



Universidad Nacional Autónoma de México

Facultad de Ingeniería

“Implementación de Servidor LTSP con Terminales Ligeras”

Informe de actividades profesionales

Que para obtener el título de:

Ingeniera en Computación

Presenta

Wendy Estefannie Martínez Ferrusca

Asesor Académico:

Ing. Cruz Sergio Aguilar Díaz



México D.F. Ciudad Universitaria, 2014

Índice

Introducción.....	1
Capítulo 1. Generalidades Estructurales de un Servidor LTSP.....	5
1.1 Protocolo de transferencia de archivos trivial (TFTP).....	5
1.2 Protocolo de configuración de host dinámico (DHCP)	6
1.3 Protocolo de entorno de ejecución de pre-arranque (PXE).....	8
1.4 Funcionamiento del protocolo PXE.....	9
1.5 Protocolo NFS (Sistema de archivos de red).....	10
1.6 Protocolo de Sesión Remota X Window System / XDMCP.....	11
Capítulo 2. Requerimientos del Proyecto.....	14
2.1 Análisis de requerimientos.....	15
2.2 Alcances y limitaciones del Proyecto.....	16
2.2.1 A nivel de hardware.....	16
2.2.2 A nivel de costos.....	17
2.2.3 Limitaciones.....	19
2.3 Especificación funcional.....	20
2.4 Plan de trabajo.....	21
Capítulo 3. Implementación.....	23
3.1 Búsqueda de Documentación.....	23
3.2 Análisis de requerimientos.....	23
3.3 Selección de software.....	24
3.4 Instalación de Ubuntu.....	25
3.5 Instalación y configuración de servicios LTSP.....	27
3.6 Pruebas de arranque con clientes ligeros.....	28
3.7 Instalación de software requerido para los clientes.....	30
Capítulo 4. Configuraciones Adicionales de acceso.....	32
4.1 Manejo de contraseñas.....	32
4.2 Restricción de acceso como usuario root.....	33
4.3 Manejo de archivos.....	33
4.3.1 Caso 1. Usuarios pertenecientes al servidor LTSP.....	34
4.3.2 Caso 2. Usuarios con sistema operativo Linux.....	35
4.3.3 Caso 3. Usuarios con sistema operativo Windows.....	35
4.4 Configuración de server DHCP.....	37
Conclusiones.....	38
Glosario.....	40

Referencias Electrónicas..... 44



Introducción

Introducción

Actualmente el crecimiento a nivel potencial de las Tecnologías de la Información (TI) obligan a las empresas a mantenerse en una constante actualización en equipos de cómputo y software de aplicación para la realización de las actividades laborales por lo cual se debe tener una búsqueda de sistemas funcionales que satisfagan las necesidades según el área o actividad específica, en ellos se buscan principalmente dos cuestiones primordiales que puedan reducir los costos en implementación sin sacrificar el desempeño de los mismos, así como también ha crecido en los últimos años la importancia de buscar una solución ecológica a los problemas ambientales y de ahorro de energía.

Aunado a lo anterior una propuesta interesante de implementación que satisface casi por completo en su mayoría los puntos anteriores es el proyecto Linux Terminal Server Project (LTSP) el cual aporta los elementos necesarios para poder brindar un sistema seguro y eficiente para los entornos educativos y empresariales disminuyendo los costos de hardware, ya que permite el uso de equipos antiguos y con pocos recursos en comparación con los actuales, así como la reducción de administración general, haciendo centralizado la instalación y el mantenimiento del servidor.

Es importante mencionar que cuando falla un equipo de trabajo, puede ser simplemente reemplazado sin pérdida de datos o la reinstalación del sistema operativo, ya que un LTSP simplemente requiere en sus clientes sólo una interfaz de red tipo entorno de ejecución de pre-arranque (PXE), que clientes ligeros y equipos tienen incorporado este tipo de tarjeta de red en la actualidad. Esto significa que no se necesita absolutamente medio alguno de almacenamiento físico (disco duro, Compact Flash, etc.) para que el cliente ligero arranque con LTSP.

LTSP (Linux Terminal Server Project) es una tecnología clave incluida en casi todas las distribuciones GNU/Linux modernas, la cual convierte una instalación normal de GNU / Linux en un servidor de terminales. El sistema de funcionamiento de un servidor LTSP consiste en repartir por medio de la red el núcleo Linux el cual será ejecutado por los clientes y que posteriormente ejecutarán secuencias de scripts típicos de una mini distribución. Los clientes a su vez sólo se ocupan de los dispositivos básicos como el teclado, el ratón y la pantalla.

Por último cabe mencionar que los sistemas basados en servidores LTSP son verdaderos sistemas operativos multiusuario, por lo que es fácil que los usuarios puedan completar sus tareas sin tener un nivel de acceso que podría comprometer la seguridad del sistema.

Objetivo

Implementación de un servidor LTSP para centralizar la mayoría de los servicios que brinda el área de sistemas dentro de nuestra empresa así como la unificación de información en un servidor que nos brinde confianza en seguridad de los datos manejados por nuestros usuarios, día a día junto con una administración más centralizada y eficaz.

Objetivos específicos

1. Brindar seguridad al servidor LTSP dado por las constantes actualizaciones de la comunidad GNU/Linux para no exponerlo a cualquier ataque o filtración.
2. Crear una imagen que nos permita restringir tanto como sea debido por cada área el uso de los recursos del servidor y que a su vez sea fácil de utilizar por el usuario final.
3. Colocar la versión más actual del software manejado por nuestros usuarios.
4. Controlar y gestionar los servicios de una manera centralizada sobre los recursos que se otorgan al usuario final y así reducir la carga de trabajo a nivel administrativo.
5. Homogeneizar la información para poder tener un mayor control de esta, con ello lograr emplear un respaldo centralizado de información.
6. Así como una configuración adecuada del sistema para otorgar el software único y exclusivamente necesario para que cada una de las áreas pueda realizar sus labores cotidianas.
7. Además de aplicar los conocimientos adquiridos durante la formación como profesional de la ingeniería.

Antecedente Empresarial

Ovoplus del Centro S.A de C.V. es una empresa dedicada a elaborar productos derivados del huevo para la industria alimenticia desde 1996, la cual en la actualidad cuenta con dos plantas productivas ubicadas estratégicamente en las ciudades de Guadalajara y D.F.

Ovoplus del centro es uno de los principales proveedores de producto de huevo en la industria alimentaria de México, teniendo entre algunos de sus clientes empresas como son: Bimbo, Marínela, Nestlé, Tía Rosa, etc.

Ovoplus del centro forma parte de Corporación Premium, empresa mexicana que a su vez está entregada por tres compañías más: Paniplus, Makymat y Intersil.

Datos Generales de la Institución (Fig.1 Datos Empresariales):



Fig.1 Datos Empresariales.

Características del área.

En Ovoplus del Centro el área de sistemas no existe como tal, ya que esta es parte del área de contraloría, siendo así a quien se le reporta cualquier incidente sobre los sistemas dentro de la empresa.

Experiencia profesional

Dentro de la empresa cumpliré este enero del 2015 tres años laborando, de los cuales los primeros catorce meses fungí como ASI (Auxiliar de sistemas) en el cual desempeñaba las siguientes funciones:

- ❖ Mantenimiento correctivo a equipos de cómputo, impresoras y telefonía.
- ❖ Mantenimiento preventivo a equipo de cómputo, impresoras, telefonía, cámaras, DVR, relojes checadores, sistema de voceo, cableados, etc.
- ❖ Monitoreo de las VPN de la empresa.
- ❖ Trato con proveedores desde ISP hasta compra de hardware y software.
- ❖ Atención a último usuario en sitio y remotamente (Planta de Guadalajara).
- ❖ Instalación de S.O. y software (variedad de este dependiendo el área).
- ❖ Configuración de sesiones y software según área (correo, sistemas ASPEL, etc.)
- ❖ Actualización de archivos en la intranet.
- ❖ Creación de manuales para usuario final en diferentes cuestiones de software.
- ❖ Cheque y asesoría sobre el trabajo en OpenERP.
- ❖ Diagnóstico de fallas en equipo de cómputo y telefonía, en algunos casos reparación.
- ❖ Realización de respaldos de información.

Introducción

Entre muchas otras funciones más, en el mes de abril de 2014 “año en curso” empecé a desempeñar el puesto de ESI (Encargada de sistemas de la información), dentro de mis actividades se encuentran:

1. Gestionar los siguientes servidores
 - ❖ Servidor de correo
 - ❖ Servidor de archivos (samba)
 - ❖ Servidor de licencias ASPEL
 - ❖ Servidor de facturación
 - ❖ Servidor de intranet
 - ❖ Servidor de OpenERP
 - ❖ Servidor DHCP
 - ❖ Servidor de proyectos
 - ❖ Servidor de respaldos
 - ❖ Servidor OpenVPN
2. Configuración y gestión de VPN en las diferentes plantas afiliadas a nuestra empresa.
3. Configuración y gestión de los servicios proporcionados por nuestro ISP.
4. Creación de usuarios así como configuración de sus diferentes servicios.
5. Gestión de host externo y creación de cuentas.
6. Creación de correos internos.
7. Gestión y configuración de DVR.
8. Supervisión de todas las actividades de mi personal a cargo (ASI).

Por mencionar algunas, las cuales se llevan a cabo en las dos empresas situadas en México D.F y Guadalajara.

¹ La información mostrada en algunas partes de este documento es de índole ejemplificativa para con ello resguardar los datos de vital importancia para la empresa Ovoplus del Centro S.A de C.V, la cual está dando su aprobación para mostrar los datos solo con fines educativos en la realización de su informe a la señorita Wendy Estefannie Martínez Ferrusca.



Capítulo 1

Generalidades Estructurales de un servidor LTSP

Capítulo 1. Generalidades Estructurales de un servidor LTSP

El servidor LTSP agrupa varios servicios necesarios para poder iniciar y correr un cliente ligero, los servicios principales que componen a un servidor LTSP son enlistados a continuación:

- ❖ Protocolo PXE
- ❖ Protocolo TFTP
- ❖ Protocolo DHCP
- ❖ Protocolo NFS
- ❖ Protocolo gráfico XDMCP

Protocolo de transferencia de archivos trivial (TFTP)

Es un protocolo de transferencia simple, semejante a una versión básica de FTP, pero este protocolo se usa muy constantemente para transferir pequeños archivos entre ordenadores en una LAN.

El puerto a utilizar por definición como protocolo de servicio es el UDP 69 y es importante dejar claras algunas diferencias con el protocolo ftp, ya que esto puede dar pistas muy significativas por qué trabajar con TFTP y no FTP en un esquema LTSP;

- ❖ No hay mecanismos de cifrado ni autenticación.
- ❖ Puerto a utilizar 69 (UDP) en lugar de 20 ó 21(TCP) que utiliza FTP.
- ❖ Tres modos de transferencia soportados, MAIL, OCTET y NETSCAII.
- ❖ Es importante mencionar que no permite listar el contenido de los directorios como un FTP.

Ya que TFTP utiliza UDP como se mencionó líneas atrás, no podemos hablar de una definición formal de sesión en el margen de cliente-servidor, aunque se puede considerar servidor a aquel que abre el puerto 69 en modo UDP y cliente a quien se conecta. Sin embargo, cada archivo transferido vía TFTP constituye un intercambio independiente de paquetes por lo cual podemos decir que existe una relación cliente-servidor informal entre la máquina que inicia la comunicación y la que responde.

El funcionamiento base del protocolo FTPT se muestra en la siguiente (Fig. 2 Funcionamiento base del protocolo FTPT).

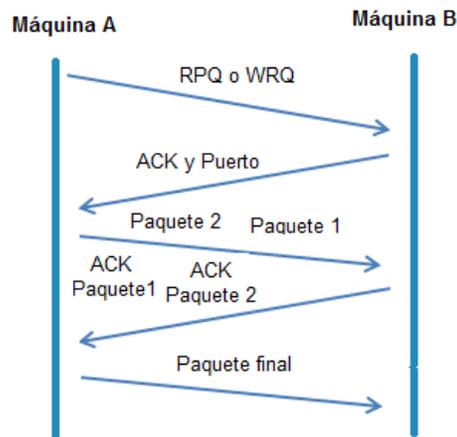


Fig. 2 Funcionamiento base del protocolo FTPT.

