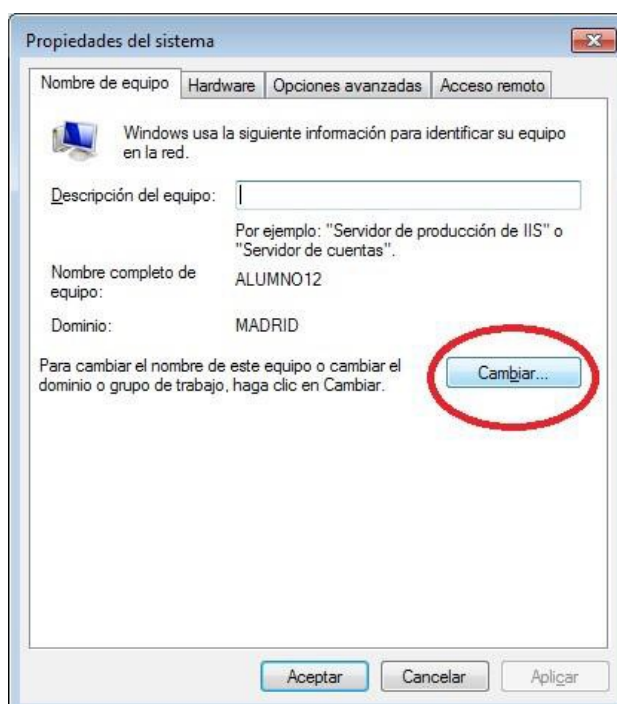
12. Para cambiar el nombre del equipo desplegamos el menú “Inicio” y hacemos clic derecho en el icono “Equipo”. Aparece un menú contextual donde elegimos la opción “Propiedades”. Nos aparece la siguiente pantalla donde seleccionaremos la opción “Cambiar configuración”.





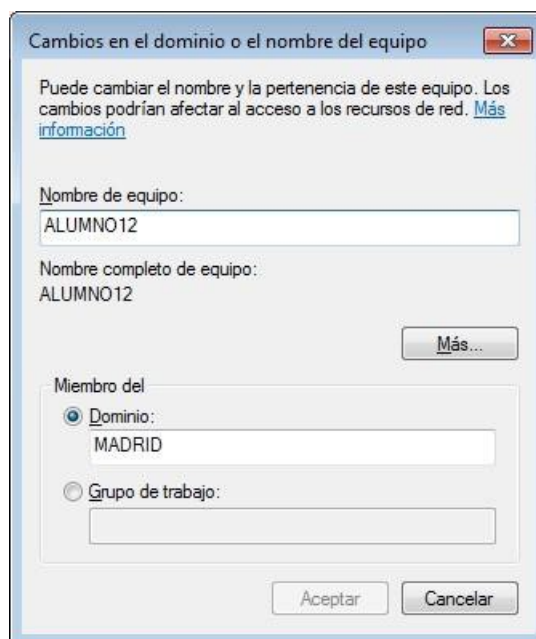


En la siguiente pantalla le damos al botón de “Cambiar”.



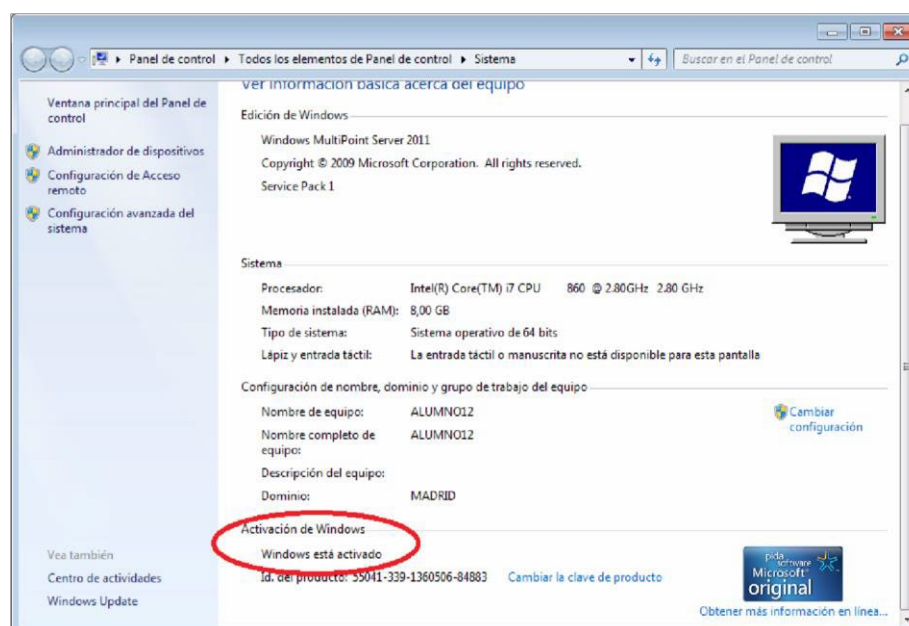
Ponemos el nombre de equipo deseado en “Nombre de equipo”





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.

