
Universidad Nacional Autónoma de Nicaragua – León
Facultad de Ciencias y Tecnologías



Título

Propuesta para la Unificación de las Cuentas de Acceso de Docentes y Estudiantes a los Servicios de Red que ofrece la UNAN – León.

Tesis para optar al título de Ingeniero en Sistemas de Información

Autor:

Br. Ervin Antonio Gutiérrez Santana

Tutor:

 MSC. Aldo Rene Martínez

León, 18 de abril de 2013

Dedicatoria

A

Dios.

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A

mi

madre

Eva.

Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A mis familiares.

A mi hermana Ana Gutiérrez quien me ha apoyado incondicionalmente en todo momento, a mi primo Jimmy Centeno por ser el ejemplo de un hermano mayor y del cual aprendí aciertos y de momentos difíciles; a mi Primo Miguel García, a mis Primas María José Centeno y María Marcela Centeno y a todos aquellos que participaron directa o indirectamente en la elaboración de esta tesis. ¡Gracias a ustedes!

A

mis

maestros.

MSC. Aldo Martínez por su gran apoyo y motivación para la culminación de nuestros estudios profesionales y para la elaboración de esta tesis; al MSC. Denis Espinoza por su apoyo ofrecido en este trabajo por su tiempo compartido y por impulsar el desarrollo de nuestra formación profesional.

A

mis

amigos.

Que me apoyaron incondicional y mutuamente en mi formación profesional y que hasta ahora, seguimos siendo amigos: Lic. Walter Soza, Lic. Carlos Mairena, Gerson González, Eddy Ruiz, Sandra Centeno haberme ayudado a realizar este trabajo.

Índice

Propuesta para la Unificación de las Cuentas de Acceso de Docentes y Estudiantes a los Servicios de Red que ofrece la UNAN – León.....	1
Dedicatoria	2
Índice de figuras	7
Titulo.....	9
Antecedentes.....	10
Planteamiento del problema.....	11
Justificación	12
Objetivos.....	13
Objetivos Generales.....	13
Objetivos específicos	13
Diseño Metodológico	14
Modelo de desarrollo del sistema	14
Actividades a desarrollar	14
1. Recopilación de información	14
2. Estudio de Viabilidad	15
3. Diseño del Sistema.....	15
4. Desarrollo del Sistema	15
Cronograma de actividades	16
Situación actual de los Servicios de Red de la UNAN - León	17
¿Qué servicios de red ofrece la UNAN-León y que mecanismos utiliza cada uno de ellos para la autenticación?	17
Labores de mantenimiento.....	18
Marco Teórico.....	19
Tecnologías Utilizadas.....	19
Aplicaciones Web	19
Servidor	19

Red Inalámbrica (WIFI).....	20
Moodle	20
Videoconferencia	20
Freeradius.....	20
Certificado Digital.....	20
LDAP	21
Estudio de Viabilidad	22
Situación Actual	22
Alternativas de Solución	22
Elección de la solución a implementar	24
OpenLDAP	24
Características de OpenLDAP:.....	24
Razones para elegir OpenLDAP	24
Costo de OpenLDAP	25
Las características propias de un servidor LDAP son:.....	25
Funcionamiento de LDAP	25
Ventajas en el uso de LDAP.....	25
Usos empresariales	26
Diseño del Sistema	27
Configuraciones del Servidor	27
Requisitos Mínimos para instalación	27
Software a Utilizar.....	27
Apache versión 2.2.22, Asterisk versión 11.2.1, OpenLDAP versión 2.4.28- 1.1ubuntu4.2, Vsftpd versión 2.3.5-1ubuntu2, Postfix versión 2.9.6, Dovecot versión 2.0.19, Pfsense versión 2.0.2-RELEASE-i386, Freeradius versión 2.1.12_1.	27
Asterisk:.....	27
Phpldapadmin:	27
Vsftpd:	27
Postfix:.....	27
Dovecot:	27

Squirrelmail:	27
Portal Cautivo:.....	28
Pfsense	28
Desarrollo del Sistema.....	29
Instalación de Ubuntu Desktop 12.04	29
Instalación de OpenLDAP SERVER en Ubuntu Desktop 12.04	30
Instalación de Central Telefónica Asterisk versión 11 y Autenticación con LDAP.....	33
Instalación de Moodle 2.4.2 y Autenticación LDAP.....	37
Instalación del Servidor de Correo y Autenticación LDAP	40
Instalación de VSFTPD y Autenticación LDAP	47
Instalación del Portal Cautivo en Máquina Virtual	49
Configuración del Servidor Freeradius para Autenticar contra LDAP.....	50
Activación y Configuración del Portal Cautivo en Red Local.....	51
Conclusiones.....	53
Recomendaciones.....	54
Referencias Bibliográficas.....	55
Instalación y Configuración del Servidor Ubuntu 12.04	55
Instalación y Configuración del Servidor OpenLdap.....	55
https://help.ubuntu.com/12.04/serverguide/openldap-server.html	55
https://help.ubuntu.com/12.04/serverguide/openldap-server.html	55
https://help.ubuntu.com/community/LDAPClientAuthentication	55
Instalación y Configuración del Servidor Asterisk	55
http://www.tribulinux.com/como-instalar-asterisk-10-en-ubuntu-12-04.html	55
http://www.asteriskdocs.org/en/3rd_Edition/asterisk-book-htmlhunk/ExternalServices_id291590.html	55
http://www.esdebian.org/wiki/realtime-ldap-asterisk-16	55
Instalación y Configuración del Servidor Moodle.....	55
http://echaleunvistazo.wordpress.com/2012/09/20/servidor-web-con-moodle-instalacion/	55
http://docs.moodle.org/24/en/LDAP_authentication	55

Instalación y Configuración del Servidor Correo	55
http://pedroreina.net/recetas/squirrelmail.html	55
http://wiki.dovecot.org/HowTo/DovecotOpenLdap	55
https://help.ubuntu.com/community/Dovecot?highlight=%28%28DovecotLDAP%29%29	55
https://help.ubuntu.com/12.04/serverguide/postfix.html#postfix-smtp-authentication	55
Instalación y Configuración del Servidor VSFTPD	55
http://linux-ubuntu1104.blogspot.com/2012/02/ubuntuvsftp-con-autenticacion-local-y.html	55
Instalación y Configuración de Portal Cautivo	55
http://www.youtube.com/watch?v=B6Hjxd1Af-s	55
Anexos	56
Estructura LDAP código implementado:	56
Diseño de la Estructura de Red a Utilizar en el Proyecto	58
Configuración de Softphone para uso como extensión VoIP	58
Configuración de Cliente de Correo Electrónico para envío y recepción de correos ...	59
Diseño de Página Index.html	61

Índice de figuras

FIGURA 1. PROCESO ITERATIVO.....	14
FIGURA 2. CRONOGRAMA DE ACTIVIDADES	16
FIGURA 3. ESTRUCTURA GENERAL	30
FIGURA 4. ACTIVACIÓN DE PERFIL PAM CONTRA LDAP	31
FIGURA 5. EXPORTACIÓN DE USUARIOS LDAP	32
FIGURA 6. EXPORTACIÓN DE GRUPOS DE LDAP	32
FIGURA 7. PRIMERA VERIFICACIÓN DE FUNCIONALIDAD DE LDAP.....	32
FIGURA 8. SEGUNDA VERIFICACIÓN DE FUNCIONALIDAD DE LDAP.....	32
FIGURA 9. ACTIVACIÓN DE FICHEROS DE SONIDOS Y MÓDULOS EXTRAS	34
FIGURA 10. VERIFICACIÓN DE MÓDULO LDAP CARGADO EN ASTERISK.....	36
FIGURA 11. VERIFICACIÓN DE FUNCIONALIDAD DE LDAP CON ASTERISK	36
FIGURA 12. CÓDIGO DE CONFIGURACIÓN DE MOODLE.....	38
FIGURA 13. PÁGINA PRINCIPAL DEL ADMINISTRADOR.....	39
FIGURA 14. ASIGNACIÓN DE CORREO LOCAL	40
FIGURA 15. ASIGNACIÓN DE NOMBRE DEL CORREO	40
FIGURA 16. CONFIGURACIÓN DE RECIPIENTE DE CORREO.....	40
FIGURA 17. ASIGNACIÓN DE DOMINIOS DE CORREO	41
FIGURA 18. MODO DE ACTUALIZACIÓN DE CORREO.....	41
FIGURA 19. ASIGNACIÓN DE REDES DE ACCESO DEL CORREO	41
FIGURA 20. CONFIGURACIÓN DEL MODO DE ENTREGA DEL CORREO	41
FIGURA 21. ASIGNACIÓN DEL TAMAÑO DEL BUZÓN DE CORREO	41
FIGURA 22. ESTABLECIMIENTO DE PROTOCOLO A UTILIZAR.....	42
FIGURA 23. PRUEBA DE FUNCIONAMIENTO DE SERVICIO SMTP	43
FIGURA 24. COMPROBACIÓN DEL FUNCIONAMIENTO DEL SERVICIO POP3	44
FIGURA 25. COMPROBACIÓN DEL FUNCIONAMIENTO DEL SERVICIO IMAP	44
FIGURA 26. CONFIGURACIÓN DEL NOMBRE DE LA ORGANIZACIÓN EN SQUIRRELMAIL	44
FIGURA 27. ASIGNACIÓN DEL DOMINIO DEL SERVIDOR DE CORREO.....	45
FIGURA 28. SELECCIÓN DEL SERVIDOR IMAP A UTILIZAR	45
FIGURA 29. COMPROBACIÓN DEL WEBMAIL EN EL DOMINIO PREESTABLECIDO	45
FIGURA 30. COMPROBACIÓN DE FUNCIONAMIENTO DE SQUIRRELMAIL.....	46
FIGURA 31. VERIFICACIÓN DE FUNCIONALIDAD DE FTP CON LDAP DESDE CONSOLA.....	47
FIGURA 32. VERIFICACIÓN DE FUNCIONAMIENTO DE FTP CON LDAP DESDE EL NAVEGADOR.....	48
FIGURA 33. COMPROBACIÓN DE ACCESO A LOS ARCHIVOS DEL USUARIO MEDIANTE FTP	48
FIGURA 34. ACCESO AL PORTAL CAUTIVO DESDE EL NAVEGADOR	49
FIGURA 35. COMPROBACIÓN DE PAQUETES INSTALADOS	49
FIGURA 36. ACTIVACIÓN DEL REGISTRO DHCP	49
FIGURA 37. CONFIGURACIÓN DEL SERVIDOR DHCP EN RED LAN	49
FIGURA 38. CONFIGURACIÓN DE FREERADIUS CONTRA LDAP	50
FIGURA 39. HABILITACIÓN DE INTERFACES	50
FIGURA 40. HABILITACIÓN DE CLIENTE GENÉRICO PARA FREERADIUS	51
FIGURA 41. HABILITACIÓN DE USUARIO GENÉRICO PARA FREERADIUS	51
FIGURA 42. HABILITACIÓN DEL PORTAL CAUTIVO	51
FIGURA 43. AUTENTICAR PORTAL CAUTIVO CON EL SERVIDOR RADIUS	51
FIGURA 44. ACTIVAR EL ENVÍO DE PAQUETES RADIUS PARA CONTABILIDAD DE USUARIOS.....	51
FIGURA 45. SELECCIÓN DE RED DONDE SE EJECUTA EL SERVIDOR RADIUS	51
FIGURA 46. COMPROBACIÓN DE SERVICIOS ACTIVOS	52

FIGURA 47. COMPROBACIÓN DE FUNCIONAMIENTO DEL PORTAL CAUTIVO DESDE MÁQUINA CLIENTE.....	52
FIGURA 48. ACCESO DE USUARIO LDAP AL PORTAL CAUTIVO.....	52
FIGURA 49. ESQUEMA LDAP	56
FIGURA 50. EJEMPLO DE INFRAESTRUCTURA DE RED UTILIZADA.....	58
FIGURA 51. INTERCAMBIO DE MENSAJES	58
FIGURA 52. INGRESO DE LOS DATOS DEL CLIENTE.....	58
FIGURA 53. REGISTRO DE LA EXTENSIÓN VOIP	59
FIGURA 54. CONFIGURACIÓN DEL NOMBRE DEL USUARIO	59
FIGURA 55. INGRESO DE LA DIRECCIÓN DE CORREO DEL USUARIO	59
FIGURA 56. INGRESO DE LOS DATOS DEL SERVIDOR DE CORREO	60
FIGURA 57. COMPROBACIÓN DE FUNCIONALIDAD DEL CLIENTE DE CORREO	60
FIGURA 58. PÁGINA INDEX.HTML	64

Título

“Propuesta para la unificación de las cuentas de acceso de docentes y estudiantes a los servicios de red que ofrece la UNAN – León”

Antecedentes

A partir del año 2007 se implementó por primera vez el sistema de red inalámbrica WIFI de libre acceso en la UNAN-León, en los siguientes 2 años se han venido efectuando y estableciendo políticas de uso para la misma, actualmente se han implementado varios servicios de red que son facilitados a toda la comunidad universitaria como una forma rápida, eficiente y segura de comunicarse y realizar investigaciones. Para hacer uso de estos servicios los docentes usan equipos portátiles y computadores de mesa que ellos tienen asignados en sus respectivas oficinas, mientras que la mayoría de los estudiantes utilizan sus equipos portátiles o de la universidad (Laboratorios y/o Bibliotecas).

Los servicios ofrecidos por esta institución son: Servidores web, sistema de correo MicrosoftLive@edu (la UNAN-León es la primera universidad en implementar este sistema a nivel nacional), plataforma de aula virtual (Moodle), servicio de registro académico (SIGACAD), servicio contable (UXIEC, este servicio solo es para el personal administrativo que se encarga de gastos y entradas generadas por la institución, por ejemplo el salario del personal y matriculas), videoconferencia, red inalámbrica (WIFI) y el servicio de llamadas de voz sobre IP.

En este mundo interconectado donde el acceso a redes de comunicaciones e Internet está ampliamente extendido, la Web se ha convertido en una plataforma casi universal para proporcionar el acceso a todo tipo de servicios. Razón por la cual la UNAN-León tiene como prioridad principal el servicio de red inalámbrica el cual les permitirá una vez autenticado acceder a los demás servicios.

Grandes instituciones como la universidad de Córdoba y la universidad Oberta de Cataluña en España, utilizan la centralización de cuentas de usuario donde un usuario hace uso de una única cuenta para acceder a los diferentes servicios ofrecidos por su centro ya sea dentro o fuera de la institución, todo esto con ayuda de un servidor de directorios LDAP para la autenticación.

La UNAN-León tiene implementado en su sistema un directorio LDAP con servidor FREERADIUS que no es empleado en todos los servicios por lo que este trabajo propone la utilización de esta misma metodología para todas las aplicaciones de la red. De esta manera, es posible especificar un único método de autenticación de usuarios para las diferentes aplicaciones y no lo que es común, que las aplicaciones definan sus usuarios de acuerdo a los usuarios del sistema sobre el cual está ejecutándose la aplicación.

En este momento existe un servidor de certificados digitales en nuestra universidad pero es necesario asignar a cada usuario un certificado y publicarlo en un servidor LDAP, para que estos puedan ser accedidos desde cualquier aplicación que los necesite. Estos servicios como SIGACAD necesitan acceder a un servidor LDAP. Otras aplicaciones como la inscripción de asignaturas, las consultas de notas y la modificación de la carga académica de docentes hacen uso de esta.

Gracias a la utilización de estos certificados, es posible autenticar a los usuarios en el momento en que éstos solicitan llevar a cabo una determinada operación evitando así que impostores puedan realizar operaciones que no les están permitidos realizar.

Por último, el uso de directorios LDAP a lo largo del mundo es una tendencia dentro de las tecnologías de información. Las organizaciones están invirtiendo en mantener su información en directorios pues es cómodo su acceso desde una gran variedad de aplicaciones en diversas plataformas. El cambio temprano a esta tendencia es una ventaja significativa en el uso de las tecnologías actuales de información.

Planteamiento del problema

Los docentes y estudiantes que utilizan la red de la UNAN-León hacen uso a diario de diversos servicios que esta institución ofrece, entre los cuales podemos mencionar: correo electrónico, llamadas por IP (VoIP), aulas virtuales (Moodle), transferencias de archivo (FTP), red inalámbrica (WIFI), sistema de gestión académica (SIGACAD) y videoconferencia. Muchos de estos usuarios muestran gran inconformidad con los servicios debido a que para cada uno deben de utilizar cuentas diferentes, razón por la cual muy pocos los utilizan y se ven forzados a emplear otras soluciones disponibles en internet (Google, Yahoo, Skype) en vez de las ofertadas por la UNAN - León.

Al no utilizar una misma cuenta para acceder a los diferentes servicios, la unidad de servicios de red de la UNAN-León se ve en la necesidad de crear una cuenta para cada uno de ellos cada vez que un usuario quiere ser dado de alta, por ejemplo:

Si un docente necesita acceder a cualquier servicio de red que ofrece la UNAN-León, este deberá registrarse en cada uno de los servicios, esto es debido a la política de autenticación y gestión de cuentas de usuarios tal es el caso, que se necesitan cuentas independientes para: el correo electrónico, VoIP, aula virtual, red inalámbrica y biblioteca virtual; lo cual resulta muy tedioso para algunos memorizarlo y hacer uso de estos con frecuencia. Similar situación sucede con los estudiantes cuando quieren acceder a estos servicios, en este caso tanto el correo, aula virtual, red inalámbrica y SIGACAD utilizan cuentas de acceso diferentes.