Para poder comprender mejor el diagrama anterior se procederá a la explicación de dicho proceso:

- ❖ La máquina A, que inicia la comunicación, envía un paquete RPQ (read request/petición de lectura) o WRQ (write request/petición de escritura) a la máquina B, conteniendo el nombre del archivo y el modo de transferencia.
- ❖ La máquina B responde con un paquete ACK de confirmación, que también sirve para informar a A del puerto de la máquina B al que tendrá que enviar los paquetes restantes.
- ❖ La máquina origen envía paquetes de datos numerados a la máquina destino, todos excepto el último conteniendo 512 bytes de datos. La máquina destino responde con paquetes ACK numerados para todos los paquetes de datos.
- ❖ El paquete de datos final debe contener menos de 512 bytes de datos para indicar que es el último. Si el tamaño del archivo transferido es un múltiplo exacto de 512 bytes, el origen envía un paquete final que contiene 0 bytes de datos.

Protocolo de configuración de host dinámico (DHCP)

Durante el proceso de arranque por red (PXE, gPXE, etherboot), una de las primeras solicitudes que realiza un cliente ligero es la petición de configuración de parámetros de red, los cuales son otorgados por un servidor DHCP. Este protocolo trabaja sobre una arquitectura CLIENTE-SERVIDOR, debido a esto podemos definir en nuestro servidor DHCP varias configuraciones de red que permitan asignar los valores a los clientes ligeros.

Capítulo 1. Generalidades Estructurales de un servidor LTSP

Los segmentos definidos en el servidor pueden realizar asignaciones dinámicas o estáticas de direcciones IP de la cuales siempre llevará un control estricto de asignación de dirección, y cuánto tiempo tuvo esa asignación en uso.

El DHCP le permite de forma centralizada las asignaciones de octetos que identifican a un host en la Red, un servidor DHCP tiene tres métodos de asignación de direcciones IP;

- ❖ Asignación Dinámica
- ❖ Asignación Estática
- ❖ Asignación Automática

El protocolo DHCP Trabaja sobre los puertos 67/UDP para servidor y 68/UDP en cliente.

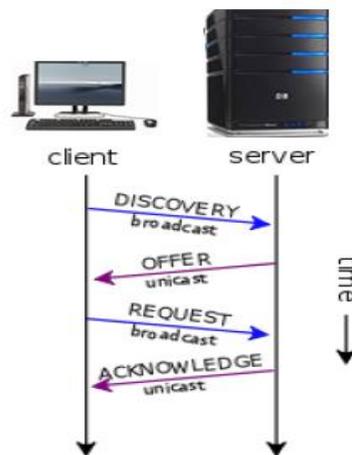


Fig. 3 Funcionamiento del servidor DHCP.

El cliente envía un paquete DHCPDISCOVER. Las direcciones IP origen y destino de dicho paquete serán 0.0.0.0 y 255.255.255.255 (broadcast) respectivamente. El servidor almacena los campos del paquete CHADDR (dirección Ethernet origen, MAC) y el de identificación del cliente.

El servidor envía un paquete DHCPOFFER, determina la configuración basándose en la dirección del soporte físico de la computadora cliente especificada en el registro CHADDR. El servidor especifica la dirección IP en el registro YIADDR.

El cliente selecciona la configuración de los paquetes recibidos de DHCPOFFER. Una vez más, el cliente solicita una dirección IP específica que indicó el servidor mediante un paquete DHCPREQUEST.

Cuando el servidor recibe el mensaje DHCPREQUEST del cliente, se inicia la fase final del proceso de configuración (Fig.3 Funcionamiento del servidor DHCP). Esta fase implica el reconocimiento DHCPACK el envío de un paquete al cliente. Este paquete incluye la duración de conexión y cualquier otra información de configuración que el cliente pueda tener solicitada. En este punto, la configuración TCP / IP se ha completado. El servidor reconoce la solicitud y le

Capítulo 1. Generalidades Estructurales de un servidor LTSP

envía acuse de recibo al cliente. El servidor DHCP responde a la DHCPREQUEST con un DHCPACK, completando así el ciclo de iniciación. La dirección origen es la dirección IP del servidor de DHCP y la dirección destino es todavía 255.255.255.255. El campo YIADDR contiene la dirección del cliente, y los campos CHADDR son la dirección física de la tarjeta de red en el cliente. La sección de opciones del DHCP identifica el paquete como un ACK.

Para optimizar el funcionamiento del servicio DHCP toda asignación cuenta con una fecha de inicio y una de vencimiento para su validez, este es el concepto de “concesión”. Para evitar los inconvenientes que se presentaban al vencimiento de la concesión en la evolución de protocolo cuando el cliente detecta que su concesión está a punto de vencer, solicita al servidor una extensión de la misma por medio de un DHCPREQUEST y del lado del servidor cuando detecta que una concesión terminará envía un DHCPNAK para consultarle al cliente si desea extenderla.

Con lo anterior aumenta la efectividad del servicio, los tiempos de las concesiones ahora son configurables en las duraciones en tiempo.

Para los fines de un servidor LTSP en este caso las concesiones se renovarán en cada inicio del cliente ligero y lo más usual es dar concesiones de 24 horas.

En un esquema de LTSP el servidor DHCP es indispensable debido a que la asignación se hace desde el inicio.

Una vez que hemos explicado el funcionamiento básico de los protocolos DHCP y TFTP vamos a ver cómo los usa PXE para llevar a cabo su proceso.

Protocolo de entorno de ejecución de pre-arranque (PXE)

Una de las partes más importantes de la estructura LTSP es el funcionamiento PXE (Preboot eXecution Environment) esta función se lleva a cabo mediante una NIC la cual se ubica en este caso en los clientes ligeros, ya que un cliente PXE puede ser un servidor, una PC de escritorio, una laptop o cualquier otra máquina que esté equipada con el código de arranque PXE.

A lo que se refiere PXE es concretamente un pre-arranque por medio de una interfaz de red, el entorno es totalmente independiente a cualquier dispositivo de almacenamiento masivo que esté presente en el equipo en cuestión.

PXE utiliza varios protocolos de red como IP, UDP, DHCP y TFTP, y conceptos como Globally Unique Identifier (GUID), Universally Unique Identifier (UUID) y Universal Network Device Interface (UNDI) los cuales solo se mencionarán pero no nos meteremos a fondo en ellos.

El protocolo PXE consiste en una combinación de los protocolos DHCP y TFTP con pequeñas modificaciones en ambos. En términos generales DHCP es utilizado para localizar el servidor de

Capítulo 1. Generalidades Estructurales de un servidor LTSP

arranque apropiado, con TFTP se descarga el programa inicial de bootstrap y archivos adicionales.

Veamos el funcionamiento de los protocolos DHCP y TFTP para posteriormente con ello poder ver como PXE utiliza ambos para conseguir el arranque del sistema en nuestros clientes ligeros.

Funcionamiento del protocolo PXE

Internamente el firmware del cliente ligero trata de encontrar un servicio de redirección PXE en la red para recabar información sobre los servidores de arranque PXE disponibles. Desde el punto de vista del esquema CLIENTE-SERVIDOR la primera petición que realiza un cliente ligero al servidor PXE es una dirección IP que está completamente asociada a un servidor DHCP definido en la arquitectura de red. Tras la asignación de IP solicitará al servidor de arranque el file path de un network bootstrap program (NBP), este será descargado a la RAM del ordenador mediante TFTP.

Se puede profundizar un poco más en el tema explicando el proceso de la siguiente manera:

Para iniciar una sesión de arranque con PXE el firmware envía un paquete de tipo DHCPDISCOVER extendido con algunas opciones específicas de PXE al puerto 67/UDP (puerto del servicio DHCP). Estas opciones indican que el firmware es capaz de manejar el protocolo PXE, por lo cual serán ignoradas por los servidores DHCP estándar.

Si un servicio de redirección PXE (Proxy DHCP) recibe el paquete DHCPDISCOVER extendido, por lo cual responde con el envío de un paquete de difusión DHCPOFFER extendido con opciones PXE al puerto 68/UDP. Este paquete se difundirá hasta que la mayoría de los clientes PXE se auto-configuren mediante DHCP. Los clientes se identificarán con su GUID/UUID.

Un paquete DHCPOFFER extendido contiene:

- ❖ Un campo PXE Discovery Control para indicar si se debe utilizar Multicasting, Broadcasting, o Unicasting para contactar con los servidores de arranque PXE.
- ❖ Una lista con las direcciones IP de los servidores PXE.
- ❖ Un menú en el que cada entrada representa un servidor de arranque PXE.
- ❖ Un prompt que indica al usuario que pulse <F8> para ver el menú de arranque.
- ❖ Un tiempo de espera que lanza la primera opción del menú de arranque cuando expira.

El servicio de proxy DHCP debe ejecutarse sobre el mismo servidor que el servicio estándar de DHCP. Puesto que ambos servicios no pueden compartir el puerto 67/UDP, el Proxy DHCP se

Capítulo 1. Generalidades Estructurales de un servidor LTSP

ejecuta sobre el puerto 4011/UDP y espera que los paquetes DHCPDISCOVER extendidos de los clientes PXE sean paquetes DHCPREQUEST. El servicio estándar DHCP debe enviar una combinación especial de opciones PXE en su paquete DHCPOFFER, de forma que los clientes PXE sepan que deben buscar un proxy DHCP en el mismo servidor, en el puerto 4011/UDP.

Para contactar con el servidor de arranque PXE el firmware debe obtener una dirección IP y el resto de información de un único paquete DHCPOFFER extendido. Tras elegir el servidor de arranque PXE y la capa de arranque PXE, permitiendo ejecutar múltiples tipos de servidores de arranque mediante un único programa de arranque.

Si un servidor de arranque PXE recibe un paquete DHCPREQUEST extendido como el descrito anteriormente y si está configurado para el tipo de servidor de arranque PXE y la arquitectura cliente solicitado, debe responder devolviendo un paquete DHCPACK extendido que son opciones específicas de PXE.

El contenido de más importancia de un paquete DHCPACK extendido se enlista a continuación:

- ❖ El file path completo para descargar el NBP vía TFTP.
- ❖ El tipo de servidor de arranque PXE y la capa de arranque PXE.
- ❖ La configuración multicast TFTP, sí debe utilizarse multicast TFTP.

Un servidor de arranque PXE debe soportar Boot Integrity Services (BIS). BIS permite al cliente PXE verificar los NBPs descargados mediante un archivo checksum que es descargado desde el mismo servidor de arranque que el NBP.

Tras recibir el paquete DHCPACK solicitado, el Network Bootstrap Program comienza a descargarse vía TFTP con los parámetros recibidos y una vez descargado se carga en la RAM del cliente y se pasa a su ejecución.

En el esquema convencional LTSP una vez que la imagen de Kernel se ha entregado y ejecutado por el cliente ligero se completa la interacción propia con un servidor PXE, esto no quiere decir que partes que lo componen dejen de interactuar en el esquema CLIENTE-SERVIDOR.

Como aportación se ha definido que un servidor PXE está compuesto por un servicio TFTP (Servicio xinet.d), FTP (vsftp), DHCP y NFS.

Servidor NFS (Sistema de archivos de red)

Es un protocolo que permite acceso remoto a un sistema de archivos a través de la red. Todos los sistemas Unix pueden trabajar con este protocolo, cuando involucramos sistemas Microsoft se debe utilizar Samba en su lugar.

El protocolo NFS tiene grandes carencias de seguridad:

- ❖ Todos los datos pasan a través de la red sin cifrar.

Capítulo 1. Generalidades Estructurales de un servidor LTSP

- ❖ El servidor fuerza restricciones de acceso basado en la dirección IP del cliente.
- ❖ Cuando se provee acceso a una máquina cliente a un espacio NFS compartido mal configurado, el usuario root del cliente puede acceder a todos los archivos en el espacio compartido ya que el servidor confía en el nombre de usuario que recibe del cliente.

En un servidor LTSP puede o no requerirse tal servicio, pero lo más usual es que a través de él se comparta la imagen del kernel que se ha creado para los clientes ligeros.

Protocolo de Sesión Remota X Window System / XDMCP

Una sesión o escritorio remoto es una tecnología que permite a un usuario poder trabajar en una computadora a través de su escritorio gráfico desde otra terminal ubicada en otro lugar físico. La tecnología de sesión o escritorio remoto se basa en el protocolo cliente-servidor que permite el envío y recepción de la entrada y salida de eventos y pantallas gráficas.