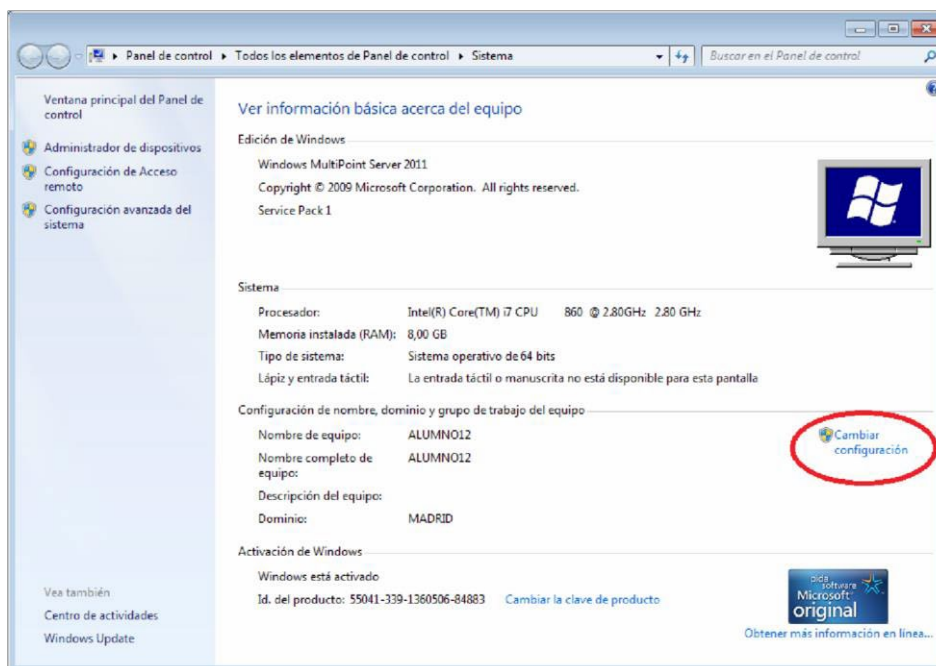


14. Instalar la impresora en Windows.

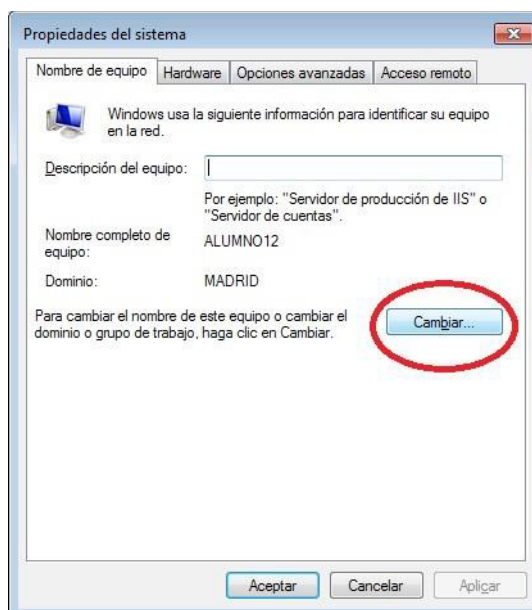
15. Para unir el equipo al dominio utilizar las credenciales del usuario “consejeria”. No reiniciar cuando lo pida. Desplegamos el menú “Inicio” y hacemos clic derecho en el icono



“Equipo”. Aparece un menú contextual donde elegimos la opción “Propiedades”. Nos aparece la siguiente pantalla donde seleccionaremos la opción “Cambiar configuración”.