El problema de necesitar varias cuentas para acceder a los diferentes servicios que ofrece la UNAN-León, conlleva a tener redundancia de información de los usuarios debido que para cada servicio ofrecido por esta institución se crean cuentas en bases de datos diferentes por ejemplo podemos mencionar que: para crear una cuenta de correo a un determinado usuario esta se guarda en un sistema gestor de base de datos MySQL y para crear una cuenta de red inalámbrica para el mismo usuario, esta se almacena en un sistema PostgreSQL, con este mecanismo que se está utilizando reúne la misma información del usuario para servicios diferentes.

Basándonos en estas dificultades pretendemos realizar una propuesta de unificación de cuentas de usuario para el acceso a los diferentes servicios de red que ofrece la UNAN-León. De esta situación surgen las siguientes dudas:

¿Cómo se puede hacer para unificar las cuentas de acceso a los servicios de la UNAN-León?

¿Qué servicios de red ofrece la UNAN-León y que mecanismos utiliza cada uno de ellos para la autenticación?

¿Qué tecnología se puede utilizar para permitir la centralización de las cuentas de usuarios para el acceso a los servicios de la UNAN-León?

¿Qué ventajas ofrece la unificación de las cuentas de usuario frente al modelo de trabajo actual?

Justificación

Con esta propuesta pretendemos demostrar que mediante la unificación de los servicios de las cuentas de usuario de la UNAN-León, se pueden eliminar muchas de las problemáticas que los servicios ofrecen logrando así poder hacer uso de ellos con una única cuenta de modo seguro y estable. Con esta implementación se lograra lo siguiente:

- Los usuarios tendrán la facilidad de acceder a los servicios de red que ofrece la UNAN-León a través de un único usuario y clave. Esto facilitará y promoverá su uso pues no será necesario el manejar varias cuentas (una por servicio), sino que bastará con una sola que será la que le dé acceso a la gama de servicios de red de la UNAN-León.
- El unificar las cuentas permitirá reducir la redundancia de información de los datos de los usuarios, debido a que por cada aplicación hay una cuenta para un mismo usuario, en este caso se podría dejar o establecer una única base de datos que reúna todas las características apropiadas para archivar la información de los usuarios y así evitar que varios SGBD almacenen los mismos datos.
- Aminorar el uso de recursos del servidor, al tener un único servicio para la autenticación y gestión de cuentas y no como se encuentra en este momento donde cada servicio emplea sus propios mecanismos de autenticación, se podría implementar una política de autenticación que permita mostrar al usuario una vez registrado, los servicios a los cuales tiene acceso y hacer uso de ellos.
- Mayor sencillez a la hora de dar de alta a un usuario en los servicios de la red de la UNAN-León, ya que la información se encontraría en un único directorio y cuando un usuario solicite un servicio ya sea por la web de la UNAN-León o en las oficinas de la unidad de redes y comunicaciones, este solo verificaría los datos en el sistema y se le daría de alta al servicio solicitado.

En definitiva con esta propuesta tanto los docentes como estudiantes de la institución harían un mayor uso de los servicios que ofrece la UNAN-León, evitándose así el empleo de varias cuentas de usuario, por la razón de que al momento de acceder se autenticará con una única cuenta donde se le mostrarán los servicios que tiene disponible y ya no habría la necesidad de estar recordando múltiples claves para autenticarse en cada uno de los servicios que tiene asignado, esto beneficiaría a los usuarios que hagan uso de la red de la UNAN-León.

Con esto se pretende incitar a la institución para que en un futuro se realice un proyecto con la posibilidad de que un usuario perteneciente a la red de la UNAN – León, pueda acceder a las redes inalámbricas de otras universidades empleando para ello la misma cuenta que utilizaría dentro de la UNAN-León y viceversa.

Objetivos

Objetivos Generales

Desarrollar una propuesta para unificar las cuentas de acceso de docentes y estudiantes a los servicios de red que ofrece la UNAN – León.

Objetivos específicos

Conocer los servicios de red que ofrece la UNAN-León y qué mecanismos utiliza cada uno de ellos para la autenticación.

Indagar qué tecnología se puede utilizar para lograr la centralización de las cuentas de usuarios de los servicios de red que ofrece la UNAN - León.

Demostrar qué ventajas ofrece la unificación de las cuentas de usuario frente al modelo de trabajo actual.

Diseño Metodológico

En esta sección se presentan la lista detallada de las actividades que se llevarán a cabo para el desarrollo del sistema.

Modelo de desarrollo del sistema

Para el desarrollo de este proyecto se ha optado por emplear un modelo evolutivo de desarrollo del sistema que en nuestro caso es el incremental. Este mitiga la rigidez del modelo en cascada, descomponiendo el desarrollo de un sistema en subsistemas a los cuales se aplica un ciclo de desarrollo en cascada completo.

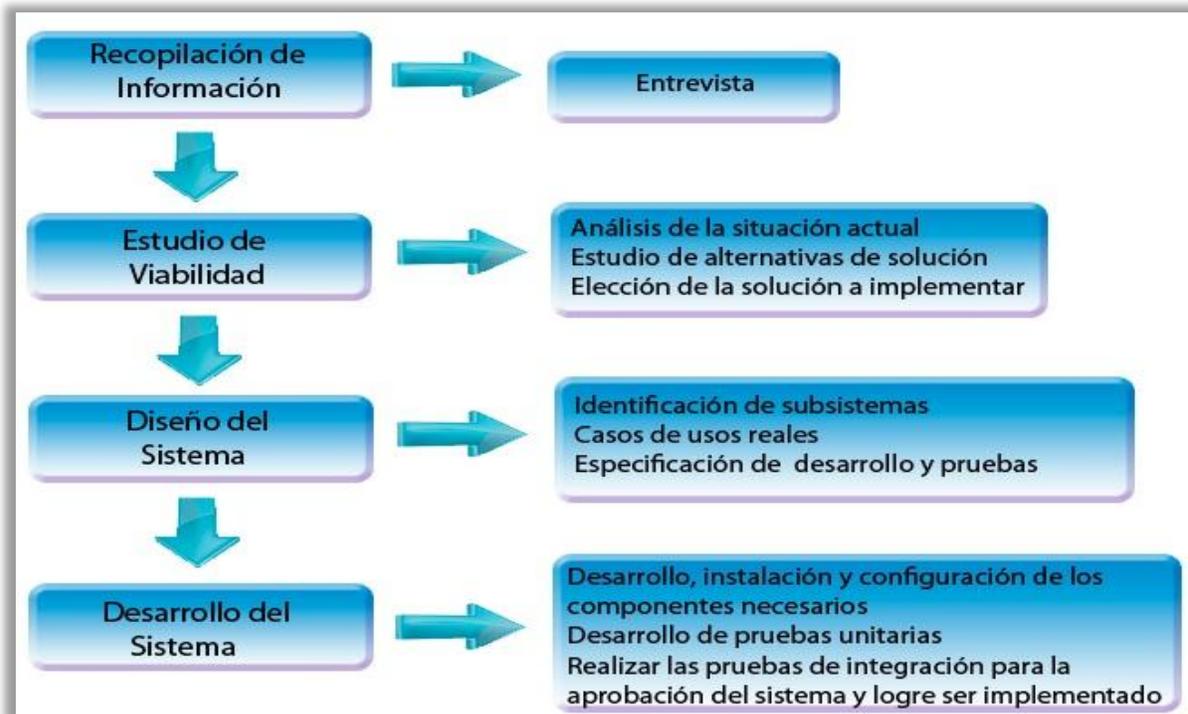


Figura 1. Proceso Iterativo

Actividades a desarrollar

Para llevar a cabo el desarrollo de este trabajo se realizarán las siguientes actividades:

1. Recopilación de información

Entrevista con el encargado del área de informática y comunicaciones de la Universidad para averiguar cuáles son los servicios de red que esta institución ofrece, como han sido implementados así como también de las necesidades de la que se carece y con qué frecuencia se utilizan.

Sistemas operativos, los servicios (software y versión), funcionamiento general, gestión de cuentas y autenticación.

2. Estudio de Viabilidad

A partir de las necesidades encontradas en la actividad anterior, nos dispondremos a buscar la mejor solución para este problema a partir de las siguientes tareas:

- a. Análisis de la situación actual
- b. Estudio de alternativas de solución
- c. Elección de la solución a implementar.

3. Diseño del Sistema

En esta fase se inicia el proceso de selección de los servicios (Servidor de correo, Servidor de llamadas VoIP, Servidor FTP, Servidor Web, Plataforma Virtual, Software para portal cautivo) y se analiza cómo serán ejecutados estos servicios en una arquitectura hardware y software, estos servicios serán gestionados por medio de un servidor de directorios. Además, se determinarán las especificaciones de desarrollo e integración, así como definir el entorno de pruebas y seleccionar qué criterios se utilizarán para que éstas sean representativas del correcto funcionamiento del sistema. Para ello se hará lo siguiente:

- a. Identificación de subsistemas
- b. Casos de usos reales
- c. Especificación de desarrollo y pruebas

4. Desarrollo del Sistema

A partir de esta etapa se orienta sobre los componentes software y hardware que se utilizara en el desarrollo el cual permitirá llegar a los objetivos propuestos. Definiremos las versiones del software o componentes software, así como estudiar dichos componentes y realizar su implantación en el entorno de desarrollo. En este inciso haremos lo siguiente:

- a. Desarrollo / Instalación y Configuración de los componentes necesarios
- b. Desarrollo de pruebas unitarias
- c. Realizar las pruebas de integración para la aprobación del sistema y logre ser implementado.

Cronograma de actividades

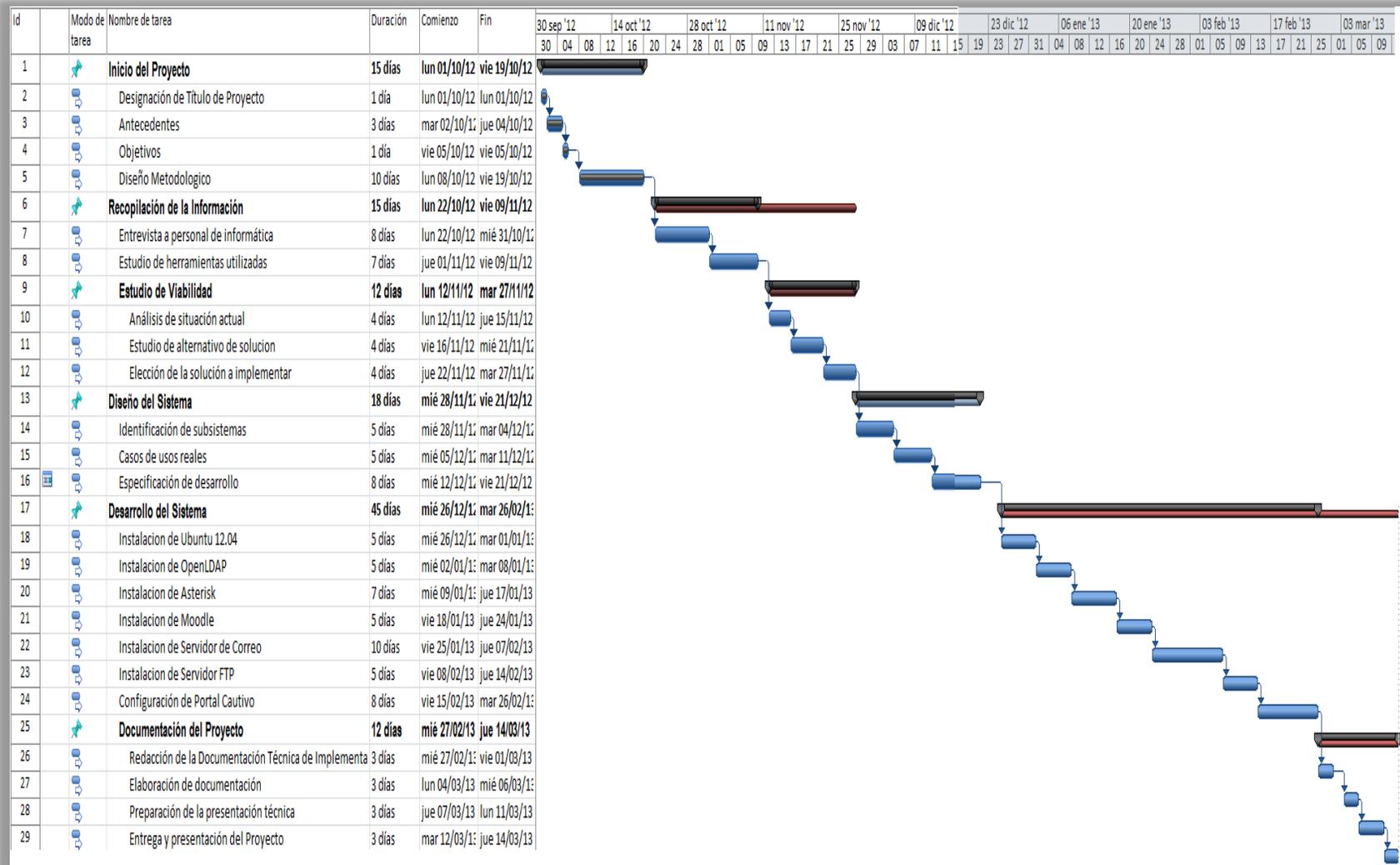


Figura 2. Cronograma de actividades

Situación actual de los Servicios de Red de la UNAN - León

Desde el año 2007 el servicio de red inalámbrica de la universidad ha tenido cambios importantes entre los cuales se encuentran los servicios mencionados anteriormente (Planteamiento del Problema), también estos servicios se han venido actualizando y es de mención que se mejoró el sistema de registro académico, se implementó un servicio para correo de estudiantes a mediados del 2010, el servicio de llamadas sobre IP que se desarrolló en el 2009 tuvo sus primeras pruebas en el 2010 el cual se ha venido mejorando, actualmente se puede solicitar el cambio de contraseña y activación de cuentas para el servicio de red inalámbrica desde la web de la institución (estud.unanleon.edu.ni).

¿Qué servicios de red ofrece la UNAN-León y que mecanismos utiliza cada uno de ellos para la autenticación?

Durante las entrevistas que realizamos al personal de informática (Ing. Jorge Treminio encargado de la Unidad de Redes y Comunicaciones) y responsable de mantenimiento de redes (Ing. Oscar Miranda) de la universidad nos informaron que esta institución cuenta con los siguientes servicios:

Servicio	Usuarios
Servidor Web	Personal de Informática
Servidor de Correo	Personal de Informática
Servicios Contables (UXIEC)	Personal Administrativo
Plataforma Virtual (Moodle)	Docentes – Estudiantes
Registro Académico (SIGACAD)	Estudiantes
FTP	Personal de Informática
Videoconferencia	Cualquiera que lo solicite
Correo Estudiantil (Microsoft Live Mail)	Estudiantes – Egresados
Red Inalámbrica (WIFI)	Docentes – Estudiantes - Otros
Llamadas sobre IP (VoIP)	Todo el Personal excepto Estudiantes

Tabla 1. Servicios de Red de la Unan-León.

La Unan-León tiene implementado en todo su sistema software libre, utilizando para ello:

1. Ubuntu server 10.10 y Debian Lenny 5.0
2. Sistemas Gestores de Bases de Datos como MySQL, Oracle y PostgreSQL
3. El correo utiliza Postfix, LDAP, RoundCube, Cyrus-imap
4. La web corre bajo un servidor Apache 2
5. El portal cautivo de acceso a internet inalámbrico utiliza Untangle y su autenticación es por Radius.

La Unan-León se ha visto en la necesidad de utilizar este tipo de plataformas por falta de presupuesto y por qué es bastante seguro, al igual un servidor de antivirus exclusivo para funcionarios y personal docente.

En base a la información recopilada en nuestra entrevista hemos clasificado estos servicios de acuerdo a la prioridad que la institución tiene asignado para estos en:

1. Servicio de red (Local) y Servicio de red inalámbrica (WIFI)
2. Servicios contables (UXIEC) y Registro académico (SIGACAD)
3. Servidor de correo y Servicio de Llamadas sobre IP (VoIP)
4. Plataforma de aula virtual (Moodle) y Servidor web.

La autenticación se dan en el propio servidor de la aplicación que se está accediendo, al momento de querer acceder a ellos por ejemplo la política que tienen para dar de alta a un usuario en la red inalámbrica es: si eres estudiante y tienes equipo portátil propio puedes solicitar al encargado de Redes y Comunicaciones de la universidad la creación de una cuenta propia para conexión a internet inalámbrico, con respecto al servicio de

correo estudiantil este se te asigna desde el momento en que el estudiante es matriculado y en relación con los otros servicios se siguen distintas políticas.