Para que se tenga un buen funcionamiento de la sesión o escritorio remoto, el protocolo a utilizarse debe cumplir una serie de requisitos:

- ❖ Latencia. El retardo de las comunicaciones es más importante que el ancho de banda.
- ❖ Balanceo de funcionalidad entre cliente y servidor.
- ❖ Representación gráfica. Indica el tipo de visualización del escritorio remoto. Existen cuatro modalidades: gráficos de alto nivel, gráficos de bajo nivel, primitivas de dibujo en 2D y píxeles en bruto.
- ❖ Sincronización.

Existen diversas implementaciones de sesión o escritorio remoto en la actualidad con sus propios protocolos de comunicaciones en nuestro caso solo nos enfocaremos en el protocolo XDMCP.

X Window System (sistema de ventanas X) es un software que fue desarrollado a mediados de los años 80 para dotar de una interfaz gráfica a los sistemas Unix. Este protocolo permite la interacción gráfica en red entre un usuario y una o más computadoras haciendo transparente la red para éste. Generalmente se refiere a la versión 11 de este protocolo, X11, el cual está en uso actualmente.

El sistema de ventanas X distribuye el procesamiento de aplicaciones especificando enlaces cliente-servidor. El servidor provee servicios para acceder a la pantalla, teclado y ratón, mientras que los clientes son las aplicaciones que utilizan estos recursos para interacción con el usuario. De este modo mientras el servidor se ejecuta de manera local, las aplicaciones pueden ejecutarse remotamente desde otras máquinas, proporcionando así el concepto de transparencia de red ya antes mencionado.

Capítulo 1. Generalidades Estructurales de un servidor LTSP

Debido a este esquema cliente-servidor, se puede decir que X se comporta como una terminal gráfica virtual. El hecho que exista un estándar definido para X permite que se desarrollen servidores X para distintos sistemas operativos y plataformas, lo que hace que el código sea muy portable. Por ejemplo, permite tener clientes X ejecutándose en un potente servidor UNIX mientras los resultados son visualizados en un PC de escritorio con cualquier otro sistema operativo funcionando.

X no es un gestor de ventanas, necesita de uno para controlar el manejo de ventanas. Esto trae la ventaja de que permite al usuario instalar uno o más administradores de ventanas de su preferencia.

X usa el modelo cliente-servidor: un servidor X se comunica con varios programas cliente. El servidor acepta los pedidos para la salida gráfica (ventanas) y devuelve la entrada del usuario (desde el teclado, del ratón, o de la pantalla táctil).

X proporciona la exhibición por pantalla y los servicios de entrada/salida a las aplicaciones, así que es un servidor; las aplicaciones usan estos servicios, por lo tanto son los clientes.

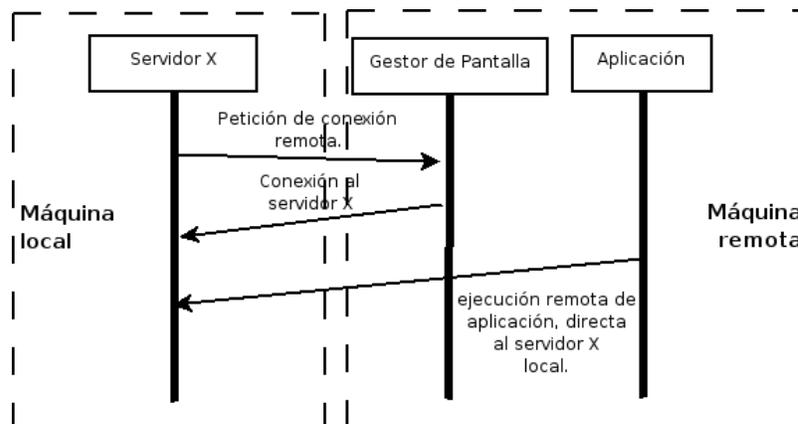


Fig. 5 Diagrama del funcionamiento base del servidor X.

Después de que se establezca la conexión, cuatro tipos de paquetes son intercambiados entre el cliente y el servidor sobre el canal de comunicación (Fig.5 Diagrama del funcionamiento base del servidor X):

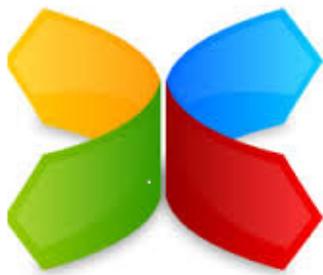
- ❖ **Petición.** El cliente pide información al servidor o solicita que éste realice una acción.
- ❖ **Respuesta.** El servidor responde a una petición.
- ❖ **Evento.** El servidor informa al cliente de un acontecimiento, tal como la entrada del teclado o del ratón, que una ventana está siendo movida, redimensionada, expuesta, etc.
- ❖ **Error.** El servidor envía un paquete de error si una petición es inválida. Puesto que las respuestas están en cola, los paquetes de error generados por una petición pueden no enviarse inmediatamente.

Capítulo 1. Generalidades Estructurales de un servidor LTSP

X es primariamente una definición de primitivas de protocolo y gráficas, y deliberadamente no contiene especificaciones de diseño de interfaz de usuario, como estilos de botón, menú, barra de título para las ventanas, etc. Para estos casos un software de aplicación tal como los manejadores de ventana que en la actualidad son diversos así como los ambientes de escritorio, o las interfaces gráficas de usuario específicas de una aplicación define y proporcionan tales detalles de personalización. Como resultado de lo anteriormente mencionado, no hay interfaz X típica por lo cual varios ambientes de escritorio que están a disposición han sido populares entre los usuarios.

Es muy común usar X con un ambiente de escritorio, que, independientemente del manejador de ventana, incluyen varias aplicaciones usando una interfaz de usuario consistente. Haciendo a GNOME, KDE y XFCE los ambientes de escritorio más populares.

Un **X Display Manager** (administrador de pantalla X) mantiene los procesos del servidor X activos en él, conectándolo a una pantalla física y proporcionando un cuadro de diálogo que permita iniciar sesión en el mismo a todos los ordenadores que lo requieran. Nuestro cliente marca una llamada al XDMCP del Display, el cual lo obtiene de la siguiente manera: X-query 192.168.x.x: display donde quiere activarse. Al ingresar tal comando, nuestro cliente inicia la llamada de conexión y el servidor de XDMCP le envía el prompt de login (un display como XDM) de respuesta, donde nuestro cliente ingresa su cuenta con su usuario y contraseña, tal y como si estuviera en la misma máquina servidora validándose en su propio escritorio.



Capítulo 2

Requerimientos del Proyecto

Capítulo 2. Requerimientos del Proyecto

Capítulo 2. Requerimientos del Proyecto

Dentro de la empresa se busca bajar costos en la adquisición de hardware en materia de computación así como cerrar el acceso a nuestra LAN mediante una solución práctica que permita tener el control sobre esta para evitar que los recursos sean mal utilizados por usuarios no identificados o bien externos a la empresa.

Ya que actualmente los nodos se encuentran libres para ser utilizados por cualquier equipo que se conecte a estos lo cual hace vulnerable la LAN si llega a ver algún usuario o externo mal intencionado.

Para corregir los dos problemas anteriores se propone un servidor LTSP que trabaje con terminales ligeras las cuales nos ayudarán a reducir considerablemente el gasto en hardware ya que no requieren, disco duro ni una RAM de capacidad elevada y mucho menos necesitarán una licencia en software ni S.O, ya que todos los servicios serán entregados por el servidor LTSP bajo GNU/Linux.

Para un mayor control de la red se empleará un servidor DHCP bajo Mac el cual restringirá el uso de la red mediante políticas que solo darán acceso al equipo que se encuentre dado de alta en este, restringiendo las IP sueltas a dos para detectar intrusos de inmediato si se llegara a dar el caso.

Lo anterior también será enriquecido configurando los aparatos de control switch y router en los cuales se colocarán dos subredes una para los usuarios LTSP y otra para los usuarios con S.O nativo, estas subredes tendrán accesos a los archivos que bajo las listas de control se les permita dentro del servidor LTSP, pero a su vez, no podrán comunicarse entre sí. Con esto se busca tener un mayor control sobre el tráfico que se genera para el server LTSP el cual quedará restringido únicamente para sus usuarios. No está por demás decir que este tema es muy extenso por lo cual solo se coloca como comentario de enriquecimiento para el cual ponemos el siguiente diagrama (Fig.6 Simulación de subredes).

Capítulo 2. Requerimientos del Proyecto

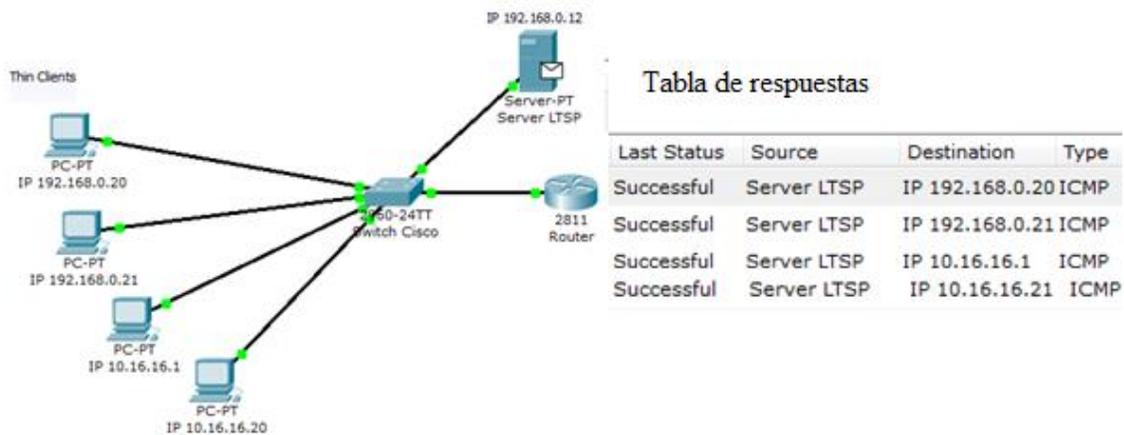


Fig. 6 Simulación de subredes.

Un punto muy importante es la seguridad por lo cual se ha convertido en un desafío clave para los administradores y LTSP reconoce y lo maneja bastante bien.

Los sistemas operativos con LTSP incluidos, siendo los sistemas operativos basados en Linux, disfrutar de las ventajas de seguridad de su Unix y herencias de código abierto. Esto se traduce en una mayor calidad del código y no hay spyware y virus, al igual que afectando otros sistemas operativos.

Además, tiene una estricta política de seguridad proactiva que significa que muchos de los problemas comunes, tales como puertos abiertos o software mal configurado, nunca lo hacen en el producto puesto en libertad. Por último, los sistemas basados en LTSP son verdaderos sistemas operativos multiusuario, por lo que es fácil que los usuarios puedan completar sus tareas sin tener un nivel de acceso que podría comprometer el sistema.

Análisis de requerimientos

Para el Servidor:

Se requiere dar servicio a 20 clientes ligeros con una proyección de crecimiento a considerar mínima del 50%.

Por lo cual un requerimiento vital para implementar en el proyecto es el cálculo de la RAM que utilizará el servidor. Para saber la cantidad de RAM ideal para utilizar en nuestro servidor seguimos esta fórmula "oficial":

$$\text{RAM Servidor} = 256 + (100 * \text{\#terminales})$$

- ❖ Por lo tanto la RAM mínima de nuestro servidor sería de 3256 MB.

Capítulo 2. Requerimientos del Proyecto

- ❖ Se necesita un procesador potente conviene que sea de varios núcleos para evitar latencias.
- ❖ Respecto a los discos, conviene que sean con capacidad mínima de un Terabyte y RAID (0, 1,10) por el mismo motivo descrito en el punto anterior, ya que las llamadas de lectura y escritura de todos los clientes caen sobre el hardware que compone al servidor.

Para los Clientes:

- ❖ Memoria RAM mínima de 256 Mb.
- ❖ Tarjeta de red de 100 Mbps que soporta PXE o arranque de red similar.
- ❖ Procesador mínimo a 300 MHz.

Alcances y limitaciones del Proyecto

Este proyecto se basará en la implementación de un servidor LTSP y la creación de la imagen que otorgará a sus clientes la cual se debe soportar el software específico para cada área de la empresa en la versión más actual que cubra las necesidades de las mismas.

Ahora bien, si se habla de los alcances que se pueden tener mediante un servidor LTSP, estos son variados dependiendo el enfoque o requerimientos del cual esté proporcionado, ya que mediante un LTSP podemos emplear variedad sistemas de administración como servicios nos convenga.

Los servicios que se pueden implementar en un servidor LTSP en este caso están enfocados a la administración de los datos y de la red.