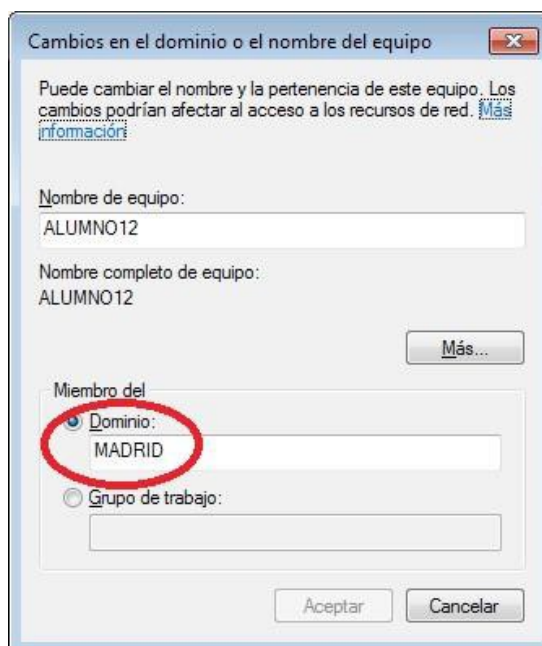


En la siguiente pantalla le damos al botón de “Cambiar”

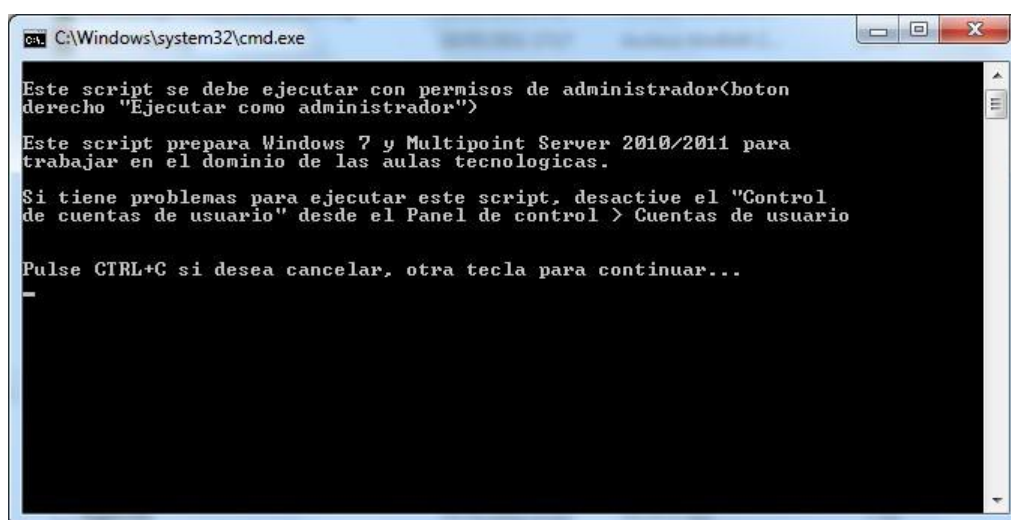


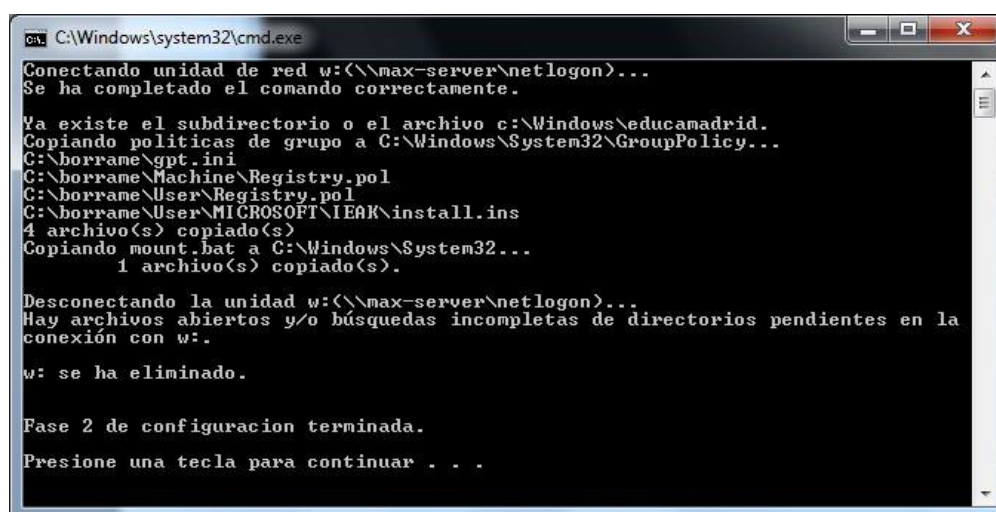
En esta pantalla se especifica el nombre de dominio y se le da a “Aceptar”. Después de introducir las credenciales del usuario “Administrador”, el equipo necesita reiniciarse para que los cambios sean efectivos.