Labores de mantenimiento

Los encargados de redes y comunicaciones de la UNAN-León realizan semanalmente respaldo de toda la información que se procesa en la universidad en servidores de respaldo asignados para esta labor y en los servidores de los propios servicios.

Hasta el momento los encargados de la unidad de redes y comunicaciones de la universidad tienen cerca de 1800 equipos activos sin incluir los equipos que se le asignaron a los docentes y equipos propios de estudiantes, es de mencionar que el servicio de ancho de banda para acceso a internet también ha venido incrementándose desde el año 2006 que se contaba con un ancho de banda de 1 MB, 2008 con 2 MB y actualmente desde el año 2010 se cuenta con 45 MB a estos cambios se le suman el mejoramiento de infraestructuras y equipos para el acceso a internet (switch, router, fibra óptica).

Marco Teórico

Tecnologías Utilizadas

Aplicaciones Web

Es una página web con contenido dinámico, es decir, cambia su contenido según la interacción de cada usuario que la visita.

Básicamente hay tres tipos de aplicaciones:

1. Las que permiten al usuario encontrar información fácil y rápidamente en una página web rica en contenido: buscadores, tablas de datos interactivas, planos de situación navegables, etc.
2. Recibir, guardar y analizar datos proporcionados por el usuario de la página: formularios, listas de correo, carritos de la compra.
3. Actualizar páginas web cuyo contenido necesita ser puesto al día: revistas y periódicos digitales.

Servidor

Un servidor es un sistema informático que ofrece un servicio o un recurso necesario para desempeñar una función o tarea utilizando una infraestructura de red para poder hacerlo, este servicio puede estar diseñado para mejorar la gestión o administración de la propia red que debería estar diseñada para ofrecer una funcionalidad y/o servicio a los clientes.

Existen diferentes tipos de servidores entre los cuales mencionaremos los utilizados por la Unan-León:

- Servidor Web: es un programa que se ejecuta continuamente en un computador, manteniéndose a la espera de peticiones de ejecución que le hará un cliente o un usuario de Internet. El servidor web se encarga de contestar a estas peticiones de forma adecuada, entregando como resultado una página web o información de todo tipo de acuerdo a los comandos solicitados.
- Servidor de Correo: es una aplicación informática que tiene como objetivo enviar, recibir y gestionar mensajes a través de las redes de transmisión de datos existentes, con el fin de que los usuarios puedan mantenerse comunicados con una velocidad muy superior a la que ofrecen otros medios de envío de documentos. Los servidores de correo trabajan como una agencia de correo postal, sólo que no envían paquetes, sino, datos digitales e información electrónica, la cual llega a su destino de forma casi inmediata
- Servidor de Archivos (FTP): es un programa cuya función es permitir el acceso remoto a archivos almacenados en él o directamente accesibles por este. En principio, cualquier ordenador conectado a una red con un software apropiado, puede funcionar como servidor de archivos.
- Servidor de Telefonía (VoIP): realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las funciones de un sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o el Internet.

-
- Servidor de Bases de Datos: provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.

Red Inalámbrica (WIFI)

Red inalámbrica (Wireless Network en inglés) es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos.

Una de sus principales ventajas es notable en los costos, ya que se elimina todo el cable ethernet y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe de tener una seguridad mucho más exigente y robusta para evitar a los intrusos.

Moodle

Moodle es un Ambiente Educativo Virtual, sistema de gestión de cursos, de distribución libre, que ayuda a los educadores a crear comunidades de aprendizaje en línea. Este tipo de plataformas tecnológicas también se conoce como LMS (Learning Management System).

Videoconferencia

Es la comunicación simultánea bidireccional de audio y vídeo, permitiendo mantener reuniones con grupos de personas situadas en lugares alejados entre sí. Adicionalmente, pueden ofrecerse facilidades telemáticas o de otro tipo como el intercambio de gráficos, imágenes fijas, transmisión de ficheros desde el ordenador, etc.

El núcleo tecnológico usado en un sistema de videoconferencia es la compresión digital de los flujos de audio y vídeo en tiempo real. Su implementación proporciona importantes beneficios, como el trabajo colaborativo entre personas geográficamente distantes y una mayor integración entre grupos de trabajo.

Freeradius

Es una variante de código libre del protocolo RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Server). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cable módem, Ethernet o WiFi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo Network Access Server (NAS) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia, los datos se pueden utilizar con propósitos estadísticos.

Certificado Digital

Un certificado digital (también conocido como certificado de clave pública o certificado de identidad) es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la

vinculación entre la identidad de un sujeto o entidad (por ejemplo: nombre, dirección y otros aspectos de identificación) y una clave pública.

Este tipo de certificados se emplea para comprobar que una clave pública pertenece a un individuo o entidad. La existencia de firmas en los certificados aseguran por parte del firmante del certificado (una autoridad de certificación, por ejemplo) que la información de identidad y la clave pública perteneciente al usuario o entidad referida en el certificado digital están vinculadas.

LDAP

En todas las redes informáticas donde hay un gran número de usuarios con diferentes usos (cuentas Windows, GNU/Linux, MacOSX, etc.), la gestión puede ser una tarea muy pesada. Tener un buen sistema de gestión de usuarios puede agilizar esta tarea. LDAP (Lightweight Directory Access Protocol) nos permite organizar de manera jerárquica todo tipo de datos como: cuentas de usuario, grupos, puntos de montaje, cuentas de equipos, etc. de manera rápida y sencilla.

Cualquier sistema de directorio LDAP está orientado a ofrecer una respuesta rápida a cualquier petición de datos de gran volumen, así como a operaciones de búsqueda. También soportan facilidad de replicación de datos, así como la distribución de los mismos por la red. Estos métodos facilitan el acceso y reutilización de cualquier dato almacenado en el servicio de directorio reduciendo su tiempo de respuesta.

Estudio de Viabilidad

Situación Actual

La constante evolución de los sistemas de información exige que las organizaciones replanteen sus modelos de funcionamientos para poder garantizar necesidades actuales y futuras. En nuestro entorno universitario se hace evidente, además, que es necesario homogenizar los diversos servicios utilizados en la institución. Como mencionamos anteriormente la Unan-León tiene implementado en su sistema un directorio LDAP con servidor FREERADIUS que no es empleado en todos los servicios por lo que este trabajo propone la utilización de esta misma metodología para todas las aplicaciones de la red.

Alternativas de Solución

¿Cómo se puede hacer para unificar las cuentas de acceso a los servicios de la UNAN-León?

En principio cuando hablamos de unificar cuentas de acceso a diferentes servicios nos referimos a “comunicaciones unificadas”, las cuales son definidas como el proceso en el cual todos los sistemas y aparatos de comunicación de una empresa se encuentran completamente integrados. Esto brinda ventajas a los usuarios ya que pueden mantenerse en contacto con cualquier persona, donde quiera que estén y en tiempo real.

El objetivo de las Comunicaciones Unificadas es el de optimizar los procedimientos laborales, mejorar las comunicaciones entre personas y simplificar procesos que benefician las ganancias de los negocios. El problema con este tipo de comunicaciones unificadas es que son demasiado caras para una implementación a gran escala como la que se pretende realizar en la Unan-León, y también porque la mayoría de los servicios que se han creado en la institución los desarrolladores han utilizado sus propias herramientas (software y hardware) y no han tenido la visión de incorporar o en este caso unificar todos los servicios.

La Unan-León, hoy en día, no cuenta con equipos realmente sofisticados y a la vanguardia de la tecnología evolutiva que actualmente domina el mundo informático, tampoco cuenta con los recursos (presupuesto) suficientes para poder hacerlo, razón por la cual, los encargados del sistema de red de la universidad, se ven forzados a implementar soluciones gratuitas que de algún modo viene a contribuir al desarrollo y colocarla a la par de otras instituciones que si lo están.

En este trabajo tomaremos como base el uso del protocolo “LDAP” que actualmente emplea la Unan-León, para desarrollar la Propuesta de Unificación de Cuentas de Usuarios en los demás servicios de red de la institución.

Existen diversas implementaciones y aplicaciones reales del protocolo LDAP las cuales se podrían utilizar y las hay tanto gratuitas como comerciales en este caso mencionaremos las basadas en software libre como son:

- **OpenLDAP** es una implementación libre del protocolo que soporta múltiples esquemas por lo que puede utilizarse para conectarse a cualquier otro LDAP. Es de libre implementación y al ser un protocolo independiente de la plataforma, varias distribuciones GNU/Linux (es de mencionar algunos como Debian, Ubuntu, Centos, OpenSuse) y BSD lo incluyen, al igual que Mac OS X, Solaris, Windows (2000/XP, Vista, Seven) y z/OS.
- **Red Hat Directory Server** es un servidor basado en LDAP que centraliza la configuración de aplicaciones, perfiles de usuarios, información de grupos, políticas así como información de control

de acceso dentro de un sistema operativo independiente de la plataforma, para implementarlo se debe de comprar el software o bien pedir una versión de prueba gratuita para su implementación.

- **Open DS** o como actualmente se le llama **Sun Java System Directory Server**, está basado en los estándares LDAPv3 y DSMLv2, surgió como un proyecto interno de SUN, aunque posteriormente se puso a disposición de la comunidad. Está desarrollado en JAVA y precisa de un entorno de ejecución (Java Runtime Environment) para funcionar. Es multiplataforma.

Elección de la solución a implementar

En la actual propuesta se evaluaron 3 opciones entre ellas **OpenLdap**, **Red Hat Directory Server** y **Open DS** y se optó por elegir OpenLdap como nuestro servidor de directorio, puesto su implementación no tendría costo alguno e igual forma, no tendríamos que instalar ningún software o programa adicional para integrar nuestra estructura, posteriormente elegimos como sistema operativo base Ubuntu 12.04 entre las opciones (Debian 6 y Centos 6) debido a que Ubuntu es una versión derivada de Debian la cual es la más potente y segura versión para servidores a nivel mundial, este sistema operativo posee características específicas como son un kernel optimizado para servidores y cuenta con soporte para 5 años y cada 6 meses hay nueva versión de su sistema. Esta opción es software libre (se trata de un entorno abierto que nos permite la configuración adecuada para nuestras necesidades particulares) y viene de una u otra forma a beneficiar al desarrollo de la institución la cual no cuenta con suficientes recursos (presupuesto) para utilizar o comprar un sistema privativo.

OpenLDAP

El proyecto OpenLDAP, creado en 1998 por Kurt Zeilenga, nació como la continuación de la versión 3.3 del servidor LDAP de la Universidad de Michigan cuando dejaron de desarrollarlo, es un servidor LDAP que se distribuye bajo licencia GNU (OpenSource), que permite que el software se pueda usar de forma gratuita tanto de forma educativa como profesional. Además disponemos del código fuente para poder realizar nuestras propias modificaciones.

Este servidor de LDAP es la única alternativa, hoy en día a los directorios propietarios. Es un servidor escrito según los estándares, que soporta LDAPv2 y gran parte de LDAPv3.

En este momento LDAP cuenta con tres piezas de software fundamentales:

- Slapd. Es el núcleo del proyecto, un servidor para recibir, gestionar las peticiones de LDAP, es lo que implementa las funciones básicas de LDAP.
- Slurpd. Es un demonio que sirve para replicar un directorio LDAP. Hasta ahora LDAP solo permite la replicación de un árbol entero sin la replicación de ninguna de sus partes.
- Librerías y utilidades. OpenLDAP prevé una serie de librerías (en C) y utilidades para el acceso a directorios, que también forman parte de su proyecto, de esta manera se desarrolla una solución completa al manejo del directorio en cuanto a sencillas aplicaciones y librerías de programación.

Características de OpenLDAP:

- OpenLDAP funciona sobre todas las plataformas Unix (Linux, HP UX, AIX, Solaris, Windows).
- Ofrece un conjunto de API que permite el desarrollo y el soporte de aplicaciones en C/C++, PHP, Perl, Java.
- El soporte de encriptación SSL permite la autenticación asegurada de los usuarios.
- Dispone de aplicaciones que permiten la administración gráfica de datos y una visión jerárquica de redes.
- La función de réplica asegura una puesta al día sincronizada de los datos de la guía sobre todos los servidores.

Razones para elegir OpenLDAP

- Es interoperable con todas las aplicaciones y guías soportando el protocolo LDAP, y es cómodo migrar de una guía propietaria hacia OpenLDAP.
- Presta exactamente los mismos servicios que sus equivalentes propietarios, con mejores rendimientos: es 10 veces menos exigente en recursos de máquina (tiempo CPU y RAM).

-
- El Coste Total de Propiedad de OpenLDAP, en particular para guías de un tamaño importante o que lo podrían ser, es muy claramente inferior al CTP de software propietario.

Costo de OpenLDAP

Siendo un servidor de código abierto, desarrollado por diferentes desarrolladores distribuidos en distintas áreas geográficas es gratuito, así como sus guías de instalación y documentación.

“El problema es que igualmente no hay ninguna forma de manutención o responsabilidad para el software instalado, no existirá ninguna empresa responsable para cualquier problema que pueda surgir, la única asistencia se podrá obtener a través del fórum de consultas, o las FAQs creados por los desarrolladores del OpenLDAP.”

Las características propias de un servidor LDAP son:

- Operaciones de lectura muy rápidas. Debido a la naturaleza de los datos almacenados en los directorios, las lecturas son más comunes que las escrituras.
- Datos relativamente estáticos. Los datos almacenados en los directorios no suelen actualizarse con mucha frecuencia.
- Entorno distribuido, fácil replicación
- Estructura jerárquica. Los directorios almacenan la información de forma jerárquica y de forma nativa.
- Orientadas a objetos. El directorio representa a elementos y a objetos. Los objetos son creados como entradas, que representan a una colección de atributos.
- Esquema Standard. Los directorios utilizan un sistema estándar que pueden usar fácilmente diversas aplicaciones.
- Atributos multi-valor. Los atributos pueden almacenar un valor único o varios.
- Replicación multi-master. Muchos de los servidores LDAP permiten que se realicen escrituras o actualizaciones en múltiples servidores.

Funcionamiento de LDAP

El servicio de directorio LDAP se basa en un modelo cliente-servidor. Uno o más servidores LDAP contienen los datos que conforman el árbol de directorio LDAP o base de datos troncal, el cliente LDAP se conecta con el servidor LDAP y le hace una consulta. El servidor contesta con la respuesta correspondiente, o bien con una indicación de donde puede el cliente hallar más información. No importa con que servidor LDAP se conecte el cliente ya que siempre observará la misma vista del directorio; el nombre que se le presenta a un servidor LDAP hace referencia a la misma entrada que se daría como referencia en otro servidor LDAP.

Ventajas en el uso de LDAP

Un directorio LDAP destaca sobre los demás tipos de bases de datos por las siguientes características:

- Es muy rápido en la lectura de registros.
- Permite replicar el servidor de forma muy sencilla y económica.
- Muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente.
- Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas.
- Usa un sistema jerárquico de almacenamiento de información.
- Permite múltiples directorios independientes.
- Funciona sobre TCP/IP y SSL/TLS.
- La mayoría de aplicaciones que gestionan usuarios disponen de soporte para LDAP.

Usos empresariales

Dadas las características de LDAP sus usos más comunes son:

- Directorios de información. Por ejemplo bases de datos de empleados organizados por departamentos (siguiendo la estructura organizativa de la empresa) o cualquier tipo de páginas amarillas.
- Sistemas de autenticación/autorización centralizada. Grandes sistemas donde se guarda gran cantidad de registros y se requiere un uso constante de los mismos. Por ejemplo:
 - Active Directory Server de Microsoft, para gestionar todas las cuentas de acceso a una red corporativa y mantener centralizada la gestión del acceso a los recursos.
 - Sistemas de autenticación para páginas Web, algunos de los gestores de contenidos más conocidos disponen de sistemas de autenticación a través de LDAP.
 - Sistemas de control de entradas a edificios, oficinas, etc.
- Sistemas de correo electrónico. Grandes sistemas formados por más de un servidor que accedan a un repositorio de datos común.
- Sistemas de alojamiento de páginas web y FTP, con el repositorio de datos de usuario compartido.
- Grandes sistemas de autenticación basados en RADIUS, para el control de accesos de los usuarios a una red de conexión o ISP.
- Servidores de certificados públicos y llaves de seguridad
- Autenticación única o "single sign-on" para la personalización de aplicaciones.
- Perfiles de usuarios centralizados, para permitir itinerancia o "roaming"
- Libretas de direcciones compartidas.

Diseño del Sistema

Para el desarrollo de nuestro sistema de Unificación de las Cuentas de Usuarios de Red de la UNAN-León, hemos decidido utilizar una distribución Linux “**Ubuntu Desktop 12.04**” porque es la tendencia actual dentro de la institución.

Configuraciones del Servidor

Se realizara la instalación de Virtual Box a partir de aquí configuraremos 2 máquinas virtuales Pfsense para uso como Portal Cautivo (2GB de almacenamiento y 128 MB de memoria RAM) y 1 como usuario Cliente Windows XP SP3 (256 MB de memoria RAM y 5GB de almacenamiento).