Desde un servidor de manejo de archivos, que cubriría el soporte de todas las áreas que componen la empresa, hasta escritorios remotos con S.O Windows según las necesidades del usuario.

A nivel software podemos mencionar ante todo es que al usar un sistema operativo bajo licencia GNU/GPL como Linux obtendremos un producto de calidad, sin coste de licencias (En Windows se pagan a nivel de servidor y de usuario) y más seguro que otros sistemas operativos.

A nivel de hardware

El ahorro en equipos y material informático derivado de trabajar con clientes ligeros es muy alto ya que se pueden reciclar equipos antiguos o bien adquirir clientes ligeros y el usuario estará utilizando un sistema operativo actual, esto trae múltiples beneficios uno de ellos son los pocos requerimientos que se necesitan para emplear este tipo de equipo, a continuación se muestra en la Tabla1 las diferencias entre el uso de un equipo normal y un cliente empleando LTSP.

Capítulo 2. Requerimientos del Proyecto

Tabla 1. Requerimientos de Hardware Generales.

Requerimientos de Hardware		
Características	CPU normal	Cliente LTSP
S.O	Windows 8	Ubuntu Server 12.04
HDD	16 GB (32 bits) o 20 GB (64 bits)	No requiere
RAM	1 (GB) (32 bits) o 2 GB (64 bits)	256 MB
Procesador	1(GHz) o superior compatible con PAE, NX y SSE2	300 MHz
Tarjeta gráfica	Dispositivo gráfico Microsoft DirectX 9 con controlador WDDM	Tarjeta Gráfica VGA

A nivel de costos

Al emplear el uso de clientes ligeros no es necesario hacer gastos por hardware innecesario podemos bajar el gasto en un 100% si se reutiliza equipo ya obsoleto o bien en un 83% si se compara el precio de un CPU que se maneja como precio mínimo en los \$6000 pesos con el costo de un cliente ligero que se maneja desde los \$1000 pesos.

De la mano de lo antes mencionado se muestra el estudio que se realizó en cuanto a costos (Tabla 2. Costos PC) en arquitectura que requiere un proyecto como el que se está realizando, así como la clara muestra del ahorro que la implementación de clientes ligeros da como resultado.

Se comenzará por mostrar el hardware básico que se utiliza en un entorno normal (No empleando clientes ligeros). Para tal caso se muestran los costos de las PC de escritorio a continuación:

Tabla 2. Costos de PC.

Costos de PC					
Costo	\$7,999	\$5,999	\$5,500	\$7,871	\$5,800
Marca	Acer AXC-603-MD15	Acer AXC-603-MO12 1	HP 2020	Lenovo h500s	Armada
Procesador	Pentium QUAD Core J2900	Intel Celeron J1900	Intel Pentium Dual 2020	Celeron J1800	Intel Pentium CG3220
RAM	4GB	4GB	4GB	4GB	4GB
HDD	1TB	500 GB	1TB	500 GB	120 GB

Como se puede notar a simple vista hay mucho hardware sobrado dentro de los elementos que componen las PC de escritorio normalmente utilizadas así bien también se puede ver en esta tabla como se muestra una máquina armada de recursos genéricos la cual aun con la reducción de varios elementos sobrados como disco duro por mencionar alguno su costo sigue siendo arriba de los \$5000 pesos.

Dado a la capacidad a cubrir por usuario dentro de la empresa el gasto mínimo considerando el precio antes mencionado sería de:

Capítulo 2. Requerimientos del Proyecto

El número de usuarios * El costo de la PC= Al gasto en equipo global

Tomando en cuenta 20 usuarios y los \$5,000 pesos base de una PC el gasto inicial sin licencias de software sería de \$100,000 pesos un gasto bastante considerable para la inversión de un proyecto.

Ahora bien veamos los costos del equipo faltante, los cuales se muestran a continuación en las siguientes tablas.

Tabla 3. Costos Switch.

Switch					
Costo	\$60,375.00	\$27,869.00	\$16,500.00	\$29,620.38	\$20,873.68
Marca	HP	Cisco	Cisco	Cisco	Cisco
Modelo	DL380E- G8	SG500X-48	SRW2048	ASG50052PK9	ASG50052K9N
Puertos	24 a 48	48	48	48	48

Tabla 4. Costos Servidores.

Servidor						
Costo	\$8,684.00	\$12,293.00	\$14,099.00	\$20,457.18	\$16,994.00	\$24,267.20
Marca	HP	HP	DELL	IBM	Lenovo ThinkServer	HP
Modelo	ML10	ML310e G8	PowerEdge R220	IBM X3250 M3	TS140	HP ProLiant DL160 Gen8 E5-2603 1P
Micro Procesador	Intel®Xeon®	Intel® Xeon®	Intel® Celeron®	Intel Xeon X3430	Intel Xeon E3- 1225V3	Intel® Xeon® E5- 2603
RAM	2 GB	4 GB	4 GB	4 GB	4 GB	4 GB
HDD	No incluido	No incluido	500 GB	No incluido	500 GB	No incluido

En este momento podemos detenernos un poco para comentar los gastos que se harían al comprar el equipo mostrado en las tablas anteriores, como se puede ver el gasto mínimo que se obtendría al adquirir este equipo nuevo sería de \$25,184.00 que en conjunto con el gasto de las PC nuevas anteriormente mostradas nos da un total de \$125,184.00 el cual es el gasto mínimo a considerar para el desarrollo del proyecto.

Es importante señalar que un gasto más a considerar serían las licencias del S.O. que se desee adquirir esto si fuera el caso de una implementación de Windows, en este punto comenzamos a ver las ventajas que nos ofrece el servidor LTSP que al ser de un S.O. libre este no tiene ningún gasto para añadir al proyecto.

Capítulo 2. Requerimientos del Proyecto

Ahora bien llegando al punto de recordar que la implementación del servidor LTSP se busca realizar mediante terminales ligeras, a continuación se muestran los costos (Tabla 5. Costos Terminal Ligera) de estas:

Tabla 5. Costos Terminal Ligera.

Thin Client					
Costo	\$1,550.00	\$2,120.00	\$1,600.00	\$1,157.00	\$970.00
Marca	Centerm C75	Centerm GM810	Centerm C13	Centerm C75	Thin Client Cloud Computer
CPU	SOC SMSC UFX 6000	ARM Cortex A9 1.0GHz	ARM Cortex A9	SOC SMSC UFX 6000	ARM
Display	VGA: 2048X1152	VGA: 1920*1200	VGA: 1920*1200	VGA: 2048*1152	VGA: 1440*900
RAM	1GB	512MB	512MB	1GB	1GB

Se puede ver claramente que una terminal ligera tiene un costo promedio de \$1,479.40 tomando en cuenta los precios mostrados en nuestra tabla. Ahora bien si sacamos el total de las máquinas a utilizar se observa lo siguiente:

El número de usuarios * El costo de la Terminal Ligera = Al gasto en equipo global

Tomando en cuanto lo anterior el gasto global por los 20 usuarios sería de \$29,588.00 un gasto significativo pero bastante inferior al gasto en PC normales.

Con este estudio de costos se muestra como la utilización de terminales ligeras ahorra un gasto del 70.41% en comparación con el gasto que se realizaría en la compra de PC normales.

Dado que se reutilizará tanto el switch como el server con los que ya cuenta la compañía el gasto total del proyecto se reduce a tan solo el total de la compra de las 20 terminales ligeras un gasto bastante pequeño para una empresa de mediana escala como lo es Ovoplus del Centro.

Limitaciones

Las limitaciones que se distinguen dentro del proyecto son:

Se debe utilizar el hardware actual tanto para el servidor como el switch, no habrá inversión para poder comprar dicho hardware nuevo. Por el motivo anterior no se puede proporcionar al servidor de algún servicio extra que consuma muchos recursos.

Los clientes ligeros no se colocarán en el área de contabilidad ya que no es posible cargar al servidor del software destinado para el funcionamiento óptimo de la misma.

Especificación funcional

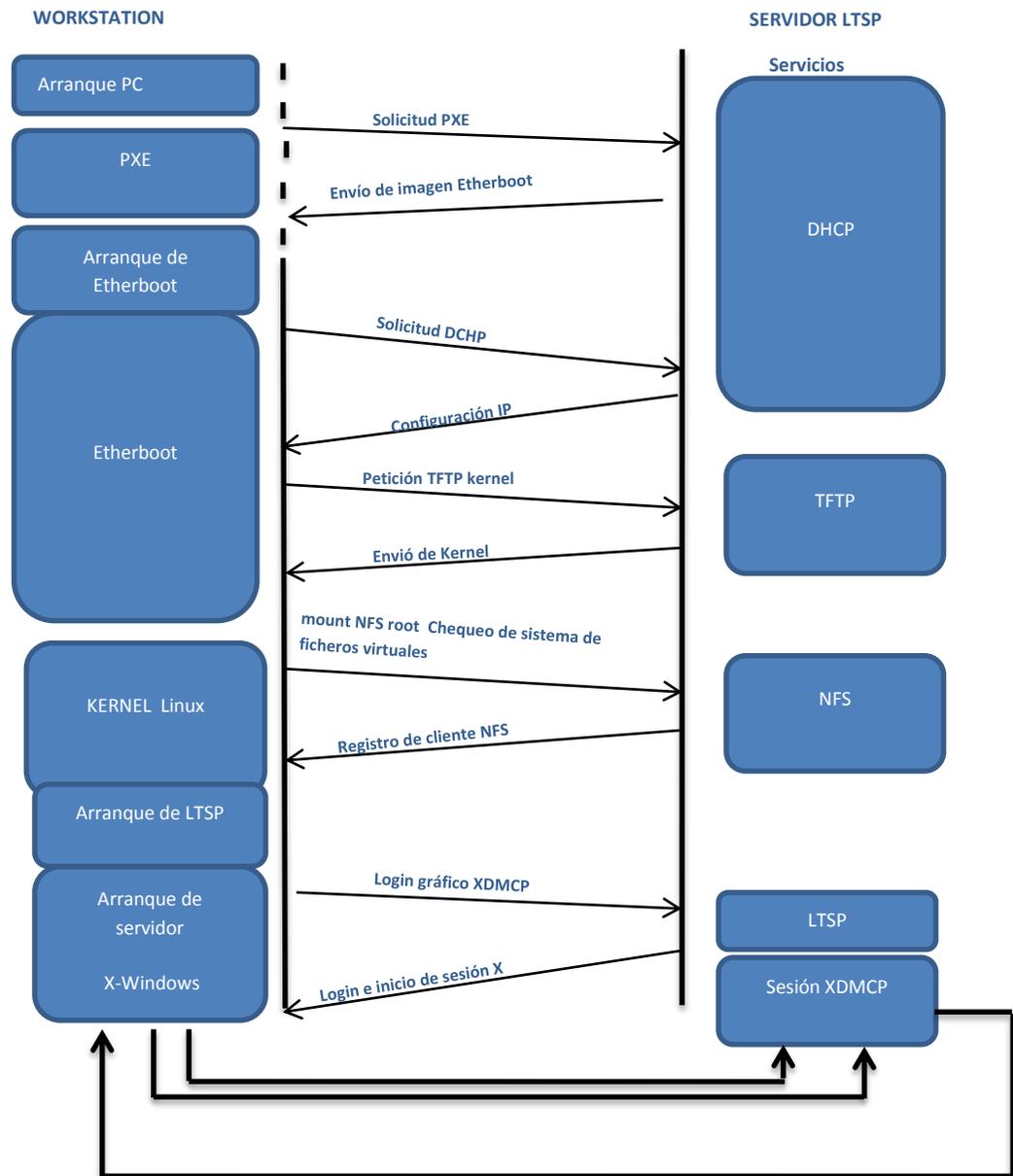


Fig. 7 Funcionamiento de un servidor LTSP.

Cuando el servidor LTSP está en funcionamiento y un cliente se inicia ocurre la siguiente interacción entre ellos (Fig. 7 Funcionamiento de un servidor LTSP):

- El cliente arranca mediante el protocolo PXE, que le permite iniciar desde la tarjeta de red como dispositivo de arranque.
- El cliente hace un requerimiento para una dirección IP mediante el protocolo DHCP

Capítulo 2. Requerimientos del Proyecto

- c.) El servidor DHCP incluido dentro del servidor LTSP responde al requerimiento y le envía su configuración de direccionamiento IP, junto con un parámetro que le indica dónde se encuentra la imagen del sistema operativo dentro del servidor TFTP.
- d.) El cliente hace una petición hacia el servidor TFTP para obtener la imagen del sistema operativo para iniciar la carga del sistema.
- e.) El cliente recibe la imagen e inicia el sistema operativo GNU/Linux, detecta el hardware, los dispositivos de almacenamiento y se conecta con el servidor X Windows.