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
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 políticas 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 . . .

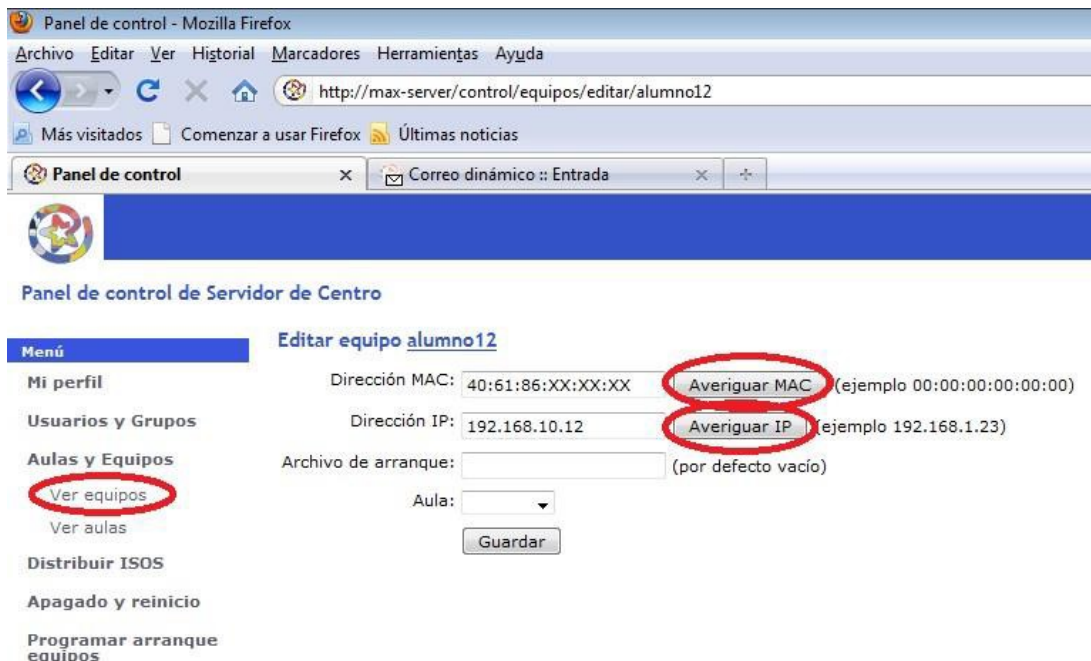
```

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).

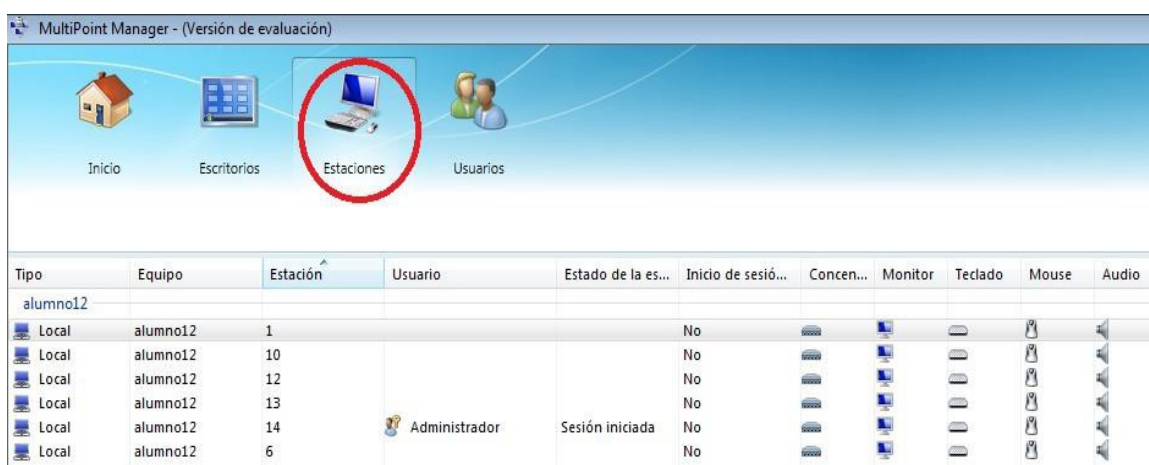
## 24. Abrir el max-control en algún equipo y actualizar la MAC e IP del equipo remaquetado:



NOTA: Si no detecta la MAC o IP correcta introducir los datos a mano y pulsar el botón de “Guardar”.