Requisitos Mínimos para instalación

Con respecto a los requisitos mínimos de instalación nos basaremos en los estándares de instalación de un servidor Ubuntu 12.04, los cuales son: Procesador de 1GHz, Memoria RAM 512 MB, Espacio en Disco 8GB, Red 100Mbps

Software a Utilizar

En este equipo se procedió a instalar los siguientes programas como forma de simular algunos de los servicios de Red que implementa la Unidad de Redes de la UNAN-León y como parte de la unificación de los servicios de red:

Apache versión 2.2.22, Asterisk versión 11.2.1, OpenLDAP versión 2.4.28-1.1ubuntu4.2, Vsftpd versión 2.3.5-1ubuntu2, Postfix versión 2.9.6, Dovecot versión 2.0.19, Pfsense versión 2.0.2-RELEASE-i386, Freeradius versión 2.1.12_1.

Asterisk:

Es una aplicación para controlar y gestionar comunicaciones de cualquier tipo, ya sean analógicas, digitales o VoIP mediante todos los protocolos VoIP que implementa, proporciona funcionalidades de una central telefónica.

Phpldapadmin:

Es una aplicación que permite administrar el contenido de un servicio de directorios, específicamente de OpenLDAP. Está desarrollado en PHP y se instala en el mismo servidor donde se encuentra el servicio de directorio (LDAP).

Vsftpd:

Es uno de los mejores servidores ftp que existen para Linux (también se lo puede utilizar en otros sistemas operativos). Es seguro, sumamente flexible, modular y fácil de configurar y es el servidor FTP por defecto de la distribución Ubuntu.

Postfix:

Es un Agente de transporte de correo (MTA) de software libre/código abierto, un programa informático para el enrutamiento y envío de correo electrónico, creado con la intención de que sea una alternativa más rápida, fácil de administrar y segura.

Dovecot:

Es un servidor de IMAP y POP3 de código abierto para sistemas GNU/Linux / Unix-Like, escrito fundamentalmente pensando en seguridad, es ligero, rápido, fácil de instalar y sobre todo seguro.

Squirrelmail:

Es un programa Webmail que te permite revisar el correo que tengas en un servidor con imap mediante cualquier navegador. Esto está muy bien apreciado por WebMaster para no tener que añadir más reglas a un firewall, para implantarlo en una oficina o pyme.

Portal Cautivo:

Es una página Web con la cual un usuario de una red pública y/o privada debe interactuar antes de garantizar su acceso a las funciones normales de la red.

Pfsense

Es una distribución basada en FreeBSD, el proyecto se inició en 2004 como derivada de m0n0wall. Su objetivo es tener un cortafuego (firewall) fácilmente configurable a través de una interface web e instalable en cualquier PC, incluyendo los mini PC de una sola tarjeta.

Softphone:

Software que hace la simulación de teléfono convencional por computadora para realizar llamadas a otros softphones o bien a teléfonos convencionales.

El procedimiento de instalación a seguir será el siguiente:

Iniciamos con la instalación del servidor Ubuntu, al cual le instalaremos todas las librerías y herramientas necesarias para compilar, así mismo se le instalara el servidor web apache, php y la base de datos mysql. Posteriormente iniciaremos la instalación del servidor OpenLDAP donde crearemos la estructura de nuestro directorio y procedemos a crear y asignar permisos a las carpetas de los usuarios, continuamos con la instalación de la central telefónica Asterisk donde luego de configurarla crearemos extensiones e instalaremos unos softphones para realizar pruebas de funcionalidad, seguimos con la instalación del Entorno de desarrollo virtual Moodle y habilitaremos a los usuarios del directorio LDAP, procedemos a instalar nuestro servidor de correo donde se configuraran las cuentas de los usuarios LDAP, realizaremos pruebas de verificación desde cliente web y luego instalamos software de escritorio para que el cliente lo reciba directamente en su programa de correo de preferencia y finalmente descargamos y configuramos el portal cautivo donde le instalaremos el paquete Freeradius para que se logre autenticar contra nuestro servidor LDAP y configuramos el servidor DHCP para que los usuarios tengan acceso a internet luego de autenticarse.

Desarrollo del Sistema

Instalación de Ubuntu Desktop 12.04

Para la instalación se procedió a descargar la ISO de Ubuntu desde la página oficial <http://www.ubuntu.com/download/> donde se eligió la versión Desktop 12.04 para realizar la instalación y configuración más cómoda.

Luego de la instalación se realiza una actualización de todos los paquetes que este incluye así como también la instalación de nuevas aplicaciones útiles para el funcionamiento de nuestro proyecto por medio de las siguientes sintaxis:

\$sudo apt-get update – comando para realizar la actualización del sistema.

\$sudo apt-get install synaptic - esta herramienta gráfica nos permite instalar, actualizar o desinstalar paquetes de programas de forma versátil. No viene instalada por defecto.

\$sudo apt-get install aptitude - Comando para instalar aplicaciones desde la terminal. No es necesario ya que se puede utilizar el comando "apt-get".

\$sudo apt-get install openjdk-7-jre - Soporte para aplicaciones Java. El OpenJDK y el plugin IcedTea, funcionan bien para la mayoría de los propósitos (programas de administración web como Moodle) y son de libre uso.

\$sudo apt-get install ubuntu-restricted-extras - Paquete de Extras restrictivos para multimedia. Contiene códec y aplicaciones restrictivos o con copyright, tales como mp3, flash, se pueden ver videos en internet pero el propósito es para utilizarlo como códec de audio en nuestra Central VoIP.

\$sudo apt-get install p7zip-full p7zip-rar rar unrar – para descomprimir archivos.

\$sudo apt-get install build-essential – software básico de compilación.

\$sudo apt-get install linux-headers-`uname -r` - librerías de desarrollo del kernel necesarias para determinados paquetes (asterisk).

Una vez finalizada la instalación anterior, procedemos a instalar el servidor Web Apache, el sistema de gestión de bases de datos Mysql y el procesador de hipertexto para el desarrollo de aplicaciones Web Php.

\$sudo apt-get install apache2 apache2-doc apache2.2-common apache2.2-bin libapache2-mod-php5 apache2-mpm-prefork apache2-utils

\$sudo apt-get install mysql-client mysql-server mysql-common libdbd-mysql-perl mysql-client-5.5 libapache2-mod-auth-mysql mysql-client-core-5.5 mysql-server-core-5.5

\$sudo apt-get install php5 php5-common php5-dev php5-dbg php5-mysql php5-ps php-pear php5-memcache php5-auth-pam php5-cgi php5-tidy php5-sqlite php5-cli php5-ming php5-mcrypt php5-gd php5-gmp php5-xmlrpc php5-xsl php5-curl php5-snmp php5-pspell php5-recode phpmyadmin

Instalación de OpenLDAP SERVER en Ubuntu Desktop 12.04

Para la instalación del servidor de Protocolo Ligero de Acceso a Directorios o por sus siglas LDAP se realizó lo siguiente:

1. Ejecutamos el siguiente comando:
`$sudo apt-get install slapd ldap-utils php5-ldap`
2. Configuramos el servidor Ldap
`$sudo dpkg-reconfigure slapd`

Este comando ejecuta un wizard para la configuración del servidor LDAP con lo cual se procede a ingresar los datos siguientes:

Desea omitir la configuración del servidor OpenLDAP? **NO**
DNS Domain Name: **unanleon.edu.ni**
Organization Name: **unanleon.edu.ni**
Database: **HDB**
Desea que se borre la base de datos cuando se purgue el paquete slapd?: **NO**
Desea mover la base de datos antigua? **SI**
Contraseña del administrador: *****
Verificar la contraseña: *****
Allow LDAPv2 protocol?: **NO**

Al finalizar este wizard, tendremos la cuenta por defecto "admin" con la contraseña "*****" para el dominio "unanleon.com"

3. Se configuro el tipo de encriptación de la contraseña del servidor para que este tenga mayor seguridad mediante el comando:
`$slappasswd -h {MD5}`
4. Procedimos a instalar una herramienta gráfica para administrar y crear nuestra estructura desde un administrador web con el comando:
`$sudo apt-get install phpldapadmin`

Se inició a crear la estructura del servidor como ejemplo para este proyecto se optó llamarle unanleon.com, dentro esta estructura base se han creado 2 usuarios uno "admin" quien será el usuario administrador del sistema, el otro "personal (unidad organizacional)" este último es el que contendrá a los grupos de usuarios docente y estudiante de tipo posixAccount dentro de los cuales se han creado 2 usuarios cada uno de tipo userAccount a los cuales se les ha asignados como atributos: nombre, apellido, id de usuario, correo electrónico, extensión telefónica y ruta de carpeta que contendrán los archivos de estos dentro del servidor.

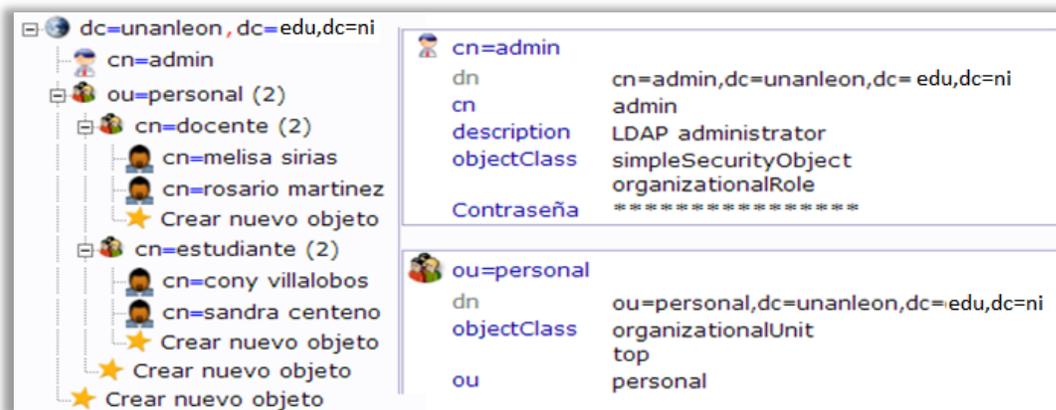


Figura 3. Estructura General

5. Una vez creada la estructura con los usuarios y grupos correspondientes se configuro la autenticación del cliente LDAP para esto se instalaron los paquetes auth-client-config y libnss-ldap

los cuales permitirán la validación de los usuarios y la cache nscd para evitar que el cliente consulte constantemente al servidor en operaciones tan frecuentes como ls/home/usuario-ldap/:

```
$sudo apt-get install libnss-ldap nscd
```

6. Se procede habilitar el perfil auth-client-config con el comando:

```
auth-client-config -t nss -p lac_ldap
```

-t: modifica el archivo nsswitch ubicado en /etc/nsswitch.conf

-p: parámetro que indica el perfil a habilitar o deshabilitar

lac_ldap: el perfil de auth-client-config que forma parte del paquete ldap-auth-config (este fichero se ubica en /etc/auth-client-config/profile.d ldap-auth-config) quedando el archivo /etc/nsswitch.conf de la siguiente manera:

```
# /etc/nsswitch.conf
passwd: files ldap
group: files ldap
shadow: files ldap
hosts:      files mdns4_minimal [NOTFOUND=return] dns mdns4
networks:   files
protocols:  db files
services:   db files
ethers:     db files
rpc:        db files
netgroup: nis
```

7. Se necesitó crear el archivo mkhomedir en /usr/share/pam-configs/my_mkhomedir con el propósito de crear automáticamente las carpetas de inicio en el servidor al momento de que el usuario inicie sesión por primera vez, los datos son los siguientes:

```
Name: activate mkhomedir
Default: yes
Priority: 900
Session-Type: Additional
Session:
    required pam_mkhomedir.so umask=0022 skel=/etc/skel
```

8. Se utiliza el comando pam-auth-update para configurar los archivos del sistema automáticamente incluidos en (/etc/pam.d/common-*) y activar el archivo creado anteriormente de esta forma se podrá utilizar la autenticación LDAP.

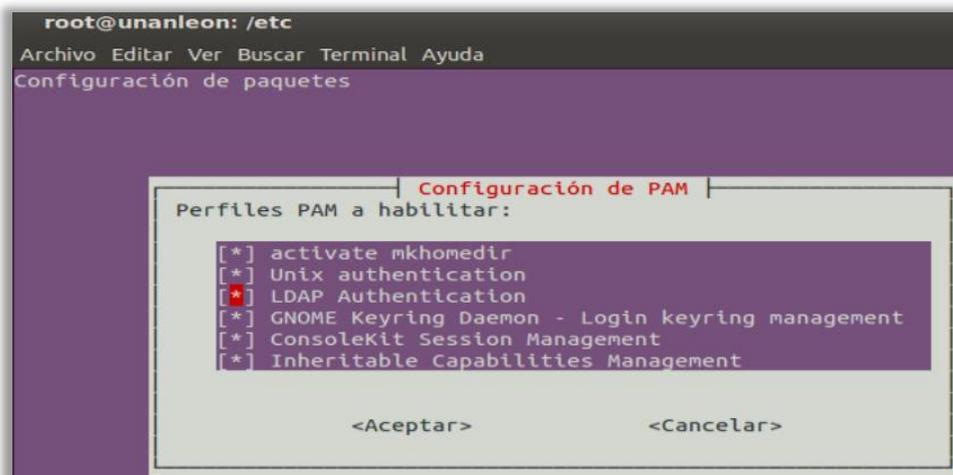


Figura 4. Activación de Perfil PAM contra LDAP

9. Se ingresaron los siguientes datos en el fichero /etc/ldap/ldap.conf

```
HOST localhost
BASE dc=unanleon,dc=edu,dc=ni
```

10. Se procedió a editar el fichero /etc/ldap.conf colocando los siguientes datos:

```
host localhost
BASE dc=unanleon,dc=edu,dc=ni
ldap_version 3
rootbinddn cn=admin,dc=unanleon,dc=edu,dc=ni
pam_password md5
```

11. Se exportan los ficheros de usuarios y grupos

```
$ getent passwd
$ getent group
```

```
msirias:*:2000:500:melisa sirias:/home/personal/docente/msirias:/bin/sh
rmartinez:*:2001:500:rosario martinez:/home/personal/docente/rmartinez:/bin/sh
scenteno:*:3000:501:sandra centeno:/home/personal/estudiante/scenteno:/bin/sh
cvillalobos:*:3001:501:cony villalobos:/home/personal/estudiante/cvillalobos:/bin/sh
root@unanleon:/etc# getent passwd
```

Figura 5. Exportación de usuarios LDAP

```
docente:*:500:
estudiante:*:501:
root@unanleon:/etc# getent group
```

Figura 6. Exportación de Grupos de LDAP

12. Se realiza prueba de funcionamiento con algún usuario de la estructura del árbol getent passwd id_usuario, posterior a ello aparecerá los atributos que el usuario posee (el gid de grupo y el uid de usuario y ruta de ficheros asignados dentro del servidor y tipo de contraseña) e igual se podría realizar la prueba de funcionamiento con el comando finger + id_usuario o simplemente con la orden "slptest"

```
root@unanleon:/etc# getent passwd rmartinez && getent passwd scenteno
rmartinez:*:2001:500:rosario martinez:/home/personal/docente/rmartinez:/bin/sh
scenteno:*:3000:501:sandra centeno:/home/personal/estudiante/scenteno:/bin/sh
root@unanleon:/etc#
```

Figura 7. Primera Verificación de Funcionalidad de LDAP

```
root@unanleon:/# finger mfernandez
Login: mfernandez                Name: merling fernandez
Directory: /home/docente/mfernandez  Shell: /bin/sh
Last login Mon Feb  4 20:57 (CST) on pts/3 from 192.168.0.10
No mail.
No Plan.
```

Figura 8. Segunda Verificación de Funcionalidad de LDAP

Instalación de Central Telefónica Asterisk versión 11 y Autenticación con LDAP

Para la instalación de nuestra central telefónica Asterisk procedimos a instalar las siguientes dependencias y herramientas necesarias:

```
$sudo apt-get install openssl libssl-dev ssh (librería para acceso vía SSH)
```

```
$sudo apt-get install gcc make g++ libldap2-dev (librerías de compilación de software, sirve para compilar Asterisk)
```

```
$sudo apt-get install ncurses-term libncurses5-dev libncurses5-dbg ncurses-doc libncurses5 libncursesw5-dev ncurses-base ncurses-bin libncursesw5 libncurses-widgets-perl mtr-tiny libtinfo5 libcurses-perl (para poder usar la consola de asterisk)
```

```
$sudo apt-get install bison bison-doc libxml2 libxml2-dev libtiff4 libtiff4-dev libnet-telnet-perl mime-construct libipc-signal-perl libmime-types-perl libproc-waitstat-perl (librerías requeridas por el servicio web de FreePBX)
```

```
$sudo apt-get install subversion curl devscript libhttp-cookies-perl libsqlite3-dev sqlite3 (librerías requeridas por Asterisk para el manejo de ayuda y de extracción de archivos del CVS)
```

Posterior a la instalación de los paquetes que necesita Asterisk para funcionar iniciamos con la descarga de los siguientes archivos:

DAHDI (Digium/Asterisk Hardware Device Interface) es una interfaz para dispositivos utilizada para controlar tarjetas telefónicas por Asterisk y es necesaria para utilizar algún tipo de hardware como tarjetas FXS o FXO en nuestro PC Asterisk. Y lo hacemos ingresando a la siguiente dirección: <http://downloads.asterisk.org/pub/telephony/dahdi-linux-complete/dahdi-linux-complete-current.tar.gz>