Aquí concluye el procesamiento en el lado del cliente, el resto de operaciones son realizadas remotamente en el servidor.

Plan de trabajo

El plan de trabajo fue estructurado mediante un mínimo de horas en horario laboral, buscando el menor impacto a las labores cotidianas ejercidas en mi puesto como se muestra en la tabla número 6 por actividades, especificando los tiempos de estas con la fig.8 Diagrama de Gantt de actividades.

Tabla 6. Calendario de Actividades.

Trabajo Técnico		
Actividad	Periodo de realización	Horas previstas
Instalación del LTSP (ILTSP)	Del 7 al 14 de Febrero	12h
Configuración de servicios (Cofg.)	Del 17 al 21 de Febrero	12h
Pruebas de funcionamiento iniciales (PI)	Del 24 al 10 de Marzo	24h
Instalación y configuración de software (Conf. Soft)	Del 11 al 21 de Marzo	16h
Pruebas de resistencia (Estrés)	Del 24 de Marzo al 11 de Abril	48h

Diagrama de Gantt

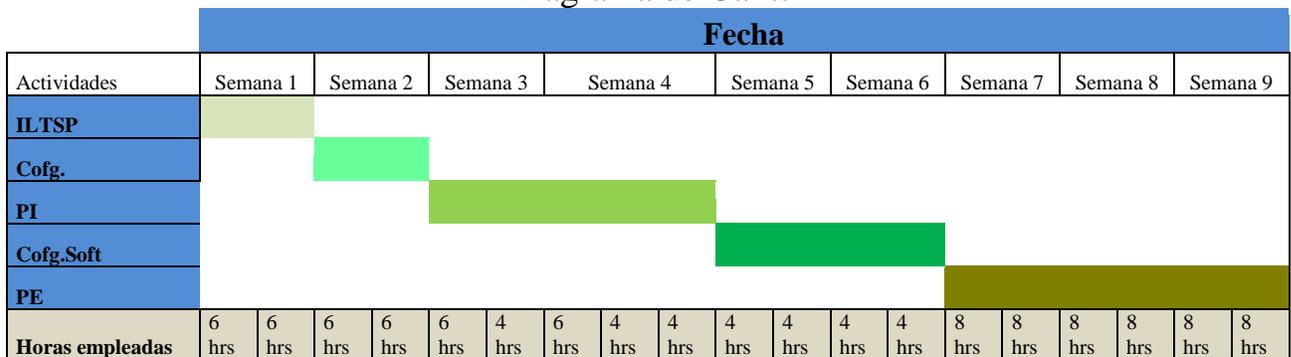


Fig. 8 Diagrama Gantt de actividades.

Capítulo 2. Requerimientos del Proyecto

A continuación se muestra el diseño estructural de red (Fig. 9 Diseño de Red) que se implementará en el proyecto haciendo énfasis en que no es el único para tales fines.

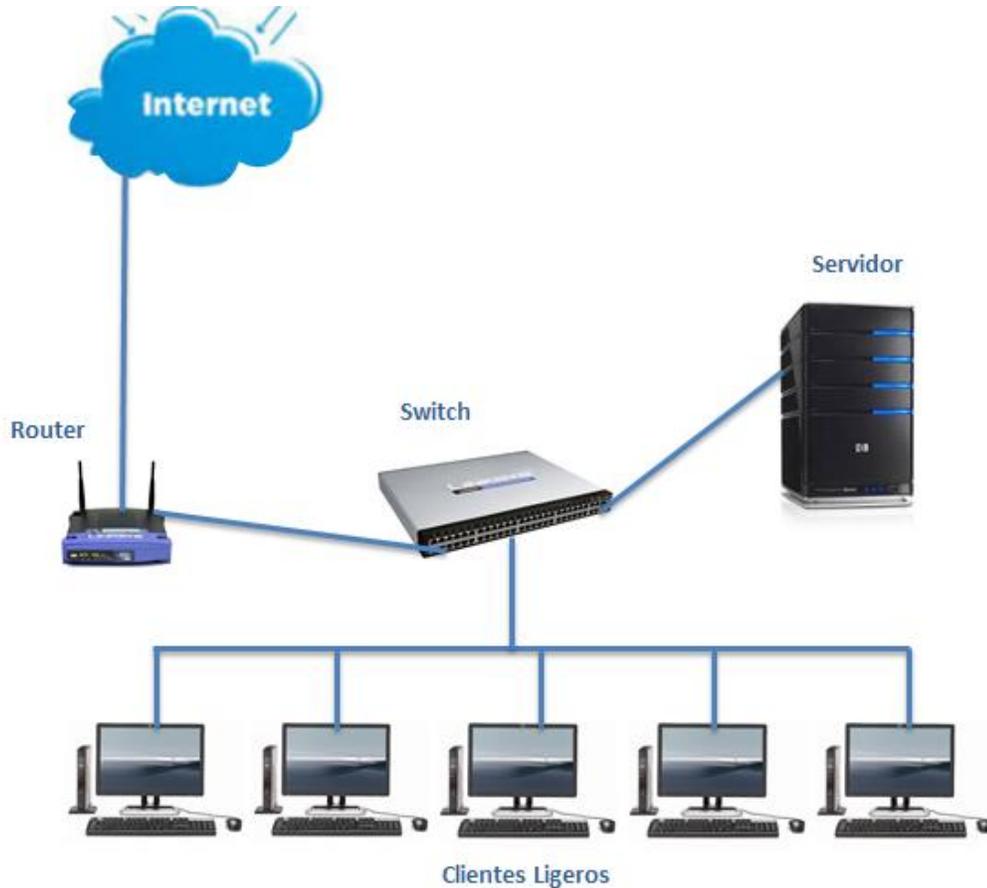
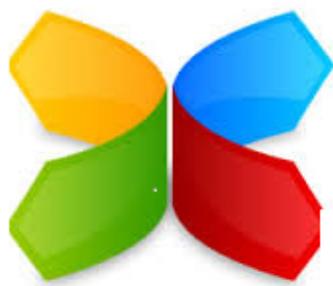


Fig. 9 Diseño de Red.

Se utilizaron direcciones IP de clase “C” ya que el servicio será brindado a menos de 250 máquinas. Se utilizó el segmento 192168.10.host para la realización de pruebas fuera de la LAN manejada dentro de la empresa.

Se utilizará el S.O Ubuntu 12.04 ya que cuenta con soporte de 5 años lo cual nos garantiza su actualización y soporte por parte de la comunidad GNU/Linux durante el tiempo mencionado.



Capítulo 3

Implementación



Capítulo 3 Implementación

Para la realización de servidor LTSP se llevaron a cabo las siguientes actividades:

Búsqueda de Documentación

La documentación fue casi obtenida en su totalidad por medio de internet siendo este el recurso con más información respecto al tema tratado y a su vez el más accesible dentro del área laboral.

Análisis de requerimientos

Los requerimientos fueron fundamentalmente basados con la prioridad de tener un servidor eficiente el cual pueda soportar adecuadamente la carga de los clientes ligeros por lo cual como anteriormente se especificó este dependerá del número de clientes a los que se les otorgará el servicio.

La definición de la estructura y topología de red es un requerimiento importante, para así poder definir adicionar más de una tarjeta de red en el servidor si esto llegara a ser necesario.

En cuanto al hardware de los clientes ligeros, deben contar con placa base, CPU, Memoria RAM, fuente de alimentación, teclado, ratón, pantalla y tarjeta de red con soporte PXE.

Según las necesidades ya expuestas anteriormente, el análisis de requerimientos se basó en específico en la funcionalidad del server cuantificando un 50% más de los usuarios actuales para con ello tomar en cuenta el crecimiento de tal proyecto en años futuros dentro de la organización.

La instalación del server LTSP se llevó a cabo en Virtual Box 4.3.10, de igual manera se crearon a los clientes en máquinas virtuales en dicho software, las cuales sirvieron para probar el funcionamiento del software seleccionado.

Capítulo 3. Implementación

Selección de software

Mediante una breve investigación sobre los componentes tanto de Ubuntu Server 12.04 LTS y Edubuntu 13.10 por traer ya incluido el paquete LTSP pero con la gran desventaja de que actualmente ya no cuenta con soporte para la distribución por lo cual se llegó a la conclusión de utilizar Ubuntu 12.04 por ser más estable y tener un tiempo 5 años de soporte en esta versión, donde se cuenta con actualizaciones de seguridad y en general sobre todo el funcionamiento del sistema, a continuación se menciona algunas de sus características:

- ❖ Entorno de escritorio GNOME 3.2, con algunos paquetes de GNOME 3.4.
- ❖ Interfaz Unity personalizable
- ❖ 100% accesible
- ❖ Centro de control más limpio
- ❖ Mejoras a Mozilla Thunderbird
- ❖ Reproductor de música Rhythmbox
- ❖ Proceso de arranque sin parpadeos
- ❖ Mejorada la velocidad del arranque
- ❖ Mejorado el soporte para múltiples monitores
- ❖ Python 3.2 y 2.7
- ❖ Mejorado el soporte para plataformas ARM
- ❖ Implementación de la producción en Juju
- ❖ Gestión de la energía en la nube y proyecto Cloud-Live
- ❖ Libre Office estaba actualizado a la versión 3.5.2
- ❖ La opción de utilizar Gnome clásico Fallback, que no es Gnome como entorno gráfico

Los mínimos requisitos recomendados para el óptimo funcionamiento del S.O Ubuntu Server 12.04 son los siguientes:

- ❖ RAM de 512 MB
- ❖ Procesador x86 a 1GHz
- ❖ HDD de 5GB

El software se descargó de la página oficial de Ubuntu, <http://www.ubuntu.com/download/server> en un formato de 32bits.

Instalación de Ubuntu

Una vez ya corriendo el CD o DVD, primero se selecciona el idioma de nuestra preferencia para realizar la instalación.

A continuación se selecciona instalar Ubuntu Server (Fig.10).

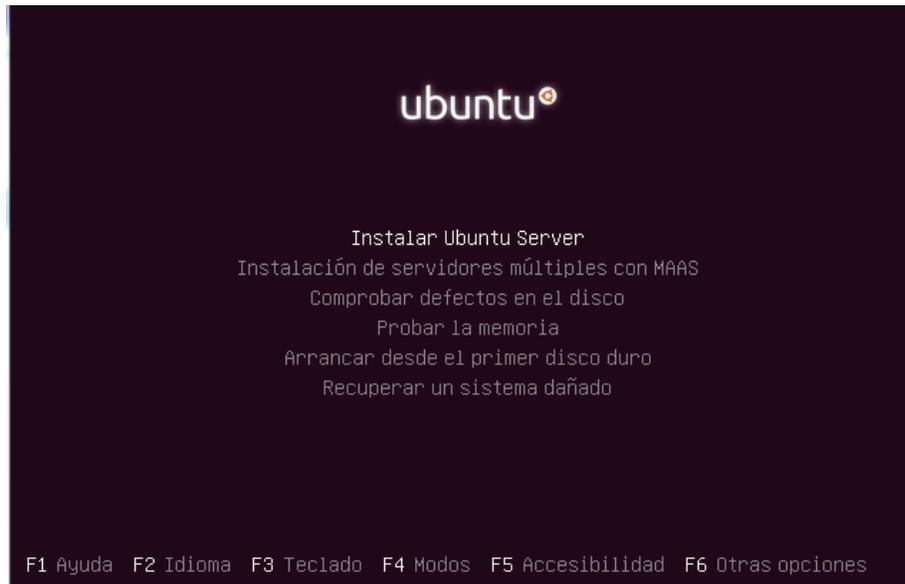


Fig. 10 Inicio de instalación Ubuntu server.

A continuación se mencionan los pasos de instalación a grandes rasgos.

- ❖ Como país de instalación le indicamos México.
- ❖ Seleccionar el idioma del teclado en este caso será en español latinoamericano.
- ❖ Comenzará la instalación de los primeros componentes y pedirá que seleccionemos nuestra interfaz de red principal.
- ❖ Enseguida nos pedirá el nombre que tendrá nuestra máquina así como la creación del primer usuario.
- ❖ La instalación sigue y nos muestra la zona horaria (Fig. 11), verificamos que sea correcta y continuamos.