- Desde el max-control, reiniciar el equipo en Windows, ahora ya en el segundo reinicio, se activarán todos los terminales.
- 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.
- 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:





## 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

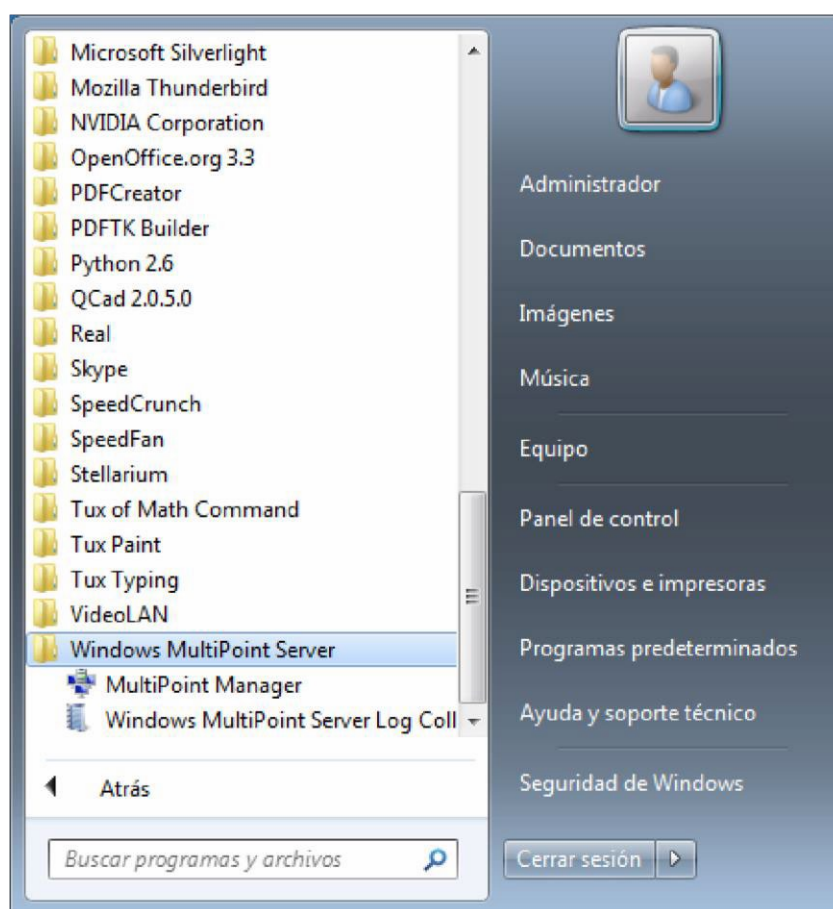
Si después de haber configurado y arrancado un equipo de alumno según el procedimiento anterior, aparece algún terminal en negro de los equipos que forman

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.



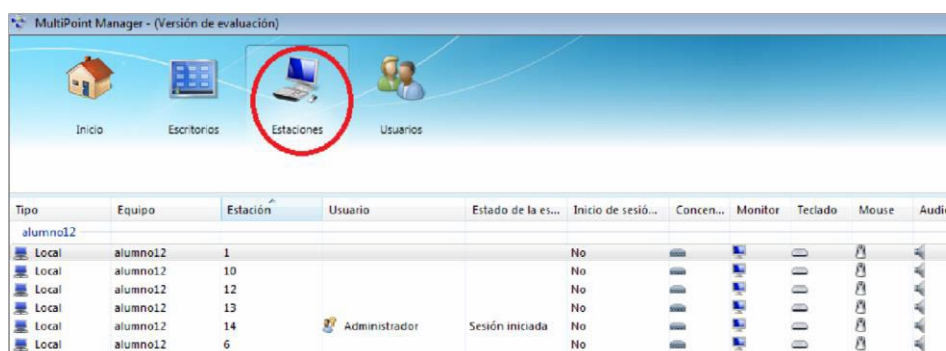