MPG123 es una librería para la decodificación de archivos mp3, podemos descargarla desde su página oficial: <http://sourceforge.net/projects/mpg123/files/>

Asterisk-11 un programa de software libre que proporciona funcionalidades de una central telefónica. Podemos adquirirlo desde la siguiente dirección: <http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-11-current.tar.gz>

Luego de adquirir el software necesario para la implementación de la central telefónica se procedió con la instalación y configuración de Asterisk para realizar la autenticación con el servidor LDAP:

Iniciamos moviendo los archivos anteriormente descargados (Dahdi, mpg123 y asterisk-10) a la carpeta /usr/src/ una vez ahí procedemos a descomprimirlos, compilarlos e instalarlos de la siguiente manera:

```
$tar xvzf dahdi-linux-complete-current.tar.gz
$cd dahdi-linux-complete-2.6.1+2.6.1/
$sudo make
$sudo make install
$sudo make config
$sudo service dahdi start
```

```
$tar -xjvf mpg123-1.14.4.tar.bz2
$cd mpg123-1.14.4/
$./configure
$sudo make
$sudo make install
```

```
$tar -xvzf asterisk-11-current.tar.gz
```

```
$cd asterisk-11/  
$ ./configure --with-ldap
```

Esta es la parte más importante de la instalación de Asterisk pues al ejecutar dicha orden se crea el fichero `res_ldap.conf` el cual nos permitirá modificar para que Asterisk se autentique con el servidor LDAP seguido

```
$make menuselect
```

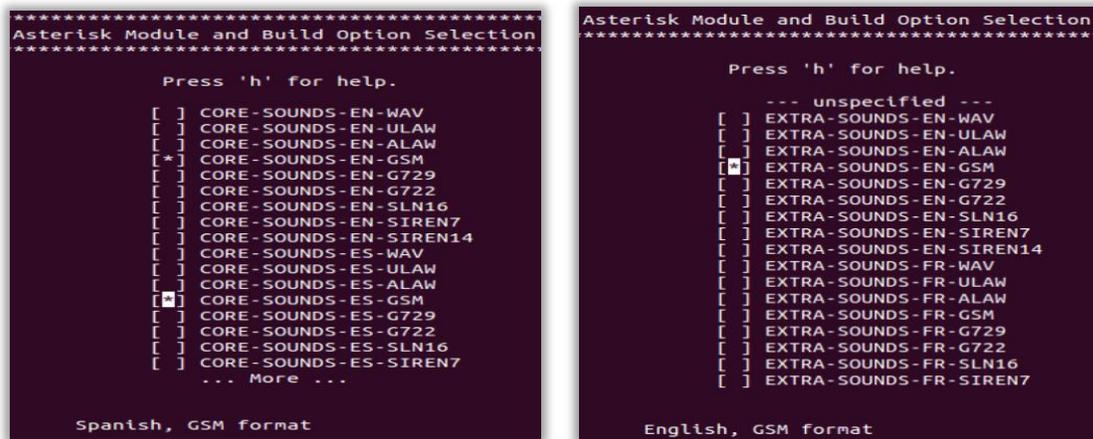


Figura 9. Activación de Ficheros de Sonidos y Módulos Extras

```
$apt-get install subversion  
$contrib/scripts/get_mp3_source.sh  
$sudo make  
$sudo make install  
$sudo make samples  
$sudo make config  
$sudo make install-logrotate
```

Se verifica si el servidor Asterisk se está ejecutando mediante la orden siguiente

```
$/etc/init.d/asterisk status
```

Una vez verificado que el servidor Asterisk se encuentra funcionando correctamente integramos al servidor LDAP un schema propio de Asterisk a la carpeta `/etc/ldap/schema/`

```
$cd /usr/src/asterisk-10.9.0/contrib/scripts/  
$/etc/init.d/slapd stop  
$sudo cp asterisk.ldap-schema /etc/ldap/schema/asterisk.schema  
$sudo ldapadd -Y EXTERNAL -H ldapi:/// -f asterisk.ldif  
$/etc/init.d/slapd restart  
$/etc/init.d/asterisk restart
```

Finalmente se procedió a editar algunos archivos para entrelazar Asterisk con LDAP

```
- $nano /etc/asterisk/res_ldap.conf
```

```
[_general]  
url=ldap://localhost  
protocol=3  
basedn=dc=unanleon,dc= edu,dc=ni  
user=cn=admin,dc=unanleon,dc= edu,dc=ni  
pass=*****
```

```
- $nano /etc/asterisk/extconfig.conf
```

```
[settings]
```

```
sipusers=>ldap,"dc=unanleon,dc= edu,dc=ni ",sip
sippeers=>ldap,"dc=unanleon,dc= edu,dc=ni ",sip
extensions=>ldap,"dc=unanleon,dc= edu,dc=ni ",extensions
```

- **\$nano /etc/asterisk/extensions.conf**

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
priorityjumping=no

[globals]
[users]

exten => 2000,1,Dial(SIP/mfernandez,20)
exten => 2000,n,VoiceMail(2000@default)
exten => 2001,1,Dial(SIP/yurbina,20)
exten => 2001,n,VoiceMail(2001@default)
exten => 4000,1,Dial(SIP/amartinez,20)
exten => 4000,n,VoiceMail(4000@default)
exten => 4001,1,Dial(SIP/scenteno,20)
exten => 4001,n,VoiceMail(4001@default)
include => aplicaciones

[aplicaciones]
exten => 9999,1,Answer()
exten => 9999,n,Playback(es/hello-world)
exten => 9999,n,Hangup()
exten => 9500,1,Answer()
exten => 9500,n,VoiceMailMain(@default)
```

- **\$nano /etc/asterisk/sip.conf**

```
[general]
videosupport=yes
allow=all
udpbindaddr=0.0.0.0
realm=unanleon.edu.ni
context=default
allowguest=no
allowoverlap=no
srvlookup=yes
transport=yes

[mfernandez]
type=friend
secret=123456
host=dynamic
insecure=port,invite
context=users
mailbox=2000@default

[yurbina]
type=friend
secret=123456
host=dynamic
insecure=port,invite
context=users
mailbox=2001@default
```

```
[amartinez]
type=friend
secret=123456
host=dynamic
insecure=port,invite
context=users
mailbox=4000@default
```

```
[scenteno]
type=friend
secret=123456
host=dynamic
insecure=port,invite
context=users
mailbox=4001@default
```

- **\$nano /etc/asterisk/voicemail.conf**

```
[default]
2000 => 2000,Merling Fernandez,mfernandez@unanleon.edu.ni
2001 => 2001,Yuriette Urbina,yurbina@unanleon.edu.ni
4000 => 4000,Antonio Martinez,amartinez@unanleon.edu.ni
4001 => 4001,Sandra Centeno,scenteno@unanleon.edu.ni
```

Se ingresa en la CLI de Asterisk para reiniciar los servicios

```
$ asterisk -rvvv
$ sip reload
$ dialplan reload
```

Se verifica si el módulo de LDAP está habilitado en Asterisk

```
unanleon*CLI> module show like ldap
Module      Description      Use Count
res_config_ldap.so  LDAP realtime interface  0
1 modules loaded
unanleon*CLI> █
```

Figura 10. Verificación de Modulo LDAP cargado en Asterisk

Luego verificamos si Asterisk se encuentra conectado al servidor LDAP

```
unanleon*CLI> realtime show ldap status
Connected to 'ldap://localhost', baseDN dc=unanleon,dc=com with username
cn=admin,dc=unanleon,dc=com for 16 minutes, 8 seconds.
unanleon*CLI> █
```

Figura 11. Verificación de funcionalidad de LDAP con Asterisk

Una vez finalizadas las configuraciones anteriores y creadas las extensiones de los usuarios, la central telefónica Asterisk se encuentra funcional y conectada con LDAP, posteriormente se procedió a instalar un softphone para la comunicación entre las extensiones creadas anteriormente, el software que se eligió para realizar la comprobación es Zoiper el cual funciona perfectamente tanto en Windows como Linux, su configuración puede observarse en los [Anexos](#).

Instalación de Moodle 2.4.2 y Autenticación LDAP

Para iniciar la instalación de nuestro Sistema de Gestión de Cursos de Código Abierto conocido también como Entorno de Aprendizaje Virtual "Moodle", se procedió a descargar desde su página web <http://download.moodle.org/> el programa Moodle en esta ocasión se descargó la versión 2.4.2 a continuación realizaremos los siguientes ajustes para su correcto funcionamiento en nuestro sistema:

1. Se inicia con descomprimir el archivo y lo moveremos a la carpeta /var/www/moodle

```
$tar -xf moodle-2.4.2.tgz
$mv moodle /var/www/moodle
```

2. Crearemos la carpeta moodledata, posteriormente especificamos al grupo "www-data" como grupo propietario cambiando los permisos de la carpeta a 770 para que únicamente tengan acceso el usuario administrador y grupo propietario por medio de los comandos siguientes:

```
$cd /var
$mkdir moodledata
$chgrp www-data moodledata
$chmod 770 moodledata
```

3. Se procedió a abrir una página en el navegador para la instalación y se digito <http://localhost/moodle> seguimos el asistente en donde seleccionaremos lo siguiente:

- Selección de Idioma para este ensayo Español internacional
- Se indica la dirección web para acceder moodle (<http://localhost/moodle>), la ruta completa del directorio de instalación (/var/www/moodle) y el directorio de datos para que moodle pueda guardar los archivos subidos (/var/moodledata)
- Seleccionamos el servidor de bases de datos (en este caso Mysql)

4. Se configuran los ajustes de la base de datos

- Servidor de la base de datos (localhost)
- Nombre de la base de datos (moodle)
- Usuario de la base de datos (root)
- Contraseña de la base de datos (password del usuario root)

5. Aparecerá un mensaje en el cual Moodle ha generado su fichero de configuración pero que no ha podido crearlo automáticamente en el sistema así que se debió de copiar el código brindado y crear el archivo en la ruta /var/www/moodle/config.php y colocar lo siguiente:

Configuración finalizada

Moodle ha creado su fichero de configuración.

El script de instalación no ha podido crear automáticamente un archivo config.php con las especificaciones elegidas. Por favor, copie el siguiente código en un archivo llamado config.php y coloque ese archivo en el directorio raíz de Moodle.

```
<?php // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype      = 'mysqli';
$CFG->dblibrary   = 'native';
$CFG->dbhost      = 'localhost';
$CFG->dbname      = 'moodle';
$CFG->dbuser      = 'root';
$CFG->dbpass      = 'erwin';
$CFG->prefix      = 'mdl_';
$CFG->dboptions   = array (
    'dbpersist' => 0,
    'dbsocket'  => 0,
);

$CFG->wwwroot     = 'http://192.168.56.101/moodle';
$CFG->dataroot    = '/var/moodledata';
$CFG->admin       = 'admin';

$CFG->directorypermissions = 0777;

$CFG->passwordsaltmain = '_>_N)c4my=.H@hFq@FM6MT>sV2e';

require_once(dirname(__FILE__) . '/lib/setup.php');

// There is no php closing tag in this file,
// it is intentional because it prevents trailing whitespace problems!
```

« Anterior Siguiente »

Figura 12. Código de Configuración de Moodle

6. Una vez creado el script anterior se dio clic en continuar en la ventana del navegador donde se está realizando la instalación, tras completarse el proceso se ingresaron los datos del sitio de administración de moodle los cuales son los siguientes:

- Nombre del usuario administrador (admin)
- Contraseña del administrador (#####)
- Nombre del administrador
- Apellido del administrador
- Dirección de correo electrónico
- Ciudad
- País

Guardar Cambios

7. Finalizado esto se ingresa al sitio de administración posteriormente en Ajustes -> Editar Ajustes -> Extensiones -> Identificación.

Se habilita la opción Usar un Servidor LDAP haciendo clic en Gestión de Identificación y con la flecha se le da clic para que al momento de ingresar algún usuario este se verifique primeramente en el servidor LDAP.

8. Los datos a ingresar para la autenticación de Moodle contra el servidor LDAP fueron los siguientes:

- Url del host (localhost)
- Version (3)
- codificación LDAP (utf-8)

En Fijar Ajustes

- Ocultar Constraseñas (si)
- Nombre Distinguido (cn=admin, dc=unanleon, dc=edu,dc=ni)
- Contraseña del usuario administrador de LDAP (*****)

Ajustes de búsqueda de Usuario

- Tipo de Usuario (posixAccount (rfc2307))
- Contextos (ou=personal, dc=unanleon, dc= edu,dc=ni)
- Buscar subcontextos (Si)
- Desreferenciar los alias (si)

Guardar cambios y proceder a verificar a los usuarios.

Página de Administración Principal de Moodle

The screenshot displays the Moodle administrator interface. At the top, it says 'Entorno de Aprendizaje Virtual Unan-Leon' and 'Usted se ha identificado como Antonio Gutierrez (Salir)'. The language is set to 'Español - Internacional (es)'. The main content area shows 'Cursos disponibles' with a single course listed: 'Diseño y Configuración de Módulos LDAP'. On the left, there are navigation and settings menus. The calendar on the right shows the month of March 2013.

Dom	Lun	Mar	Mié	Jue	Vie	Sáb
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Figura 13. Página Principal del Administrador

Instalación del Servidor de Correo y Autenticación LDAP

Para la instalación de nuestro servidor de correo iniciamos con la instalación del agente de transferencia de correo SMTP predeterminado Postfix el cual nos permitirá transferir y enrutar correo electrónico:

```
$sudo apt-get install postfix postfix-doc postfix-ldap libsasl2-2 sasl2-bin libsasl2-modules
```

Luego de la instalación procedemos a configurar el servidor ejecutando el comando siguiente `dpkg-reconfigure postfix` el cual nos mostrara en pantalla el asistente de configuración de Postfix en nuestro sistema colocamos las opciones siguientes:

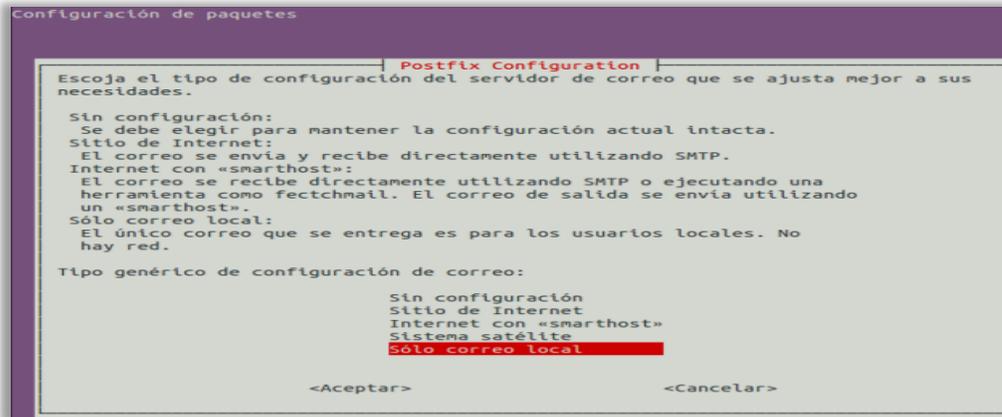


Figura 14. Asignación de Correo Local

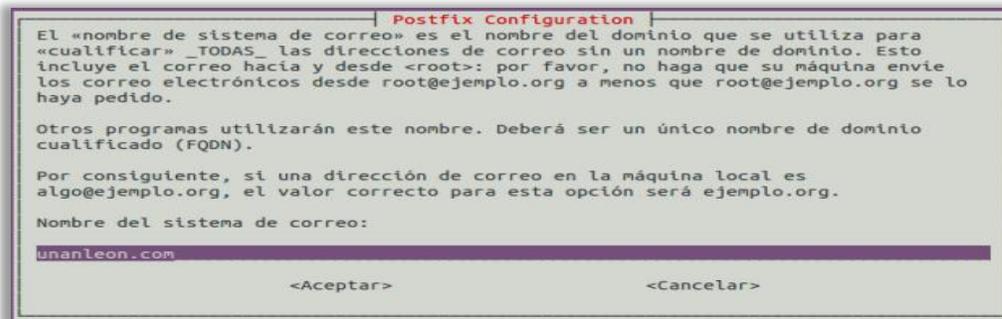


Figura 15. Asignación de Nombre del Correo

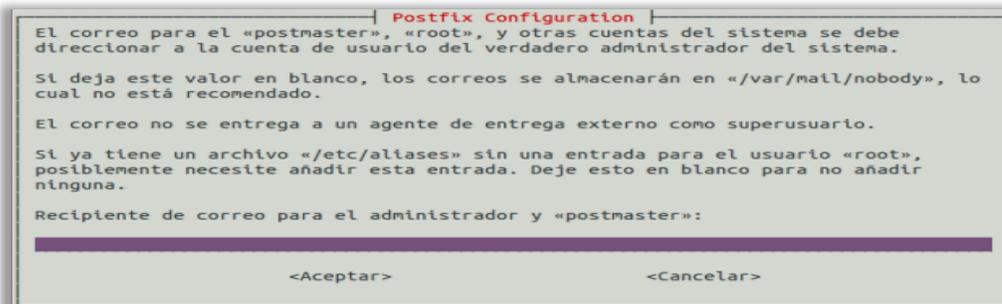


Figura 16. Configuración de Recipiente de Correo

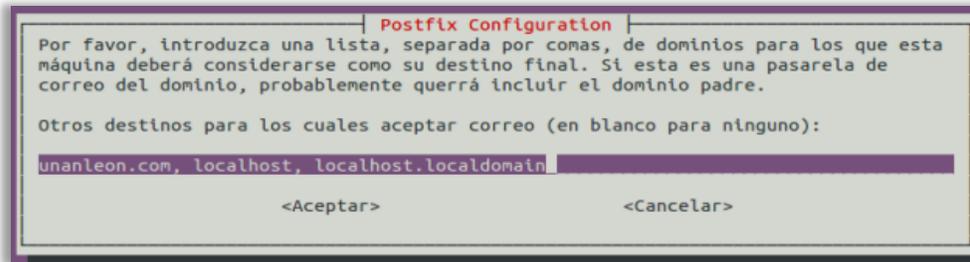


Figura 17. Asignación de Dominios de Correo

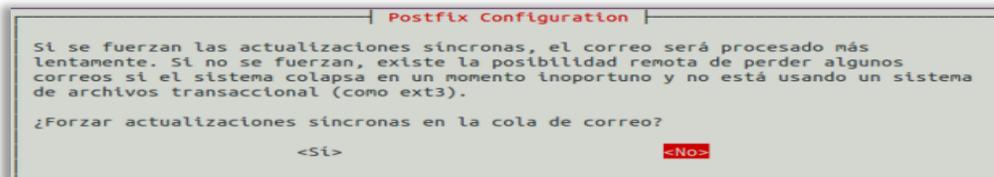


Figura 18. Modo de Actualización de Correo

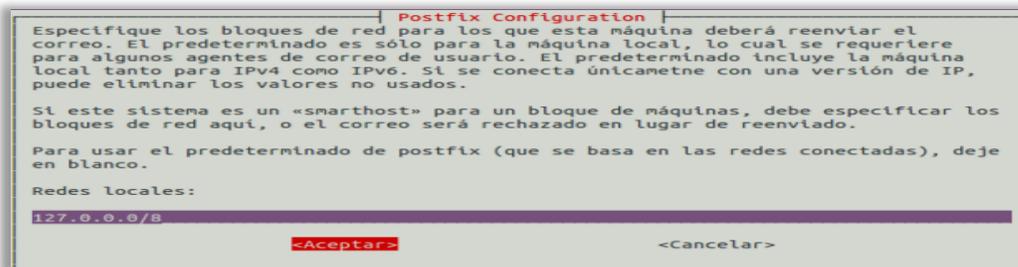


Figura 19. Asignación de Redes de Acceso del Correo

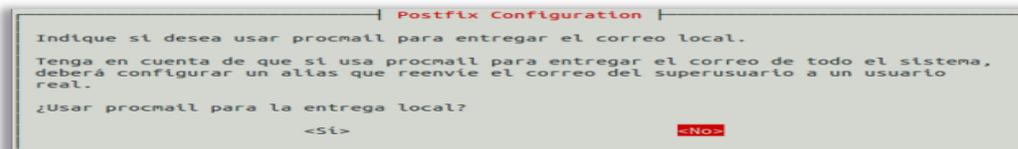


Figura 20. Configuración del Modo de Entrega del Correo

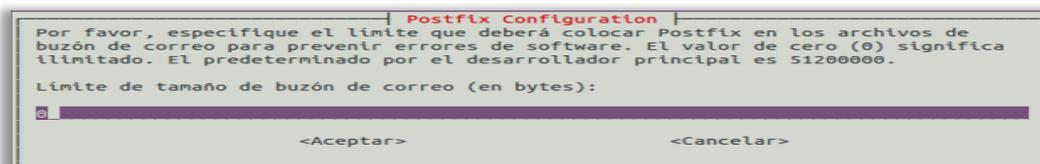


Figura 21. Asignación del tamaño del buzón de correo

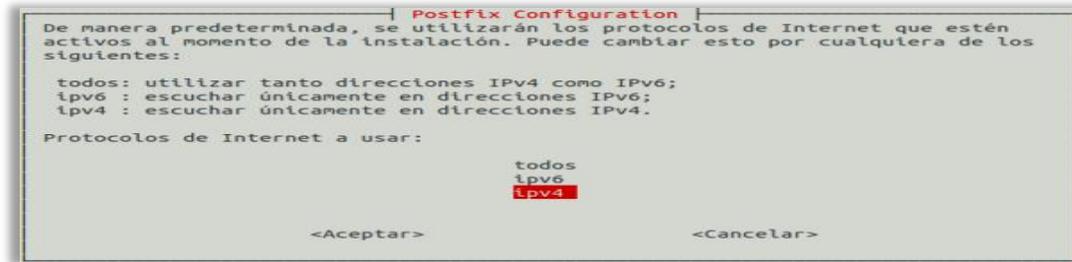


Figura 22. Establecimiento de Protocolo a utilizar

Procedemos a configurar el formato de buzón de correo de Postfix con ayuda del comando `$sudo postconf -e 'home_mailbox = Maildir/'`

Y con el siguiente comando colocamos el correo Nuevo en la carpeta del usuario correspondiente `$sudo postconf -e 'mailbox_command ='` y luego configuramos el agente de entrega de correo para que utilice la misma ruta

```
$sudo postconf -e 'smtpd_sasl_local_domain ='
$sudo postconf -e 'smtpd_sasl_auth_enable = yes'
$sudo postconf -e 'smtpd_sasl_security_options = noanonymous'
$sudo postconf -e 'broken_sasl_auth_clients = yes'
$sudo postconf -e 'smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination'
$sudo postconf -e 'inet_interfaces = loopback-only'
```

Verificamos que el código de Postfix sea el correcto (Este es el archivo `/etc/postfix/main.cf`)

```
smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
biff = no
append_dot_mydomain = no

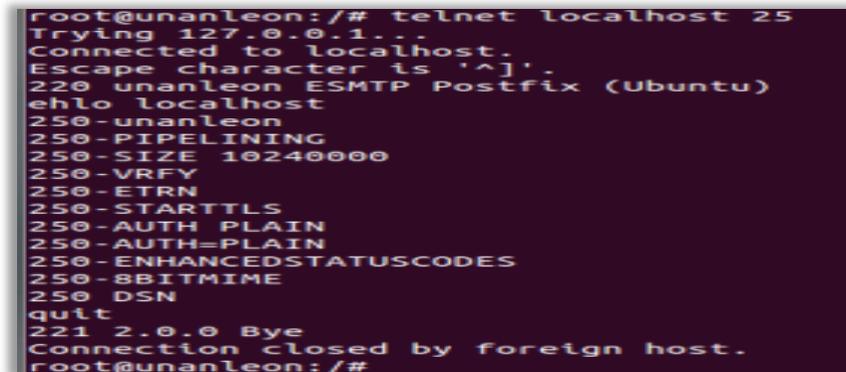
readme_directory = /usr/share/doc/postfix

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

myhostname = unanleon
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = unanleon.edu.ni, unanleon, localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
home_mailbox = Maildir/
mailbox_command =
smtpd_sasl_local_domain =
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination
inet_protocols = ipv4
```

```
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth-client
```

A continuación se procede a realizar prueba de funcionamiento la cual resultado satisfactoria



```
root@unanleon:/# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 unanleon ESMTP Postfix (Ubuntu)
ehlo localhost
250-unanleon
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN
250-AUTH=PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
quit
221 2.0.0 Bye
Connection closed by foreign host.
root@unanleon:/#
```

Figura 23. Prueba de Funcionamiento de servicio SMTP

Se inicia la instalación Dovecot el cual es el servidor IMAP y POP3 con el comando siguiente:

```
$sudo apt-get install dovecot-common dovecot-ldap dovecot-pop3d dovecot-imapd dovecot-core
```

Y configuramos el archivo `/etc/dovecot/dovecot.conf` colocando lo siguiente

```
listen = *
protocols = imap pop3 imaps pop3s
disable_plaintext_auth = no
log_timestamp = "%Y-%m-%d %H:%M:%S "
ssl_cert_file = /etc/ssl/certs/dovecot.pem
ssl_key_file = /etc/ssl/private/dovecot.pem
mail_location = maildir:~/Maildir
mail_debug = yes
mail_privileged_group = mail

protocol lda {
    postmaster_address = ervin@unanleon.edu.ni
    hostname = unanleon.com
    auth_socket_path = /var/run/dovecot/auth-master
}

auth default {
    mechanisms = plain login

passdb ldap {
    args = /etc/dovecot/dovecot-ldap.conf
}

userdb ldap {
    args = /etc/dovecot/dovecot-ldap.conf
}

user = root
socket listen {
    client {
        path = /var/spool/postfix/private/auth-client
        mode = 0660
        user = postfix
        group = postfix
    }
}
```

```
}  
login_greeting = Dovecot ready
```

Seguidamente se configuro el archivo /etc/dovecot/dovecot-ldap.conf

```
hosts = 127.0.0.1  
uris = ldap://localhost  
dn = cn=admin,dc=unanleon,dc=edu,dc=ni  
dnpass = ervin  
auth_bind = yes  
ldap_version = 3  
base = dc=unanleon,dc=edu,dc=ni  
user_attrs = homeDirectory=home,uidNumber=uid,gidNumber=gid  
user_filter = (&(objectClass=posixAccount)(uid=%u))  
pass_attrs = uid=user,userPassword=password  
pass_filter = (&(objectClass=posixAccount)(uid=%u))  
default_pass_scheme = MD5
```

Se procedió a reiniciar tanto postfix como dovecot y se realizan pruebas de verificación resultando exitosas:

```
root@unanleon:/# telnet localhost 110  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^]'.  
+OK Dovecot ready.  
quit  
+OK Logging out  
Connection closed by foreign host.  
root@unanleon:/#
```

Figura 24. Comprobación del Funcionamiento del servicio POP3

```
root@unanleon:/# telnet localhost 143  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^]'.  
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=PLAIN] Dovecot ready.
```

Figura 25. Comprobación del Funcionamiento del Servicio IMAP

Procedimos a instalar una interfaz gráfica o webmail para verificar las cuentas de correo cuya aplicación seleccionada fue squirrelmail, la instalación se realizó con los comandos siguientes

```
$sudo apt-get install squirrelmail squirrelmail-locales squirrelmail-viewashtml
```

Una vez instalado se configuro lo siguiente con el comando `$squirrelmail-configure`
El nombre de la organización

```
SquirrelMail Configuration : Read: config.php (1.4.0)  
-----  
Organization Preferences  
1. Organization Name      : Simulacion de Sistema de Correo Unan-Leon  
2. Organization Logo     : ../images/sm_logo.png  
3. Org. Logo Width/Height : (308/111)  
4. Organization Title    : SquirrelMail $version  
5. Signout Page          :  
6. Top Frame             : _top  
7. Provider link         : http://squirrelmail.org/  
8. Provider name         : SquirrelMail  
  
R Return to Main Menu  
C Turn color on  
S Save data  
Q Quit  
Command >>
```

Figura 26. Configuración del Nombre de la Organización en Squirrelmail

```

SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Server Settings
General
-----
1. Domain                : unanleon.edu.mx
2. Invert Time           : false
3. Sendmail or SMTP     : SMTP

A. Update IMAP Settings : localhost:143 (dovecot)
B. Update SMTP Settings : localhost:25

R Return to Main Menu
C Turn color on
S Save data
Q Quit

Command >>

```

Figura 27. Asignación del Dominio del Servidor de Correo

```

SquirrelMail Configuration : Read: config.php
-----
While we have been building SquirrelMail, we have discovered some
preferences that work better with some servers that don't work so
well with others.  If you select your IMAP server, this option will
set some pre-defined settings for that server.

Please note that you will still need to go through and make sure
everything is correct.  This does not change everything.  There are
only a few settings that this will change.

Please select your IMAP server:
bincimap    = Binc IMAP server
courier     = Courier IMAP server
cyrus       = Cyrus IMAP server
dovecot     = Dovecot Secure IMAP server
exchange    = Microsoft Exchange IMAP server
hmailserver = hMailServer
macosx      = Mac OS X Mailserver
mercury32   = Mercury/32
uw          = University of Washington's IMAP server
gmail       = IMAP access to Google mail (Gmail) accounts

quit        = Do not change anything
Command >> dovecot

```

Figura 28. Selección del Servidor IMAP a utilizar

Se crea un enlace simbólico de squirrelmail al directorio DocumentRoot de apache, es decir, en este caso, /var/www. Con eso conseguiremos poder acceder a squirrelmail de forma sencilla.

```
$sudo ln -s /usr/share/squirrelmail/ /var/www/webmail
```

Posteriormente se accede al webmail digitando la dirección <http://localhost/webmail> o <http://unanleon.com/webmail>



Figura 29. Comprobación del Webmail en el dominio preestablecido

Para verificar si todo funciona correctamente con el correo se puede ingresar a <http://localhost/webmail/src/configtest.php> donde se realiza un test de verificación de php, apache, smtp, pop3 e imap, en donde se mostrara un mensaje como el siguiente indicando que squirrelmail se encuentra bien configurado.

```
SquirrelMail configtest

This script will try to check some aspects of your SquirrelMail configuration and point you to errors wherever it can find them. You need to go run conf.pl in the config/ directory first before you run this script.

SquirrelMail version: 1.4.22
Config file version: 1.4.0
Config file last modified: 08 February 2013 23:07:02

Checking PHP configuration...
  PHP version 5.3.10-1ubuntu3.4 OK.
  Running as www-data(33) / www-data(33)
  display_errors:
  error_reporting: 22527
  variables_order OK: GPCS.
  PHP extensions OK. Dynamic loading is disabled.
Checking paths...
  Data dir OK.
  Attachment dir OK.
  Plugins OK.
  Themes OK.
  Default language OK.
  Base URL detected as: http://192.168.0.12/webmail/src (location base autodetected)
Checking outgoing mail service...
  SMTP server OK (220 unanison ESMTP Postfix (Ubuntu))
Checking IMAP service...
  IMAP server ready (+ OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=PLAIN] Dovecot ready.)
  Capabilities: + CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS AUTH=PLAIN
Checking internationalization (i18n) settings...
  gettext - Gettext functions are available. On some systems you must have appropriate system locales compiled.
  mbstring - Mbstring functions are available.
  recode - Recode functions are unavailable.
  iconv - Iconv functions are available.
  timezone - Webmail users can change their time zone settings.
Checking database functions...
  not using database functionality.

Congratulations, your SquirrelMail setup looks fine to me!
```

Figura 30. Comprobación de Funcionamiento de Squirrelmail

Instalación de VSFTPD y Autenticación LDAP

Para la instalación del paquete de servidor Vsftpd y autenticarlo con nuestro servidor Ldap primeramente instalamos y configuramos correctamente nuestro servidor Ldap (realizado anteriormente) y luego instalar vsftpd de la siguiente manera:

```
$apt-get install vsftpd
$service vsftpd start
```

Para configurar algunos ajustes del vsftpd se procedió a detener el servidor y luego editar el archivo /etc/vsftpd.conf

```
$service vsftpd stop
```

Configuraciones Generales

```
#!/bin/bash
# Ejemplo del archivo de configuración /etc/vsftpd.conf
# General Settings
listen=YES
# Permite el modo escritura.
write_enable=YES
# Activa mensajes de directorio.
dirmessage_enable=YES
# Mensaje de bienvenida
ftpd_banner=Bienvenido al Servidor ftp de la Unan-Leon
# Local FTP user Settings
# Permitir conexiones anónimas.
anonymous_enable=YES
# Permite que usuarios locales puedan conectarse.
local_enable=YES
# Activa la generación de registros logs por cada uploads/downloads.
xferlog_enable=YES
# (ftp-data).
connect_from_port_20=YES
```

Se habilito el servidor con el comando `$service vsftpd restart` y realizamos una prueba de funcionamiento con un usuario del servidor Ldap por consola y vía web.