Capítulo 3. Implementación

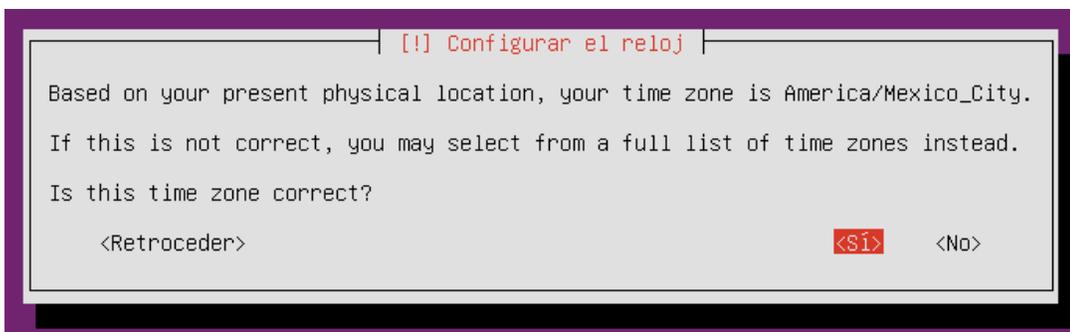


Fig. 11 Verificación de Zona horaria.

- ❖ Nos mostrará la forma de partición (Fig.12) que te ofrece para el disco, selección el deseado y continuamos.

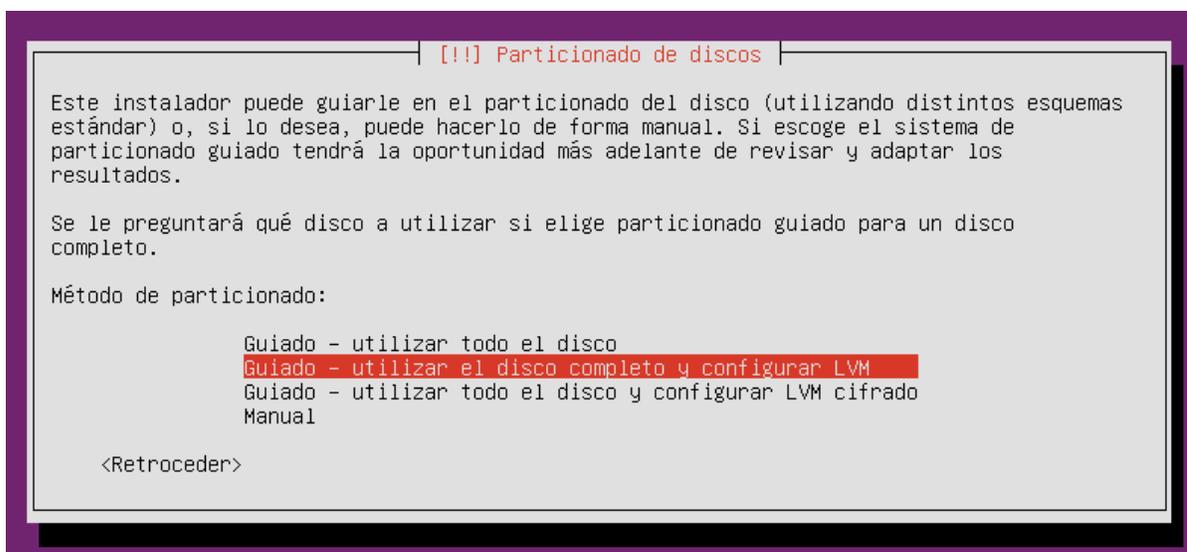


Fig. 12 Particionado de discos.

- ❖ Autorizamos la escritura en los discos. Ahora solo queda esperar que comience la instalación del sistema operativo (Fig.13) el tiempo puede variar según las características del sistema en el cual se está llevando a cabo la instalación.

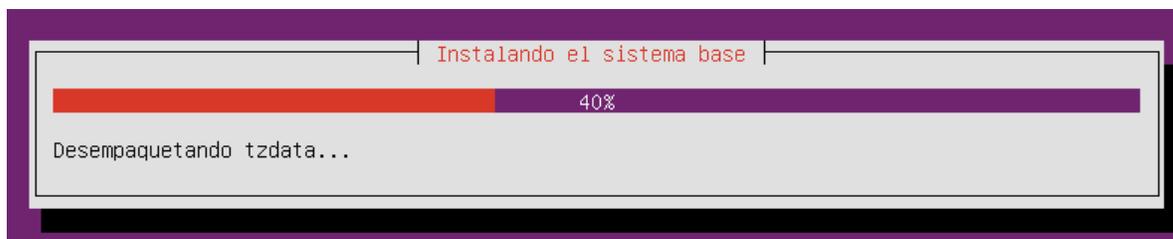


Fig.13 Carga de archivos.

Capítulo 3. Implementación

- ❖ La instalación se detiene para mostrarnos los paquetes que podemos instalar (Fig. 14), se realiza selección. En este caso no selecciono ninguno y posteriormente voy instalando las cosas conforme las necesito.



Fig. 14 Preinstalación de software.

Para finalizar nos pedirá el reinicio de la máquina una vez terminada la instalación, con lo cual ya tenemos Ubuntu Server funcionando, sin interfaz gráfica solamente con Kernel instalado.

Instalación y configuración de servicios LTSP

Una vez teniendo instalado el servidor comenzamos con la instalación del paquete LTSP.

- ❖ Instalación del servidor SSH.

```
apt-get install ssh
```

- ❖ Se instala el paquete LTSP.

```
apt-get install ltsp-server-standalone
```

Nota: El proceso se tardará de 10 a 30 minutos según los recursos del sistema.

- ❖ Una vez terminada la instalación anterior crearemos la imagen del servidor LTSP.

```
sudo ltsp-build-client
```

- ❖ Ya con lo anterior se procede a configurar las interfaces de la red.

Capítulo 3. Implementación

```
sudo vim /etc/network/interfaces
```

- ❖ Así como también se debe configurar al server DHCP para proporcionar la IP a los clientes.

```
sudo vim /etc/ltsp/dhcpd.conf
```

- ❖ Una vez hecho lo anterior se crean usuarios.

```
sudo adduser usu1
```

- ❖ Para que los cambios realizados en las configuraciones tengan efecto en los clientes debemos actualizar la imagen.

```
sudo ltsp-update-image
```

- ❖ Por último reiniciamos el sistema.

```
sudo shutdown -r now
```

Pruebas de arranque con clientes ligeros

Una vez terminada la instalación del servidor LTSP se llevó a cabo la primera prueba de arranque de una terminal ligera, para dicho caso se conectó a la LAN una terminal ligera la cual fue configurada desde BIOS para bootear desde red.

Una vez que enciende la terminal se muestran las siguientes pantallas en su inicio (Fig. 15).

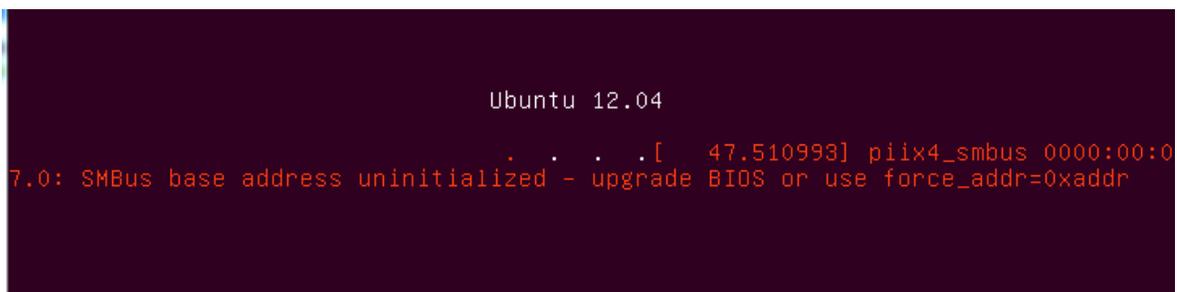


Fig. 15 Pre-arranque del cliente.

Una vez culminada la carga de inicio de sesión el servidor DHCP dentro del sistema ya ha proporcionado una IP al cliente, con lo cual se nos mostrará la pantalla donde se debe introducir

Capítulo 3. Implementación

usuario y posteriormente contraseña (Fig. 16) para así comenzar a utilizar los recursos del servidor LTSP.



Fig. 16 Inicio de sesión del cliente.

Hay que mencionar que las sesiones de usuario se pueden personalizar según convenga individualmente sin olvidar que el software y los recursos solo se ejecutarán desde el server principal, a continuación se muestra un pantallazo del escritorio XFCE (Fig. 17) el cual fue elegido para darle una mayor versatilidad a nuestro servidor ya que este consume un mínimo de recursos del sistema.



Fig. 17 Escritorio cliente.

Instalación de software requerido para los clientes

El escritorio que se cargó al servidor ya cuenta con software precargado (Fig. 18) el cual se puede apreciar en la siguiente imagen.



Fig. 18 Software precargado.

Para las funciones principales de los usuarios se cargó el software básico dentro del servidor LTSP.

Instalación de software básico mediante terminal comandos a ejecutar:

- ❖ Navegador Mozilla Firefox

```
# apt-get install firefox
```

- ❖ Cliente de correo Thunderbird

```
#apt-get install thunderbird
```

- ❖ Herramienta de oficina Libre office

```
# add-apt-repository ppa:libreoffice/ppa
```

```
# apt-get update
```

```
# apt-get install libreoffice
```

- ❖ Skype: Se instala desde el centro de software, simplemente se coloca Skype en el apartado de buscar se selecciona y da clic en el botón instalar.

Capítulo 3. Implementación

Una vez concluida la instalación de software y realizadas las configuraciones pertinentes de restricción a cada escritorio dependiendo del usuario y área al que esta pertenecerá, se ha obtenido la sesión del usuario final.

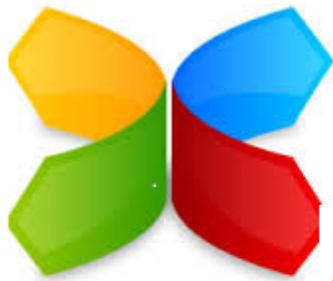
Con lo anterior se concluyó la instalación de software que los usuarios necesitan para poder laborar, es importante mencionar que la configuración de los escritorios es individual en cuanto a preferencias, si se desea algún software adicional o bien desinstalar alguno se debe ejecutar desde el servidor con un usuario con privilegios para dicha acción.

Una vez terminada la instalación simple de la cual se habló en el capítulo anterior se probó que dicha imagen cargue en varios clientes a la vez para ver que entregue correctamente las características aplicadas a esta.

Las pruebas fueron satisfactorias ya que las terminales ligeras cargaron sin problema y el inicio de sesión fue en fracción de segundos entre 5 y 10 para cargar el inicio de sesión de igual forma la carga del escritorio gráfico para cada usuario.

Los escritorios se configuraron de forma diferente quitándole propiedades como por ejemplo:

- ❖ Se dejó la vista básica de las aplicaciones del sistema
- ❖ Se quitó la vista de los escritorios dejando solo el que se da por default
- ❖ Se ocultó el disco duro del escritorio.



Capítulo 4

Configuraciones Adicionales de acceso

Capítulo 4. Configuraciones Adicionales de acceso

Una vez terminada la configuración básica del server LTSP se procedió a colocar algunas herramientas y arreglos en él para dar un mejor funcionamiento a este.

Algunas medidas de seguridad que se tomaran para el control de acceso al sistema son:

Manejo de Contraseñas

Las contraseñas de Linux utilizan el algoritmo de cifrado de IBM Data Encryption Standard (DES). Estas contraseñas son de longitud fija de 8 caracteres. Pero, siempre que sea posible es preferible utilizar contraseñas MD5. Ya que MD5 es un algoritmo hash que mejora a DES en los siguientes aspectos: las contraseñas son de longitud infinita, permiten a la inclusión de signos de puntuación y otros caracteres.

Las contraseñas se almacenan, en principio, en el archivo */etc/passwd* al cual se le establecerán los permisos 644, por seguridad ya que es necesario mantener la lectura sobre este archivo, se utilizan las *shadow passwords* y, en este caso, las contraseñas se almacenan en el archivo */etc/shadow* con permisos 600, o dicho de otra manera sin lectura para el grupo y los otros usuarios. De esta forma se impide que los usuarios normales puedan ver las contraseñas cifradas. El propietario de ambos archivos debe ser root.