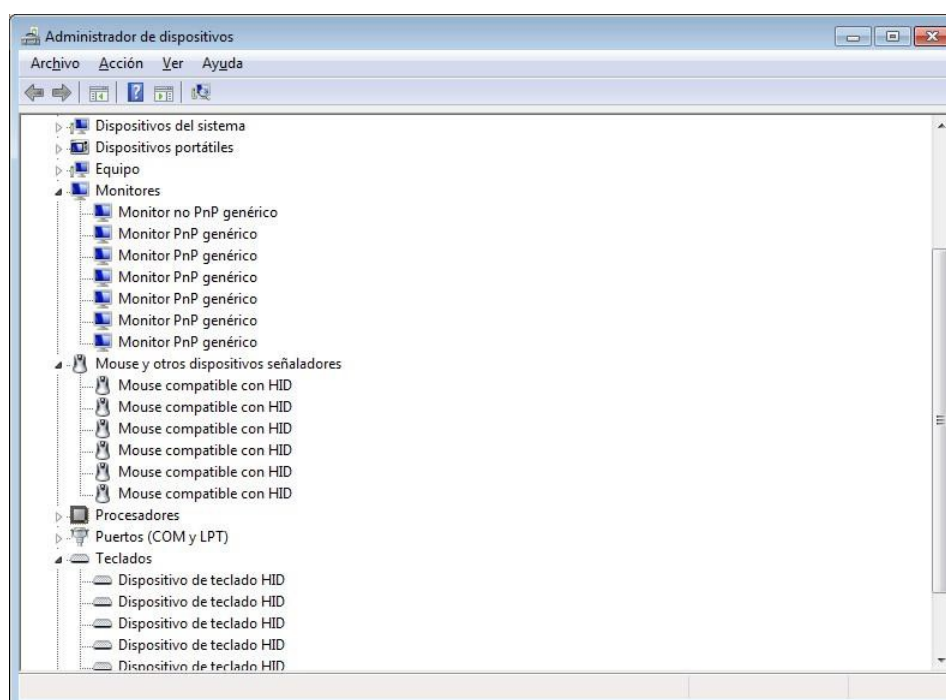




En la pestaña “Estaciones” verificaremos también si ha reconocido todos los terminales de la isla. En caso de no ser así, podemos ver qué estación no ha sido reconocida y ver si está fallando algún cableado o componente en mal estado que haya que sustituir (teclado, ratón, monitor, audio).

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.

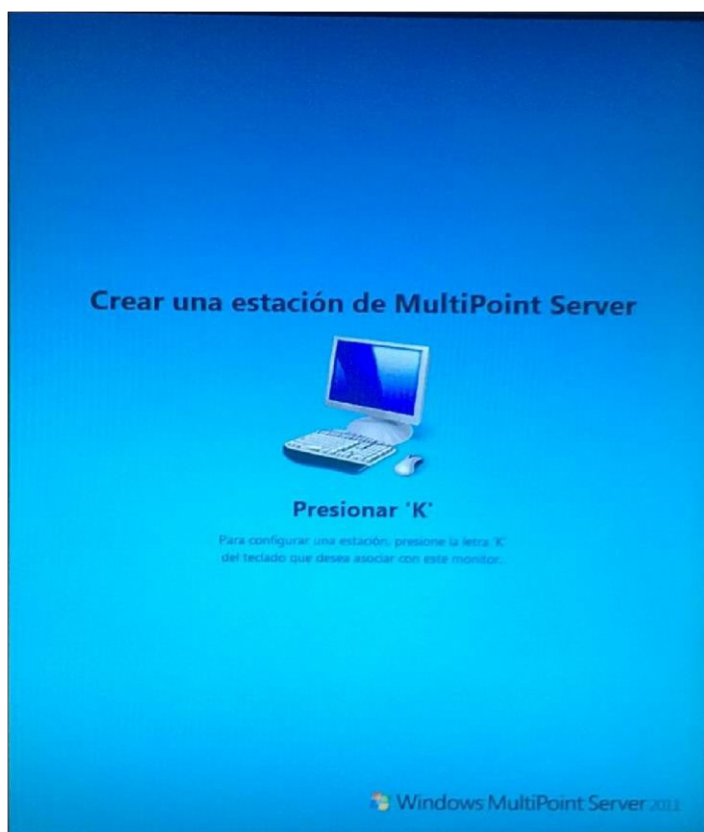




## b) Estaciones que no se asignan

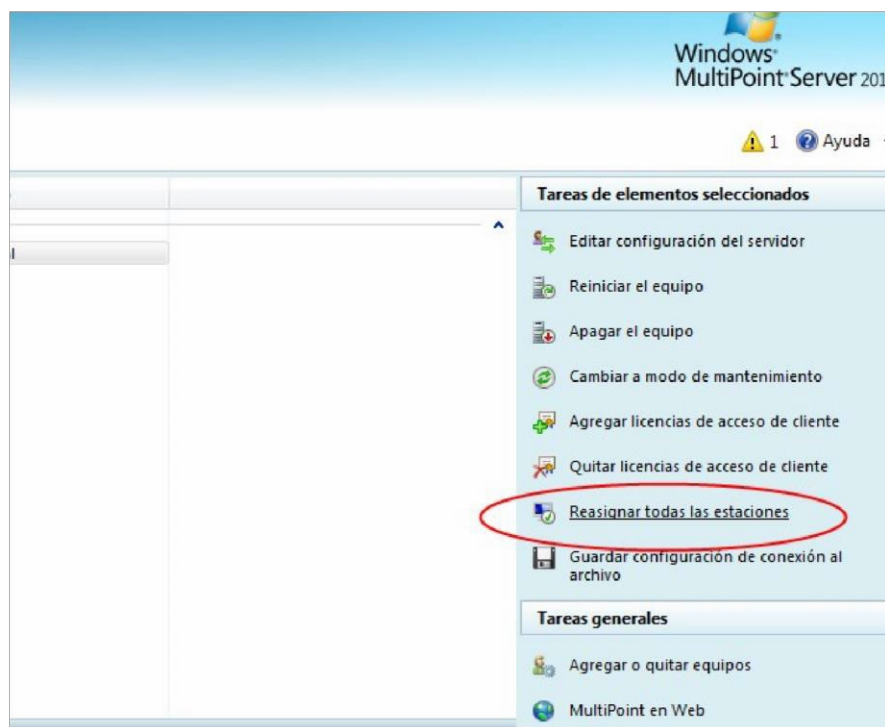
Si después de configurado un equipo, se arranca la isla y aparece un mensaje con pantalla azul