```
root@unanleon:/# ftp localhost
Connected to localhost.
220 Bienvenidos al Servidor de Archivos de la Unanleon
Name (localhost:ervin): yurbina
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwx-----  8 2001    500    4096 Feb 16 00:28 Mail
drwx-----  5 2001    500    4096 Feb 16 00:27 Maildir
-rw-r--r--   1 2001    500    8445 Feb 04 20:21 examples.desktop
226 Directory send OK.
ftp> █
```

Figura 31. Verificación de Funcionalidad de FTP con LDAP desde Consola

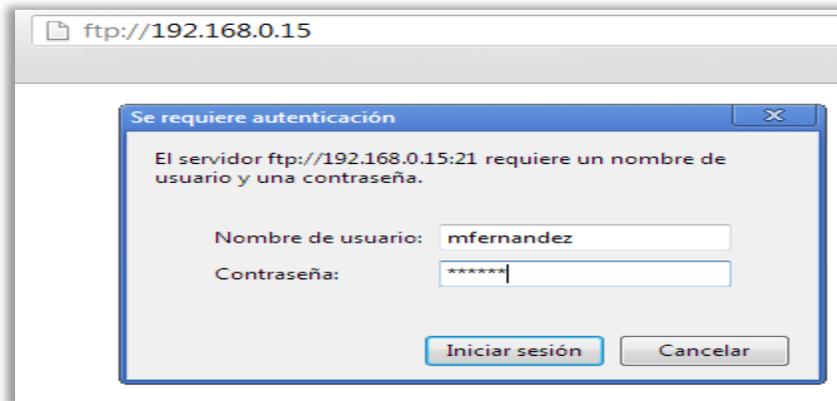


Figura 32. Verificación de Funcionamiento de FTP con LDAP desde el Navegador



Figura 33. Comprobación de Acceso a los Archivos del Usuario mediante FTP

Instalación del Portal Cautivo en Máquina Virtual

Para el proceso de instalación del Portal Cautivo se procedió a descargar el programa PFSense desde la página oficial <http://www.pfsense.org/> y descargamos la versión pfSense-LiveCD-2.0.2-RELEASE-i386, una vez instalada configuramos la red desde la consola para tener acceso desde el navegador seguido se instalaron los paquetes siguientes:

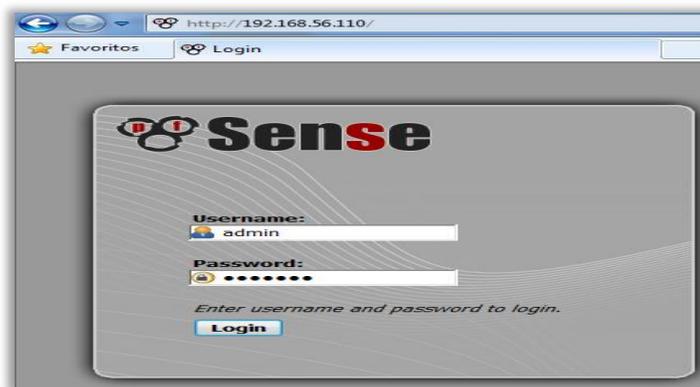


Figura 34. Acceso al Portal Cautivo desde el Navegador

System: Package Manager

Available Packages | Installed Packages

Package Name	Category	Package Info	Package Version	Description
freeradius2	System	Package Info	2.1.12_1 pkg v1.6.6_4	A free implementation of the RADIUS protocol. Support: MySQL, PostgreSQL, LDAP, Kerberos. FreeRADIUS and FreeRADIUS2 settings are not compatible so don't use them together or try to update. On pfSense docs there is a how-to which could help you on porting users.
squid	Network	No info, check the forum	2.7.9 pkg v.4.3.3	High performance web proxy cache.

Figura 35. Comprobación de Paquetes instalados

Services: DNS forwarder

General DNS Forwarder Options

Enable Enable DNS forwarder

DHCP Registration Register DHCP leases in DNS forwarder

If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

Figura 36. Activación del Registro DHCP

LAN

Enable DHCP server on LAN interface

Deny unknown clients
If this is checked, only the clients defined below will get DHCP leases from this server.

Subnet 192.168.56.0

Subnet mask 255.255.255.0

Available range 192.168.56.1 - 192.168.56.254

Range to

WINS servers

DNS servers

NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS forwarder is enabled, otherwise the servers configured on the General page.

Gateway

The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network.

Domain name

The default is to use the domain name of this system as the default domain name provided by DHCP. You may specify an alternate domain name here.

Domain search list

The DHCP server can optionally provide a domain search list.

Figura 37. Configuración del Servidor DHCP en Red LAN

Configuración del Servidor Freeradius para Autenticar contra LDAP

Primeramente se procedió a configurar pfsense para que se pueda autenticar contra el servidor ldap ingresando los siguientes datos

FreeRADIUS: LDAP

Users | MACs | NAS / Clients | **Interfaces** | Settings | EAP | SQL | Certificates | **LDAP** | View config | XMLRPC Sync

ENABLE LDAP SUPPORT - SERVER 1

Enable LDAP For Authorization
This enables LDAP in authorize section. The ldap module will set Auth-Type to LDAP if it has not already been set. (Default: unchecked)

Enable LDAP For Authentication
This enables LDAP in authenticate section. Note that this means "check plain-text password against the ldap database", which means that EAP won't work, as it does not supply a plain-text password.

GENERAL CONFIGURATION - SERVER 1

Server
No description. (Default: ldap.your.domain)

Identity
No description. (Default: cn=admin,o=My Org,c=UA)

Password
No description. (Default: mypass)

Basedn
No description. (Default: o=My Org,c=UA)

Figura 38. Configuración de Freeradius contra LDAP

Se habilitan 2 interfaces: 1 para autenticación y otra para la contabilidad de los usuarios del sistema

FreeRADIUS: Interfaces

Users | MACs | NAS / Clients | **Interfaces** | Settings | EAP | SQL | Certificates | LDAP | View config | XMLRPC Sync

Interface IP Address	Port	Interface Type	IP Version	Description
*	1812	auth	ipaddr	
*	1813	acct	ipaddr	

Figura 39. Habilitación de Interfaces

Se configura un cliente y usuario genérico para el servidor Freeradius

FreeRADIUS: Clients

Users | MACs | **NAS / Clients** | Interfaces | Settings | EAP | SQL | Certificates | LDAP | View config | XMLRPC Sync

Client IP Address	Client IP Version	Client Shortname	Client Protocol	Client Type	Require Message Authenticator	Max Connections	Description
192.168.56.110	ipaddr	captiveportal	udp	other	no	16	

Figura 40. Habilitación de Cliente genérico para Freeradius

FreeRADIUS: Users

Users | MACs | NAS / Clients | Interfaces | Settings | EAP | SQL | Certificates | LDAP | View config | XMLRPC Sync

Filter by: A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Filter field: Username Filter text: Filter

Username	Use One Time Password	Simult. Connections	IP Address	Expiration Date	Session Timeout	Possible Login Times	VLAN ID	Description
internet								

Figura 41. Habilitación de Usuario genérico para Freeradius

Activación y Configuración del Portal Cautivo en Red Local

Services: Captive portal

Captive portal | Pass-through MAC | Allowed IP addresses | Allowed Hostnames | Vouchers | File Manager

Enable captive portal

Interfaces: WAN, LAN

Select the interface(s) to enable for captive portal.

Figura 42. Habilitación del Portal Cautivo

Authentication

No Authentication
 Local User Manager / Vouchers
 RADIUS Authentication

Primary RADIUS server

IP address: 192.168.56.110
Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.

Port:
Leave this field blank to use the default port (1812).

Shared secret: 123
Leave this field blank to not use a RADIUS shared secret (not recommended).

Figura 43. Autenticar Portal Cautivo con el Servidor Radius

Accounting

send RADIUS accounting packets
If this is enabled, RADIUS accounting packets will be sent to the primary RADIUS server.

Figura 44. Activar el envío de paquetes Radius para Contabilidad de Usuarios

RADIUS options

RADIUS NAS IP attribute: LAN - 192.168.56.110
Choose the IP to use for calling station attribute.

Figura 45. Selección de Red donde se ejecuta el servidor Radius

Finalmente se verifica que los servicios estén ejecutándose correctamente y realizamos la prueba de funcionamiento.

Status: Services

Service	Description	Status
captiveportal	Captive Portal	Running
dnsmasq	DNS Forwarder	Running
ntpd	NTP clock sync	Running
radiusd	FreeRADIUS Server	Running
squid	Proxy server Service	Running

Figura 46. Comprobación de Servicios Activos



Figura 47. Comprobación de Funcionamiento del Portal Cautivo desde Máquina Cliente

Status: Dashboard

System Information

Name	pfSense.localdomain
Version	2.0.2-RELEASE (I386) built on Fri Dec 7 16:30:14 EST 2012 FreeBSD 8.1-RELEASE-p13 You are on the latest version.
Platform	pfSense
CPU Type	AMD A6-3400M APU with Radeon(tm) HD Graphics
Uptime	00:26
Current date/time	Wed Mar 13 10:02:27 CST 2013
DNS server(s)	127.0.0.1 192.136.45.66 200.85.160.4 200.85.160.2

Interfaces

WAN (DHCP)	↑	192.168.0.13	1000baseT <full-duplex>
LAN	↑	192.168.56.110	1000baseT <full-duplex>

Captive Portal Status

IP address	MAC address	Username
192.168.56.10	08:00:27:62:3b:e5	mfernandez

Figura 48. Acceso de Usuario LDAP al Portal Cautivo

Conclusiones

A lo largo de este documento se presentó un estudio de las tecnologías necesarias para crear una alternativa al modo de funcionamiento de los servicios que ofrece la Unan-León. También se describen los detalles para su implementación como solución informática a esos problemas. A continuación se presentan las conclusiones de este proyecto.

- Globalmente se pueden señalar como ventajas de la integración desarrollada el hecho de estar basada en software libre, que facilita un bajo coste de desarrollo, así como la utilización de tecnología VoIP para las comunicaciones, que aprovecha excedentes en la red de datos evitando costes adicionales en líneas telefónicas dedicadas.
- Utilizando herramientas de software libre fue posible construir un prototipo del modelo de infraestructura utilizado por la Unan-León, eliminando de esta manera la redundancia de datos de los usuarios, ahorro de recursos en infraestructura (otros equipos servidor) y simplificar la administración de la red. A su vez ofrece a los usuarios múltiples formas de conectarse a los servicios, a través de las mismas credenciales.
- El uso de protocolos libres permite que la infraestructura que se utiliza para la implementación, pueda ser usada simultáneamente por otros servicios que requieren de autenticación, disminuyendo el costo total de propiedad de la infraestructura de red al no duplicar servicios de autenticación.

En resumen, integrar un sistema de servicios de red y un directorio de usuarios tiene un importante interés comercial, más aun tratándose de la mejora de un producto ya comercializado en el mercado, para el cual se introduce la posibilidad de gestionar la autenticación mediante directorio LDAP.

Recomendaciones

En el actual proyecto se consideró un sistema automático de creación de cuentas, que ayuda en forma considerable a la administración.

Asimismo se pensó necesaria la creación de la Interfaz de administración Web de Asterisk para que resulte más cómoda la creación o modificación de extensiones VoIP, asignación y restricción de permisos a determinados usuarios.

Además se puede implementar un servidor Samba para compartir uno o más archivos entre usuarios Windows y Linux, Cups para instalar un sistema de impresión ya sea a nivel Administrativo o Docente y una VPN para que un mismo usuario pueda acceder a internet desde diversas facultades donde se encuentre con sus mismas credenciales.

Se recomienda la realización de un sistema de seguridad para evitar que otros usuarios utilicen cuentas no asignadas.

Una posible evolución a este proyecto sería realizar un producto nuevo que considerase como base de autenticación un directorio LDAP existente, en lugar de reutilizar un desarrollo existente en el que se paralelice el uso de una base de datos local con el directorio externo.

Referencias Bibliográficas

Instalación y Configuración del Servidor Ubuntu 12.04

http://doc.ubuntu-es.org/12.04:Instalaci%C3%B3n_est%C3%A1ndar

<http://www.ubuntu-guia.com/2012/04/cosas-que-hacer-despues-de-instalar.html>

Instalación y Configuración del Servidor OpenLdap

<https://help.ubuntu.com/12.04/serverguide/openldap-server.html>

<https://help.ubuntu.com/12.04/serverguide/openldap-server.html>

<https://help.ubuntu.com/community/LDAPClientAuthentication>

Instalación y Configuración del Servidor Asterisk

<http://www.tribulinux.com/como-instalar-asterisk-10-en-ubuntu-12-04.html>

http://www.asteriskdocs.org/en/3rd_Edition/asterisk-book-htmlhunk/ExternalServices_id291590.html

<http://www.esdebian.org/wiki/realtime-ldap-asterisk-16>

Instalación y Configuración del Servidor Moodle

<http://echaleunvistazo.wordpress.com/2012/09/20/servidor-web-con-moodle-instalacion/>

http://docs.moodle.org/24/en/LDAP_authentication

Instalación y Configuración del Servidor Correo

<http://pedroreina.net/recetas/squirrelmail.html>

<http://wiki.dovecot.org/HowTo/DovecotOpenLdap>

<https://help.ubuntu.com/community/Dovecot?highlight=%28%28DovecotLDAP%29%29>

<https://help.ubuntu.com/12.04/serverguide/postfix.html#postfix-smtp-authentication>

Instalación y Configuración del Servidor VSFTPD

<http://linux-ubuntu1104.blogspot.com/2012/02/ubuntUvsftp-con-autenticacion-local-y.html>

<http://www.forosuse.org/forosuse/showthread.php?t=16557&highlight=vsftpd>

Instalación y Configuración de Portal Cautivo

<http://www.javcasta.com/2011/06/18/freebsd-firewall-portal-cautivo-con-pfsense/>

<http://forum.pfsense.org/index.php/topic,25576.msg133719.html>

<http://www.youtube.com/watch?v=B6Hjxd1Af-s>

http://www.bellera.cat/josep/pfsense/index_cs.htm

Anexos

Estructura LDAP código implementado:

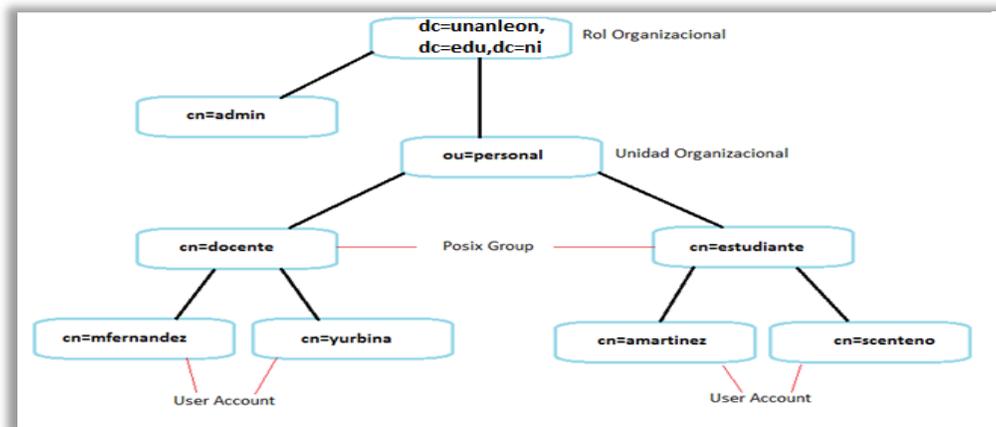


Figura 49. Esquema LDAP

```
dn: dc=unanleon,dc=edu,ni
cn=admin,dc=unanleon, dc=edu,dc=ni
dc: unanleon
o: unanleon.com
objectclass: top
objectclass: dcObject
objectclass: organization
structuralobjectclass: organization
```

```
dn: cn=admin,dc=unanleon,dc=edu,dc=ni
cn: admin
cn=admin,dc=unanleon, dc=edu,dc=ni
objectclass: organizationalRole
structuralobjectclass: organizationalRole
```

```
dn: ou=personal,dc=unanleon, dc=edu,dc=ni
ou=personal,dc=unanleon, dc=edu,dc=ni
objectclass: organizationalUnit
objectclass: top
ou: personal
structuralobjectclass: organizationalUnit
```

```
dn: cn=docente,ou=personal,dc=unanleon, dc=edu,dc=ni
cn: docente
cn=docente,ou=personal,dc=unanleon, dc=edu,dc=ni
objectclass: posixGroup
objectclass: top
structuralobjectclass: posixGroup
```