Es importante indicar que las modificaciones o intentos de modificaciones de las contraseñas quedan registradas en el archivo */var/log/messages*. Como normas para la formación de una contraseña “segura” se puede decir que es conveniente seguir las siguientes reglas:

1. Abstenerse de utilizar nuestro nombre, apellidos o apodo.
2. Abstenerse de utilizar nombres de parientes o amigos.
3. Prescindir seleccionar una contraseña en la que se repita la misma letra o dígito.
4. Utilizar una contraseña con 8 o más dígitos.
5. Utilizar mezclas de letras mayúsculas y minúsculas.
6. Utilizar algún carácter no alfabético, como signos de puntuación.
7. Utilizar contraseñas fáciles de memorizar, y no escribirlas en sitio alguno.
8. Utilizar contraseñas que se puedan escribir rápidamente, por si alguien nos vigila.

Algunos casos de contraseñas a aplicar son:

- ❖ El acceso a la BIOS protegida con contraseña, con lo cual evitamos que usuarios curiosos tengan acceso para modificar parámetros del sistema, como la fecha y hora del sistema, secuencia de arranque, etc.
- ❖ Contraseña de inicio de sesión de cada usuario.
- ❖ Contraseñas para petición de uso de recursos (datos) en la red.

Restricción de acceso como root

Es importante señalar que en ocasiones el causante de los “desastres” en el sistema es el propio administrador. Es importante que cuando se realicen tareas de administración primero se conecte como un usuario normal y por un medio seguro donde la información viaje cifrada en caso de llevar a cabo la conexión remotamente. Es importante que la contraseña de root no viaje por la red en texto plano. Debe hacerlo de forma cifrada. Evitar el uso de órdenes *-r-* (*rlogin*, *rcp*, *rsh*,...) y utilizar las ordenes *SSH* o *SCP*, en las que la contraseña viaja encriptada.

Para tal caso, se pueden instalar herramientas tales como *SSH* o *PUTY* para dichas conexiones.

Ya que *SSH* (o *Secure SHell*) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y a diferencia de otros protocolos de comunicación remota tales como *FTP* o *Telnet*, *SSH* cifra la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas de nuestras conexiones, es el protocolo a implementar dentro de nuestro server.

Se puede utilizar la orden *sudo* para permitir a ciertos usuarios realizar tareas de administración. Para ello hay que especificar en el archivo de configuración */etc/sudoers* qué usuarios están permitidos y qué acciones pueden llevar a cabo. El sistema mantiene un registro de todas las actividades realizadas por esos usuarios autorizados.

En principio y como medida de seguridad, solo se debe poder acceder a la cuenta root desde la consola. Como ya se ha comentado, si se necesita hacer un acceso remoto a la cuenta root, entrar primero con cuenta de usuario y luego ejecutar el comando “*su*” para pasar a root. Estos intentos quedan registrados en el archivo de logs */var/log/messages*. De esta forma un posible atacante tendría que conocer el nombre de un usuario del sistema, conocer su clave y también conocer la clave del *root*, y añadiría dificultades para obtener privilegios remotos en el sistema.

Con lo cual sumaremos más puntos a la seguridad en el server *LTSP*.

Manejo de archivos

Los documentos de los usuarios se colocaron en un *HDD* adicional para así tener una mejor respuesta en tiempo con cada consulta de información ya que de esta manera no la trabajará el *HDD* del server haciendo que este sea consultado simplemente para peticiones de software con lo cual se ayuda a un mejor funcionamiento del mismo evitando una saturación de este por las diversas consultas de usuarios. Esto a su vez favorece administrativamente aislando la información y protegiéndola en el caso que el server llegara a tener algún fallo tanto en hardware como en software.

Es muy importante señalar que se creará un control de archivos y directorios entre las diferentes áreas de nuestra empresa con base en una estructura de permisos mediante usuarios y la creación

Capítulo 4. Configuraciones Adicionales de acceso

de grupos para con esto incrementar la seguridad en la información de cada uno de los usuarios y minimizar el mal uso de los recursos, pérdida o fuga de información entre usuarios de diferentes áreas.

En general, en un sistema LINUX se manejan dos conceptos de protección en archivos que son:

- ❖ Recursos: el conjunto de recursos está formado por todos los archivos del sistema.
- ❖ Dominio: será un usuario y los procesos que él ejecuta y que, por tanto, tengan el mismo UID efectivo.

Para controlar el acceso de los dominios a los recursos se utilizan las Listas de Control de Acceso por cada recurso. La lista de control de acceso (ACL) especifica qué dominios tienen acceso al recurso y qué operaciones asociadas al recurso pueden utilizar. El problema que plantea la lista de control de acceso es su tamaño variable, ya que depende del número de dominios que tengan acceso al recurso y de las operaciones que pueda realizar cada uno de ellos.

En Linux, para conseguir Listas de tamaño constante, se utilizan 2 técnicas:

1. Reducir el número de operaciones posibles sobre un recurso (archivo): podemos controlar 3 operaciones sobre los archivos, que son la lectura (r), escritura (w) y la ejecución (x).
2. Reducir el número de dominios que aparecen en la lista. Esto se consigue mediante el concepto de grupos de usuarios.

Todos los usuarios de un sistema Linux deben pertenecer, al menos, a un grupo. Existen 3 grupos o categorías en la relación entre un dominio (usuario) y un recurso (archivo):

- Propietario: indica quién creó el archivo
- Grupo del propietario: reúne a todos los usuarios que pertenecen al grupo del propietario.
- Resto de usuarios: los que no crearon el archivo y no pertenecen al grupo del propietario.

Con base en lo anterior mencionaremos los casos de acceso a datos y el medio para utilizarlos que se manejarán dentro de la empresa.

Caso 1. Usuarios pertenecientes al servidor LTSP

Se colocó en el escritorio del usuario un enlace a su carpeta personal utilizando el comando “ln” el cual permite hacer enlaces a un directorio de la manera en que deseemos para este caso simplemente colocando el atributo -s con el cual se crea el enlace simbólico a la carpeta que requiera el usuario. Es importante señalar que en los enlaces simbólicos si se borra o realiza alguna modificación en el nombre del archivo o directorio al cual está apuntado, tal enlace queda inservible.

Caso 2. Usuarios con sistema operativo Linux

En este caso se utilizará el servicio FTP para colocar los recursos necesarios a cada usuario, por lo cual, tanto en el server LTSP como en el cliente se debe instalar mediante consola con la indicación siguiente:

```
# apt-get install vsftpd
```

Una vez realizada la instalación se procede a la configuración del servicio por parte del server LTSP, que para este caso solo mencionaremos que debe tener la opción de usuario anónimo activada para poder compartir los recursos.

Con lo anterior ya dentro del cliente según la versión de Linux que este tenga, colocamos el recurso, para este caso se colocará en el escritorio del usuario simplemente colocando en consola la siguiente instrucción:

```
#sftp://IP_del_server/ruta/del/recurso
```

Con lo cual se termina la configuración de dicho acceso mediante un cliente con sistema operativo nativo Linux el cual mostrará el directorio como se ve en la imagen (Fig.19) siguiente:

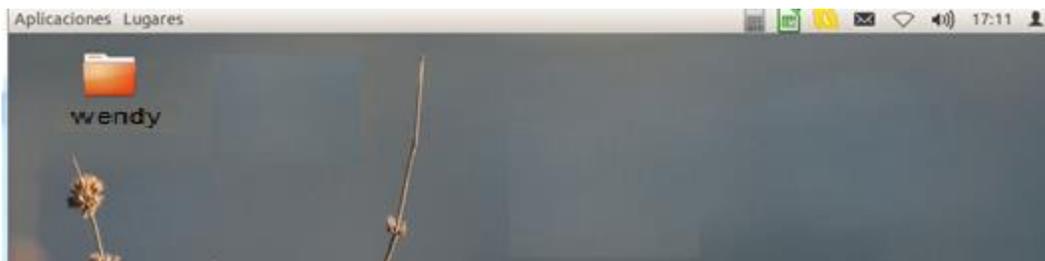


Fig. 19 Muestra de directorio en escritorio Ubuntu.

Caso 3. Usuarios con sistema operativo Windows

El servicio que se utiliza para tal caso es Samba el cual se instalará en el servidor LTSP siguiendo los pasos a continuación.

1. Instalación del paquete samba ejecutando en línea de comandos:

```
#apt-get install samba
```

Capítulo 4. Configuraciones Adicionales de acceso

2. Una vez instalado se llevará a cabo la configuración de este servicio no sin antes tener definidos los usuarios que harán uso de este servicio, para fines ilustrativos se colocará el ejemplo de un recurso compartido mediante este servicio.

Para definir un recurso a compartir se entra al archivo de configuración de samba.

```
# /etc/samba/smb.conf
```

En el cual se posiciona en la parte para agregar directorios y procede a crear los directorios necesarios colocando las líneas que se muestra a continuación para cada uno de ellos.

[Logística]

Comment = Comentario de la carpeta, de ser necesario

Path = /ruta/del/directorio/a_compartir

Browseable = yes

Writable = yes

Valid users = usuarios validos

3. Creación de usuarios Samba.

Para dicha creación basta con colocar en consola la siguiente instrucción.

```
# pdbedit -a nombre_del_usuario_nuevo
```

Nota. Es muy importante recordar que los usuarios que se crearán en samba ya deben existir como usuarios UNIX en el servidor LTSP.

4. Una vez hecho lo anterior dentro del server LTSP (habiendo definido los permisos necesarios para cada directorio y su contenido), se procederá a colocar la carpeta como un recurso de red en el host requerido.

Se procede a colocar el recurso compartido dentro de la sesión del usuario Windows mediante los siguientes pasos:

- ❖ Clic en “inicio”
- ❖ Dar clic derecho sobre la opción “Equipo” y seleccionar del listado “Conectar unidad de red”
- ❖ Se deben colocar los datos correspondientes a la carpeta a la cual se tendrá acceso y dar clic en aceptar.

La conexión exitosa se verá como muestra la siguiente imagen (Fig. 20):

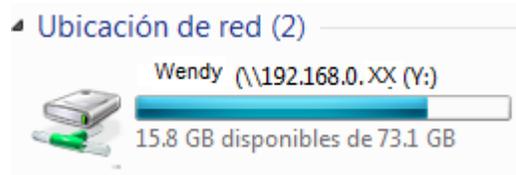


Fig. 20 Unidad de red en S.O Windows.

Configuración del servidor DHCP

Como ya se comentó este servicio es de suma importancia para la conexión de nuestros clientes, por tal motivo es muy conveniente configurarlo de tal forma que aparte de dar una mayor respuesta a la hora de otorgar una IP a los clientes para que brinde un servicio de mayor seguridad ya que la configuración estará basada en la MAC de las terminales ligeras con lo cual evitaremos brindar servicios de red a usuarios no autorizados.

Para tal caso se agrega la siguiente configuración en el servicio DHCP:

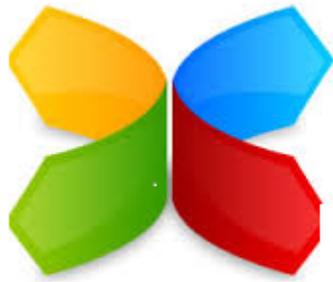
- ❖ Abrimos el archivo de configuración

```
# vi /etc/ltsp/dchpd.conf
```

- ❖ Se colocan las siguientes líneas por cada uno de los clientes de la siguiente forma.

```
host Wendy{  
  
    hardware ethernet 46:87:f8:0f:29:d0;  
  
    fixed-address 192.168.0.xx;  
  
}
```

Con esta simple configuración mediante MAC cerramos el servicio de la red para cualquier usuario no registrado previamente dentro del servidor DHCP y evitamos intrusos o conexiones no autorizadas dentro de la LAN.



Conclusiones



Conclusiones

En este trabajo profesional se presentó la implementación de un servidor LTSP el cual fue mostrando sus múltiples beneficios a lo largo del desarrollo de este proyecto. Así bien para concluir de manera asertiva, se mostrarán los puntos más importantes de dicho trabajo a continuación.

Podemos mencionar que un servidor LTSP tiene bastantes beneficios, comenzaremos mencionando algunos por parte del gran ahorro monetario que nos suma al tenerlo trabajando en una empresa mediana como en este caso.

❖ Costo Beneficio

Tenemos una reducción anual de costos por licencias de software las cuales pueden variar en precio y funcionabilidad de tiempo, ya que con el servidor LTSP el software a utilizar es libre. A continuación se muestra un pequeño listado de software donde se emplea dicho ahorro.