en algún terminal, relativo a que alguna de las estaciones no ha podido ser asignada, primeramente presionaremos la tecla indicada en dicha pantalla para ver si se asigna correctamente la estación.





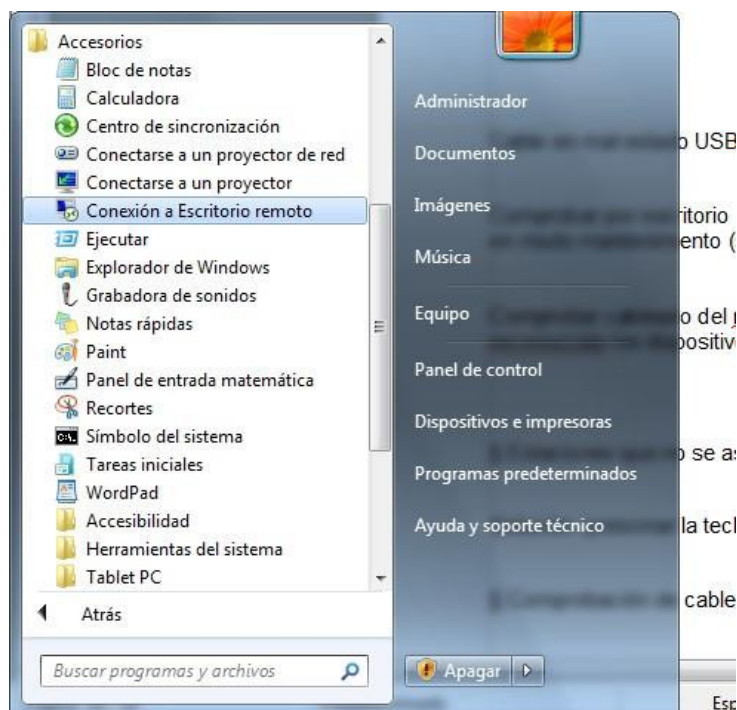
Si esto no funcionase accederemos desde otro puesto operativo de la isla a la aplicación Multipoint Manager y usaremos la opción de la pestaña “Inicio” llamada “*Reasignar todas las estaciones*”. Si hecho esto no funcionase la estación después de reiniciada la isla, se debería de reinstalar el driver 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.