```
dn: cn=merling fernandez,cn=docente,ou=personal,dc=unanleon, dc=edu,dc=ni
cn: merling fernandez
gidnumber: 500
givenname: merling
homedirectory: /home/personal/docente/mfernandez
loginshell: /bin/sh
mail: mfernandez@unanleon.edu.ni
objectclass: inetOrgPerson
objectclass: posixAccount
```

objectclass: top
sn: fernandez
structuralobjectclass: inetOrgPerson
uid: mfernandez
uidnumber: 2000
userpassword: {MD5}4QrcOUm6Wau+VuBX8g+IPg==

dn: cn=yuriette urbina,cn=docente,ou=personal,dc=unanleon, dc=edu,dc=ni
cn: yuriette urbina
gidnumber: 500
givenname: yuriette
homedirectory: /home/personal/docente/yurbina
loginshell: /bin/sh
mail: yurbina@unanleon. edu.ni
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
sn: urbina
structuralobjectclass: inetOrgPerson
uid: yurbina
uidnumber: 2001
userpassword: {MD5}4QrcOUm6Wau+VuBX8g+IPg==

dn: cn=estudiante,ou=personal,dc=unanleon,dc=edu,dc=ni
cn: estudiante
gidnumber: 501
objectclass: posixGroup
objectclass: top
structuralobjectclass: posixGroup

dn: cn=antonio martinez,cn=estudiante,ou=personal,dc=unanleon, dc=edu,dc=ni
cn: antonio martinez
gidnumber: 501
givenname: antonio
homedirectory: /home/personal/estudiante/amolinares
loginshell: /bin/sh
mail: amartinez @unanleon. edu.ni
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
sn: martinez
structuralobjectclass: inetOrgPerson
uid: amartinez
uidnumber: 4000
userpassword: {MD5}4QrcOUm6Wau+VuBX8g+IPg==

dn: cn=sandra centeno,cn=estudiante,ou=personal,dc=unanleon, dc=edu,dc=ni
cn: valentin martinez
gidnumber: 501
givenname: sandra
homedirectory: /home/personal/estudiante/vmartinez
loginshell: /bin/sh
mail: scenteno@unanleon. edu.ni
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
sn: centeno
structuralobjectclass: inetOrgPerson
uid: scenteno
uidnumber: 3001
userpassword: {MD5}4QrcOUm6Wau+VuBX8g+IPg==

Diseño de la Estructura de Red a Utilizar en el Proyecto

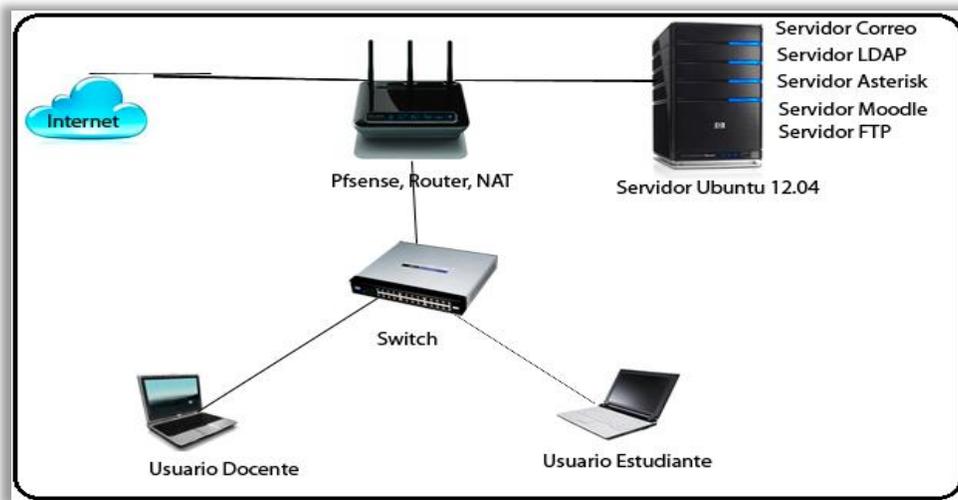


Figura 50. Ejemplo de Infraestructura de Red utilizada

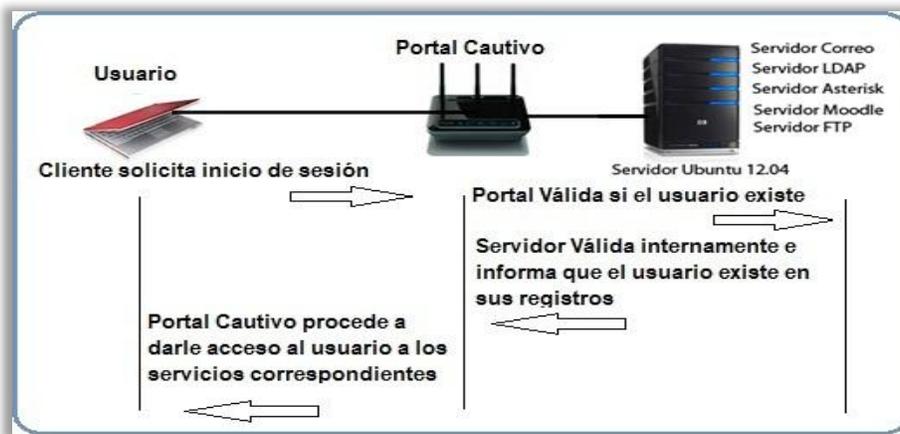


Figura 51. Intercambio de Mensajes

Configuración de Softphone para uso como extensión VoIP



Figura 52. Ingreso de los datos del Cliente



Figura 53. Registro de la Extensión VoIP

Configuración de Cliente de Correo Electrónico para envío y recepción de correos

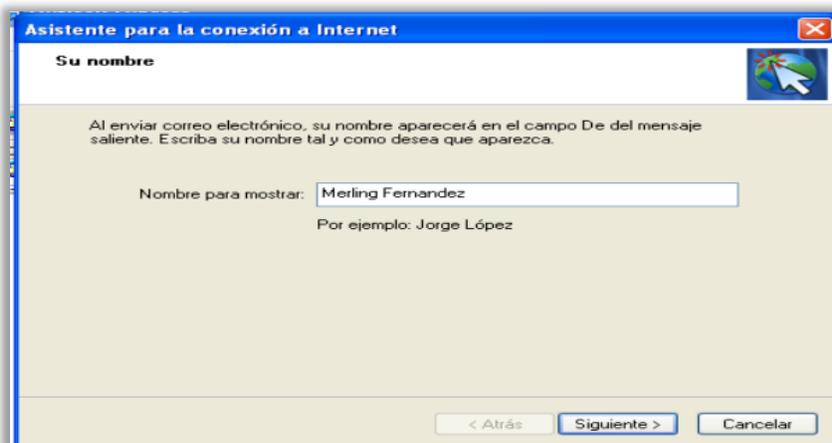


Figura 54. Configuración del Nombre del Usuario

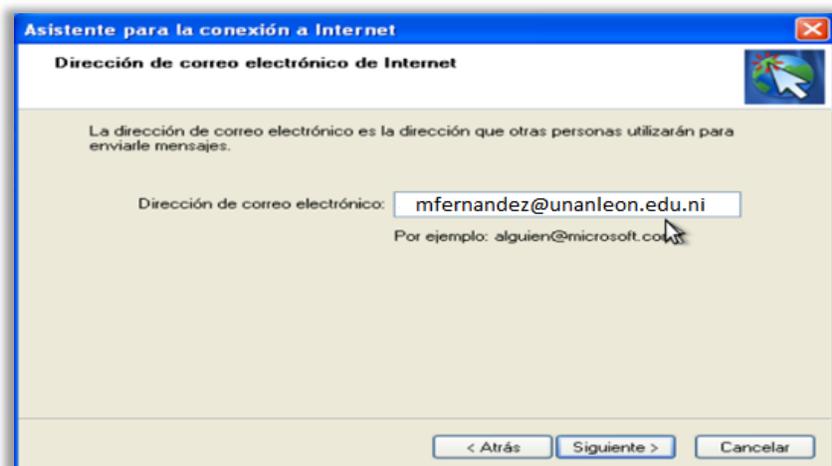


Figura 55. Ingreso de la Dirección de Correo del Usuario

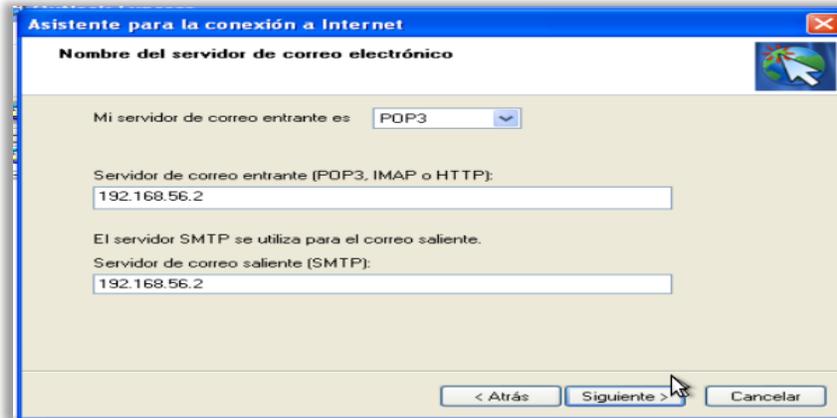


Figura 56. Ingreso de los Datos del Servidor de Correo

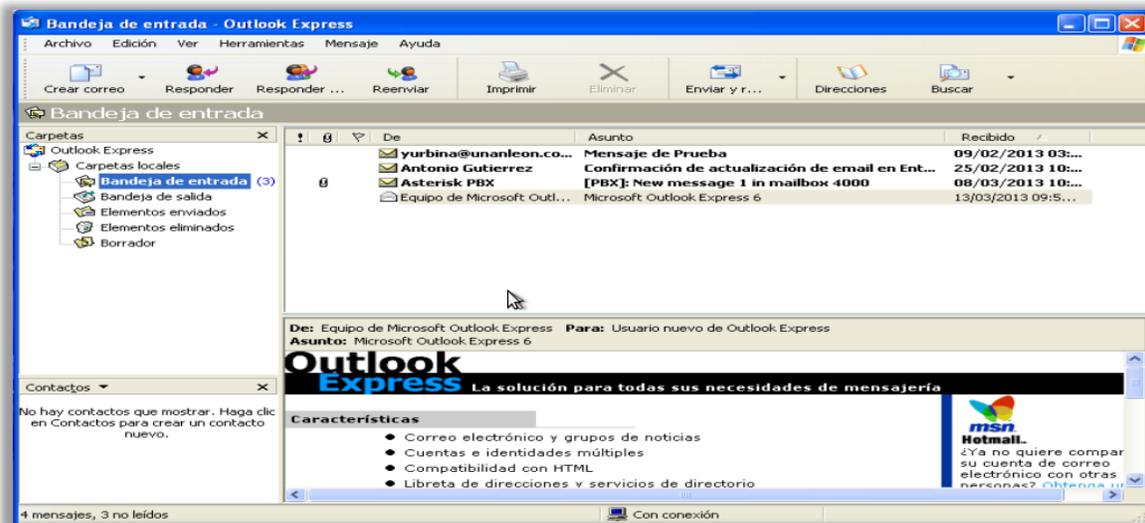


Figura 57. Comprobación de Funcionalidad del Cliente de Correo

Diseño de Página Index.html

```
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>Servicios de Red Unan-Leon</title>
<meta charset="utf-8">
<meta name="autor" content="Ervin Gutiérrez"/>
<link rel="stylesheet" href="css/reset.css" type="text/css" media="all">
<link rel="stylesheet" href="css/layout.css" type="text/css" media="all">
<link rel="stylesheet" href="css/style.css" type="text/css" media="all">
</head>
<body id="page1">
<!-- / header -->
<!-- content -->
  <div class="body5">
    <div class="body6">
      <div class="main">
        <div class="wrapper">
          <figure class="left"></figure>
          <h2>Servicios de Red <span>Unan-León</span></h2>
          <h2 align="center">Red Inálambrica Unan-León</h2>
        </div>
      </div>
    </div>
  </div>
  <div class="body7">
    <div class="main">
      <section id="content">
        <div class="wrapper">
          <article class="col1">
            <div class="box1"><div class="box1_bot"><div class="box1_top">
              <div class="pad"><div class="pad1">
                <p><a href="http://192.168.56.1/webmail"></p>
                <div class="wrapper center">
                  <a href="http://192.168.56.1/webmail"
class="button"><span><span>Acceder</span></span></a>
                </div>
              </div></div></div>
            </div></div></div>
          </article>
          <article class="col1 pad_left1">
            <div class="box1"><div class="box1_bot"><div class="box1_top">
              <div class="pad">
                <div class="pad1">
                  <p><a href="ftp://usuario@192.168.56.1"></p>
                  <div class="wrapper center">
                    <a href="ftp://usuario@192.168.56.1"
class="button"><span><span>Acceder</span></span></a>
                  </div>
                </div></div></div>
            </div></div></div>
          </article>
          <article class="col1 pad_left1">
            <div class="box1"><div class="box1_bot"><div class="box1_top">
              <div class="pad">
                <div class="pad1">
                  <p><a href="http://192.168.56.1/moodle"></p>
                  <div class="wrapper center">
                    <a href="http://192.168.56.1/moodle"></p>
                  </div>
                </div></div></div>
            </div></div></div>
          </article>
        </div>
      </section>
    </div>
  </div>
</div>
```

```

class="button"><span><span>Acceder</span></span></a>
                                </div>
                                </div></div>
                                </div></div></div>
                                </article>
                                <article class="col1">
                                <div class="box1"><div class="box1_bot"><div class="box1_top">
                                <div class="pad"><div class="pad1">
                                <p><a
href="http://www.unanleon.edu.ni/directorio_telefonico.html"></p>
                                <div class="wrapper center">
                                <a
href="http://www.unanleon.edu.ni/directorio_telefonico.html"
class="button"><span><span>Acceder</span></span></a>
                                </div>
                                </div></div>
                                </div></div></div>
                                </article>
                                <article class="col1 pad_left1">
                                <div class="box1"><div class="box1_bot"><div class="box1_top">
                                <div class="pad">
                                <div class="pad1">
                                <p><a
href="http://www.google.com.ni"></p>
                                <div class="wrapper center">
                                <a
href="http://www.google.com.ni"
class="button"><span><span>Acceder</span></span></a>
                                </div>
                                </div></div>
                                </div></div></div>
                                </article>
                                <article class="col1 pad_left1">
                                <div class="box1"><div class="box1_bot"><div class="box1_top">
                                <div class="pad">
                                <div class="pad1">
                                <p><a
href="http://www.unanleon.edu.ni"></p>
                                <div class="wrapper center">
                                <a
href="http://www.unanleon.edu.ni"
class="button"><span><span>Acceder</span></span></a>
                                </div>
                                </div></div>
                                </div></div></div>
                                </article>
                                </div>
                                <div class="wrapper">
                                <article class="col2">
                                <div class="pad1">
                                <iframe width="570" height="300" frameborder="0" scrolling="no" marginheight="0" marginwidth="0"
src="https://maps.google.com.ni/maps?f=q&source=s_q&hl=en&geocode=&q=Edificio+Central+de+
la+UNAN-Le%C3%B3n,+Le%C3%B3n&aq=0&oq=unan&sl=12.869165,-
85.0177&sspn=5.577976,10.821533&t=h&ie=UTF8&hq=Edificio+Central+de+la+UNAN-
Le%C3%B3n,+Le%C3%B3n&ll=12.436811,-
86.879037&spn=0.021792,0.032015&output=embed"></iframe><br
                                </small><a
href="https://maps.google.com.ni/maps?f=q&source=embed&hl=en&geocode=&q=Edificio+Central
+de+la+UNAN-Le%C3%B3n,+Le%C3%B3n&aq=0&oq=unan&sl=12.869165,-
85.0177&sspn=5.577976,10.821533&t=h&ie=UTF8&hq=Edificio+Central+de+la+UNAN-
Le%C3%B3n,+Le%C3%B3n&ll=12.436811,-86.879037&spn=0.021792,0.032015"
style="color:#0000FF;text-align:left">View Larger Map</a></small>></iframe>
                                </div>

```

```

        </article>
        <article class="col1 pad_left1">
            <h2>Adicionales</h2>
            <ul class="list2">
                <li><a href="http://estud.unanleon.edu.ni/">Correo
Estudiantil Live@edu</a></li>
                <li><a href="http://www.unanleon.edu.ni/wifi/">Red
Wifi Unan-León</a></li>
                <li><a
href="http://www.it.comp.unanleon.edu.ni/inicio/">Departamento de Computación</a></li>
                <li><a href="http://www.accuweather.com/es-
mx/ni/leon/leon/quick-look.aspx">Pronóstico del Tiempo</a></li>
                <li class="bg_none"><a
href="http://www.unanleon.edu.ni/galeria_fotos.html">Galería de Fotos</a></li>
            </ul>
        </article>
    </div>
</section>
</div>
</div>
<!-- / content -->
<!-- footer -->
<div class="body8">
<div class="body9">
    <div class="main">
        <footer>
            <div align="center">
                <h3>© Departamento de Computacion 2013, Edificio Central, Contiguo Iglesia
La Merced. Ext. 1040, <a href="mailto:mail@unanleon.edu.ni">mail@unanleon.edu.ni</a></h3>
            </div>
        </footer>
    </div>
</div>
<!-- / footer -->
</div>
</div>
</body>
</html>

```



Servicios de Red Unan-León

Red Inálambrica Unan-León



Acceder



Acceder



Acceder



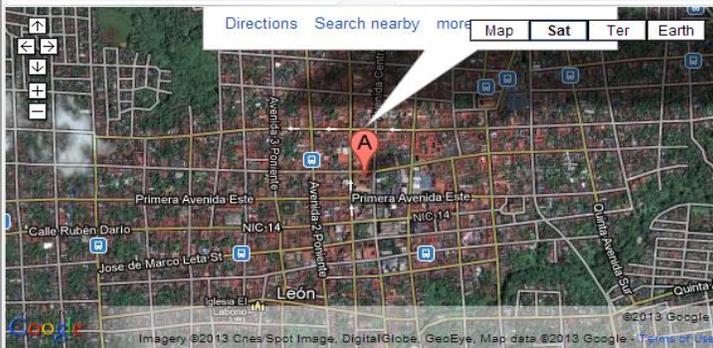
Acceder



Acceder



Acceder



[View Larger Map](#)

Adicionales

[Correo Estudiantil Live@edu](#)

[Red Wifi Unan-León](#)

[Departamento de Computación](#)

[Pronóstico del Tiempo](#)

[Galería de Fotos](#)

© Departamento de Computacion 2013, Edificio Central, Contiguo Iglesia La Merced. Ext. 1040
mail@unanleon.edu.ni

Figura 58. Página Index.html