- 1.- Sistema Operativo Windows sustituido en el server LTSP por Ubuntu Server software libre.
- 2.- Paquetería Microsoft Office sustituido en el server LTSP por Open Office software libre.
- 3.- Antivirus, actualmente no se requiere dicho software a base del funcionamiento del sistema operativo empleado.

También es notable la reducción de costo del hardware por usar terminales ligeras las cuales se observó crean un ahorro del 83% a diferencia de las PC normales.

La estructura permite cambios de bajo impacto económico debido a que el performance deseado para servir a los clientes es muy bajo en comparación con otros servicios por ejemplo terminal server de Windows el cual requiere una amplia capacidad de recursos y su constante actualización.

❖ Control y Seguridad

Dentro de este marco podemos mencionar que mediante el servidor LTSP se proporciona a los usuarios las siguientes características.

- 1.- Sesiones de clientes por túnel cifrado y encriptado desde la autenticación por SSH seguro.
- 2.- Toda aplicación está monitorizada y centralizada en el servidor LTSP.
- 3.- Gestión de recursos por cliente.
- 4.- Administración de permisos y políticas centralizadas en el servidor.

Conclusiones

6.- Gestión y centralización de recursos de impresión, lo cual no se comentó en este trabajo pero es posible.

7.- Optimización de memoria principal (RAM).

9.- Mitigación en un 90% de fuga de información sensible con base en los controles por permisos.

10.- Cada servicio ofrecido está enjaulado y totalmente restringido a acceso a partes sensibles del sistema.

11.- Al tener una asignación de IP's por reconocimiento de MAC se garantiza por hardware que el cliente ligero es quien está dado de alta y se evitan intrusos a la red.

12.- Al tener un servicio centralizado y soportando toda la carga de procesamiento el sistema LTSP proporciona mecanismos que permiten entregar los recursos únicamente necesarios para satisfacer la carga del servicio.

Con todos los puntos mencionados anteriormente podemos concluir que se cumplieron los objetivos de nuestro proyecto al brindar al usuario final un sistema actualizado, seguro y centralizado el cual nos permitió homogenizar los datos dentro de este para tener un mayor control sobre estos tanto en uso como en respaldo. No queda de más mencionar que el trabajo mostrado representa solo una parte mínima del gran poder que tiene un servidor LTSP en su manejo de datos, seguridad y gestión.

Así como también concluir que el desempeño que este tiene es óptimo dentro del área empresarial ya que cuenta con una variedad de recursos para poder satisfacer las necesidades de cualquier usuario de manera eficaz y segura lo cual es de suma importancia en la actualidad para satisfacer las necesidades que crecen día a día a base de la actualización de servicios con los que se debe contar en una empresa para dar satisfacción a sus empleados para con ello poder proporcionar un servicio de calidad a sus clientes.



GLOSARIO



GLOSARIO

ASI: Simplemente son las siglas de Auxiliar de Sistemas de la Información.

ASPEL: Es una empresa 100% mexicana y líder en el mercado de software administrativo que desarrolla y comercializa sistemas de cómputo y servicios relacionados que automatizan la administración de las micro, pequeñas y medianas empresas favoreciendo la correcta toma de decisiones, simplificando sus actividades administrativas e integrándolas fácilmente a la era digital. Aspel actualmente cuenta con más de 500,000 empresas usuarias en México y Latinoamérica.

ACK: Un *ACK* (del inglés *acknowledgement*, en español acuse de recibo o asentimiento), en comunicaciones entre computadores, es un mensaje que el destino de la comunicación envía al origen de ésta para confirmar la recepción de un mensaje.

BIOS: El Basic Input/Output System, es un software que es instalado dentro de la PC, y es el primer programa que se ejecuta cuando se enciende la computadora. El propósito fundamental del BIOS es inicializar y probar el hardware del sistema y cargar un bootloader o un sistema operativo de un dispositivo de almacenamiento de datos.

Broadcast: Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

CPU: Sigla de la expresión inglesa *central processing unit*, 'unidad central de proceso', que es la parte de una computadora en la que se encuentran los elementos que sirven para procesar datos.

DES: Data Encryption Standard (DES) es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como un estándar FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo.

DHCP: Sus siglas en inglés de Dynamic Host Configuration Protocol, en español «protocolo de configuración dinámica de *host*» es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

DVR: Un grabador de vídeo digital, es un dispositivo interactivo de grabación de televisión y vídeo en formato digital. Un DVR se compone, por una parte, del hardware, que consiste principalmente en un disco duro de gran capacidad, un microprocesador y los buses de comunicación; y por otra, del software, que proporciona diversas funcionalidades para el

Glosario

tratamiento de las secuencias de vídeo recibidas, acceso a guías de programación y búsqueda avanzada de contenidos.

FTP: File Transfer Protocol, este protocolo de red llamado Protocolo de Transferencia de Archivos es como su nombre lo indica una de las formas en la cual podemos enviar archivos hacia una Red TCP (siglas en inglés de Transmission Control Protocol) en la que utilizaremos la clásica arquitectura de Cliente - Servidor para dicha transferencia.

GNOME: Es un entorno de escritorio totalmente libre, atractivo y fácil de utilizar para sistemas UNIX, con aplicaciones para cumplir con todos los requerimientos de la computación moderna.

HDD: En informática, la unidad de disco duro o unidad de disco rígido (en inglés: *Hard Disk Drive*, *HDD*) es el dispositivo de almacenamiento de datos que emplea un sistema de grabación magnética para almacenar datos digitales. Se compone de uno o más platos o discos rígidos, unidos por un mismo eje que gira a gran velocidad dentro de una caja metálica sellada. Sobre cada plato, y en cada una de sus caras, se sitúa un cabezal de lectura/escritura que flota sobre una delgada lámina de aire generada por la rotación de los discos.

ISP: Un proveedor de servicios de Internet (ISP) es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cable módem, GSM, Dial-up.

KDE: Es una comunidad internacional que desarrolla software libre. Produce un entorno de escritorio, multitud de aplicaciones e infraestructura de desarrollo para diversos sistemas operativos como GNU/Linux, Mac OS X, Windows, etc.

LAN: Son las siglas de *Local Area Network*, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

LTSP: Linux Terminal Server Project. Paquete de aplicaciones para distribuciones basadas en GNU-Linux que permite a varios usuarios, utilizar las capacidades funcionales de un servidor en la red por medio de terminales de recursos mínimos y de forma simultánea.

MAC: En las redes de computadoras, la dirección MAC (siglas en inglés de *media access control*; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

Multicast: Significa comunicación entre un solo emisor y múltiples receptores dentro de una red. Los usos típicos incluyen la actualización de personal móvil desde una oficina central y el manejo periódico del correo electrónico. Multicast es soportado por redes de datos inalámbricas como parte de la tecnología de paquetes de datos Digitales Celulares (CDPD).

Glosario

MD5: En criptografía, MD5 (Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

OpenERP: es un completo sistema de gestión empresarial (ERP) de código abierto que cubre las necesidades de las áreas de contabilidad, finanzas, ventas, RRHH, compras, proyectos y almacén entre otras. OpenERP, la herramienta de gestión empresarial más potente, se encuentra ahora a su alcance.

OpenVPN: Es una solución de conectividad basada en software libre. Es una solución multiplataforma que ha simplificado la configuración de VPN's frente a otras soluciones más antiguas y difíciles de configurar como IPsec y haciéndola más accesible para gente inexperta en este tipo de tecnología.

PUTY: Es un emulador gratuito de terminal que soporta SSH y muchos otros protocolos. La mayoría de usuarios, especialmente los que trabajan sobre sistemas operativos Windows, lo encuentran muy útil a la hora de conectar a un servidor Unix o Linux a través de SSH.

PXE: Entorno de ejecución de pre-arranque, es un entorno para arrancar e instalar el sistema operativo en ordenadores a través de una red, de manera independiente de los dispositivos de almacenamiento de datos disponibles (como discos duros) o de los sistemas operativos instalados.

Python: Se trata de un lenguaje de programación multiparadigma, ya que soporta orientación a objetos, programación imperativa y, en menor medida, programación funcional. Es un lenguaje interpretado, usa tipado dinámico y es multiplataforma.

Rhythmbox: Es un reproductor de audio que reproduce y ayuda a organizar la música digital. Fue originalmente inspirado por el reproductor de Apple, iTunes. Es software libre, diseñado para trabajar bien bajo el escritorio GNOME y muchos otros.

SCP: Secure Copy Medio de transferencia segura de archivos informáticos entre un servidor local y otro remoto, o entre dos servidores remotos, usando SSH (protocolo Secure Shell).

S.O.: singlas que abrevian la palabra sistema operativo.

SSH: Secure *S*hell es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

TCP: El Protocolo de Control de Transmisión (TCP) permite a dos anfitriones establecer una conexión e intercambiar datos. El TCP garantiza la entrega de datos, es decir, que los datos no se pierdan durante la transmisión y también garantiza que los paquetes sean entregados en el mismo orden en el cual fueron enviados.

Glosario

Telnet: TELEcommunication NETwork es el nombre de un protocolo de red que nos permite viajar a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

UDP: User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción.

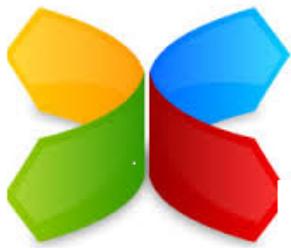
UID: En sistemas tipo Unix, los usuarios son representados por un identificador de usuario, normalmente abreviado como UID o User ID.

Unicast: Es comunicación entre un solo emisor y un solo receptor sobre un ambiente de red. Un término más antiguo conocido como comunicación punto a punto, es similar en significado a unicast. Ejemplos básicos de aplicaciones unicast son los protocolos HTTP, SMTP, FTP o Telnet. Actualmente es la forma predominante de transmisión en Internet.

Unity: Es un interfaz de usuario creada para el entorno de escritorio GNOME, y desarrollado por Canonical para la distribución de Ubuntu.

VPN: Una red privada virtual (VPN) construida dentro de una infraestructura de red pública, como por ejemplo Internet. Las empresas pueden usar una red VPN para conectar de manera segura oficinas y usuarios remotos por medio de un acceso a Internet económico suministrado por un tercero, en lugar de a través de enlaces WAN dedicados o enlaces de acceso telefónico de larga distancia.

XFCE: Es un entorno de escritorio bastante ligero y muy completo, especialmente orientado para ser utilizado por equipos de bajos recursos, ya que consume muy poca memoria RAM. Es un entorno de escritorio diseñado para ser utilizado en sistemas operativos Linux, Solaris y BSD, así como sus derivados.



Referencias Electrónicas

Referencias Electrónicas

- 1. Capítulo 1. Generalidades Estructurales de un Servidor LTSP, subtemas “Protocolo PXE” y “Funcionamiento del protocolo PXE”.**
(Última revisión 22-Noviembre-2014)
http://es.wikipedia.org/wiki/Preboot_Execution_Environment
- 2. Capítulo 2. Requerimientos del Proyecto, subtema “A nivel de costos”.**
(Última revisión 22-Noviembre-2014)
<http://www.chippe.com>
- 3. Capítulo 2. Requerimientos del Proyecto, subtema “A nivel de costos”.**
(Última revisión 22-Noviembre-2014)
<http://www.cisco.com>
- 4. Capítulo 2. Requerimientos del Proyecto, subtema “A nivel de costos”.**
(Última revisión 04-Marzo-2015)
<http://es.wikipedia.org/wiki/ACK>
- 5. Capítulo 3. Implementación, subtema “Selección de software”.**
(Última revisión 21-Noviembre-2014)
<https://es.opensuse.org/>
- 6. Capítulo 4. Configuraciones Adicionales de acceso, subtemas “Manejo de contraseñas”, “Restricción de acceso como usuario root” y “Manejo de archivos”.**
(Última revisión 17-Noviembre-2014)
<http://recursostic.educacion.es/observatorio/web/ca/software/software-general/562-elvira-misfud>
- 7. Introducción.**
(Última revisión 22-Noviembre-2014)
<http://es.wikipedia.org/wiki/OpenVPN>
- 8. Introducción.**
(Última revisión 22-Noviembre-2014)
<http://openerpspain.com/>
- 9. Se utilizó a lo largo de todo el documento.**
(Última revisión 25-Noviembre-2014)
<http://www.ltsp.org>
- 10. Se utilizó a lo largo de todo el documento.**
(Última revisión 25-Noviembre-2014)
<http://www.ubuntu.com/>