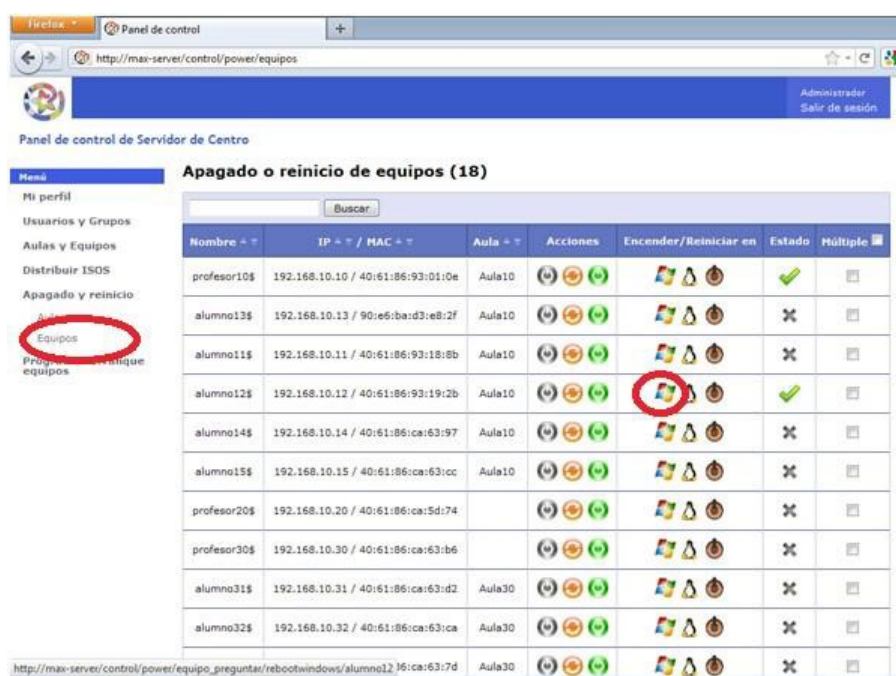


Ponemos la dirección IP del equipo al que nos queremos conectar en remoto y le damos a “Conectar”. Nos pedirá las credenciales de usuario de la máquina, utilizaremos las del usuario “Administrador” local.



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.



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.





### ANEXO 3

## LISTADO DE EQUIPAMIENTO INFORMÁTICO: PORTÁTILES Y TABLETAS

Dotación, descripción	Número de dispositivos	Número de centros destinatarios	Características del dispositivo	Configuración
Portátiles 14" HP PROBOOK 440G7 (BAC_04/2020)	11.251	461	CPU I3 10110U, RAM 8GB, SSD NVMe 256GB, pantalla 14"	Windows 10 Pro Education + MAX10
Portátiles 15" Portátil HP ProBook 455G7 (BAC_03/2020)	14.205	1.095	CPU AMD Ryzen 3 4300U, RAM 8GB, SSD NVMe 256GB, pantalla 15,6"	Windows 10 Pro Education + MAX10
Portátiles 15" Lenovo IdeaPad 3 15iil05 (D_1500/2020)	758	100	CPU I5-1035G1, RAM 8GB, SSD 256GB, pantalla 15,6"	Windows 10 HOME + MAX10
Portátiles 15" Lenovo IdeaPad 3 15ADA05 (D_1500/2020)	503	67	CPU AMD Ryzen 3 3250U, RAM 8GB, SSD 256GB, pantalla 15,6"	Windows 10 HOME + MAX11
Portátiles 15" Lenovo V15-iiL (D_1500/2020)	239	43	CPU I3-1005G1, RAM 8GB, SSD 256GB, pantalla 15,6"	Windows 10 HOME + MAX12
Tabletas 10,1" Lenovo TB-X605LC (CE_03/2020)	3.899	162	CPU Qualcomm Snapdragon 450, RAM 3GB, Almacenamiento 32GB, WLAN 802.11 a/b/g/n/ac, 2,4 GHz & 5 GHz, FDD-LTE, TDD-LTE, WCDMA, Pantalla 10,1"	Android
Tabletas 10,1" Lenovo TB-X605FC 4G(CE_03/2020)	2.099	173	CPU Qualcomm Snapdragon 450, RAM 3GB, Almacenamiento 32GB, WLAN 802.11 a/b/g/n/ac, 2,4 GHz & 5 GHz, Pantalla 10,1"	Android
Tabletas 10,4" Samsung Galaxy Tab A7 (CE_03/2020)	8.000	470	CPU Octa Core, RAM 3GB, Almacenamiento 32GB, WLAN 802.11 a/b/g/n/ac 2.4G+5GHz, Pantalla 10,4"	Android
Tabletas 8" Lenovo TB-8604F (Donación Profuturo)	993	143	CPU Qualcomm Snapdragon 425(MSM8917)(4 núcleos a 1.4GHz)64 bits, RAM 2GB, Almacenamiento 32GB, Wifi 802.11 b/g/n, canal único 2.4 GHz, Pantalla 8"	Android: 8.1 (Oreo)