CAPÍTULO 1: PLANTEAMIENTO DEL PROBLEMA

1.1 Definición del problema.

1.1.1 Síntesis.

El propósito fundamental de esta tesis es presentar una solución a organizaciones que posean sistemas híbridos dentro de su infraestructura tecnológica, partiendo de un análisis de factibilidad en el que se exponen situaciones y consideraciones previas a su implementación. La medida que utilizamos está basada en un sistema de clave pública que hace uso de certificados digitales para proveer seguridad y autenticación en el entorno global de la infraestructura de la empresa, ya sea actividades sobre Internet, Ethernet o Intranet.

Con lo expuesto anteriormente se pretende implementar un prototipo con seguridad a nivel de correo electrónico que trabaje en plataformas híbridas y se encargue de gestionar y manejar certificados y firmas digitales, brindando al usuario confiabilidad y seguridad en cada una de sus transacciones electrónicas tanto internas como externas a la red.

1.1.2 Antecedentes.

Hace no tantos años los sistemas de gestión y la informática en sí, no estaban incluidos dentro de los temas prioritarios de una empresa o comerciante pequeño y mediano de nuestro país. Hoy en día y como consecuencia a las bondades que presenta la red de redes toda empresa que maneje distintas líneas de negocio se han visto volcadas al uso prioritario de cualquier servicio informático, sean estos publicaciones de páginas web, correos electrónicos, redes sociales, etc., trayendo como

consecuencia un gran avance tecnológico por la implementación de infraestructuras muchas de ellas híbridas que permitan la administración de los sistemas informáticos y aportando consigo grandes necesidades de seguridad para resguardar cualquier tipo de información de la empresa.

Es así, que una infraestructura informática se ha convertido en un complejo surtido de sistemas y dispositivos necesarios para la comunicación entre los mismos, debido al reciente interés de sistemas híbridos se conoce que la combinación de sistemas de software representan un reto para que se encuentren simultáneamente acopladas y que trabajen de manera cooperativa. Cuando una organización debe convivir con diferentes sistemas operativos, se debe buscar la forma de facilitar a los usuarios acceder a los recursos independientemente de la plataforma que estos decidan utilizar y sobre todo proveer la seguridad necesaria para realizar este intercambio de información. Tomando en cuenta que el movimiento principal de las empresas en su gran mayoría está basado en el comercio y marketing electrónico, la seguridad a nivel de tecnología no basta que sea considerada solamente a nivel interno o intranet pues el tema de pérdidas de datos puede resultar muy costosa para la organización.

Una vez identificado el problema y la necesidad vemos que el agrupamiento de diferentes sistemas en una única administración centralizada que maneje seguridad en correos electrónicos, principal servicio utilizado en la red, y encriptamiento de los mismos no es trivial, ya que la diferencia de diseño entre los sistemas y los estándares que se implementan no son compatibles, es por eso necesario implementar una infraestructura interna de seguridad que nos permita tener una Autoridad de Certificación que genere certificados digitales de cada usuario y encripte los mensajes. Con la implementación de este proyecto se quiere evaluar la factibilidad, ventajas y

desventajas que hay tanto en Windows como GNU/Linux y proveen el mismo servicio. Los beneficiarios principales son las empresas que convivan con diferentes sistemas operativos y deseen conocer sobre la factibilidad que tener corriendo diferentes ambientes.

1.1.3 Justificación e importancia del proyecto.

Muchos son los problemas que una empresa debe enfrentar ante la falta de un sistema de seguridad en un servicio como el correo electrónico, la ausencia de la firma digital en la gestión de documentos electrónicos puede hacer que cualquier mensaje emitido en una transacción electrónica no llegue a su destino íntegramente, por lo tanto ante el gran volumen de gestión en correos electrónicos es necesario una implementación de un sistema de seguridad que permita emitir mensajes con firmas digitales, además de la encriptación de los mismos con el objetivo de llevar un registro de mensajes íntegros tanto en el envío como en la recepción. Acrecentando con esto la integridad de datos, autenticación de usuarios, y facilitando la legitimidad de los correos electrónicos en cualquier empresa.

El tema de esta tesis tiene una estrecha relación con un proyecto implementado en la Escuela Superior Politécnica del Litoral, que cuenta con un servidor de claves públicas PGP, cliente administrador y cliente para ciframiento y desciframiento de correo electrónico. Lo que nos ayuda a verificar que este proyecto es totalmente realizable y aplicable dentro de una institución y que los objetivos que hemos planteando son totalmente ejecutables. Sin embargo, los alcances de este proyecto son más amplios pues la integración que se desea probar es una infraestructura híbrida con sistemas operativos GNU/Linux y Microsoft Windows 2003 server, tomando en cuenta que muchas empresas tienen su infraestructura montada bajo esta hetero-

geneidad; el prototipo que se desea implementar sería de mucha ayuda pues un gran número de empresas carecen de un sistema de seguridad a nivel de correo electrónico, un ejemplo interesante es la Universidad San Francisco que ya cuenta con esta infraestructura diferida, teniendo en Windows 2003 un servidor de directorio activo el cual autentica y aplica políticas de directorio a usuarios y computadoras de la red interna, Microsoft Exchange 2007, en un servidor con Microsoft Windows 2008, el mismo que brinda el servicio de correo electrónico a usuarios pertenecientes al directorio activo. Por otro lado, bajo GNU/Linux distribución DEBIAN específicamente un servidor Mail Gateway pues trabaja con una infraestructura SMARTHost a nivel de correo electrónico. Lo que se quiere analizar son las ventajas, desventajas que representa tener una infraestructura heterogénea trabajando en cualquier empresa con estas características.

1.1.4 Funcionalidad de una infraestructura híbrida GNU Linux/Windows.

La funcionalidad de una infraestructura híbrida está definida por el conjunto de características que hacen a la misma práctica y utilitaria, las mejorías que tiene la fusión de estas plataformas se ven reflejadas en seguridad, rapidez, economía, facilidad, aplicabilidad, etc. El desarrollo de este prototipo nos va a permitir ayudar a empresas que cuentan con una infraestructura heterogénea, y no presentan seguridad al nivel de correo electrónico.

Este prototipo representa dos conjuntos de redes que simulan un ambiente de trabajo con servidores de correo electrónico, directorio, firewall, servidor de claves públicas y usuarios híbridos. Bajo las características descritas con anterioridad la funcionalidad se basa en un sistema que provea certificados digitales para asegurar

el plan de mensajería electrónica y brinde al usuario confiabilidad, seguridad en cada una de sus transacciones electrónicas.

CAPÍTULO 2: FUNDAMENTOS TEÓRICOS

En este capítulo introduciremos algunos conceptos que nos ayudarán al desarrollo de esta tesis y explicarán la factibilidad de utilizar una infraestructura híbrida que brinde seguridad en correo electrónico.

Es necesario contar con una explicación de los conceptos básicos para comprender la estructura y funcionamiento de una infraestructura mixta GNU Linux/ Windows. Por lo tanto, a continuación analizaremos las diferentes herramientas de software que se van a ocupar para el desarrollo de esta tesis.

2.1 Herramientas de Desarrollo

Para la implementación de este prototipo usaremos la siguiente constitución de red la cual debe poseer un servidor de directorio, un servidor de correo, un servidor firewall, un servidor de claves públicas. Con la tabla a continuación explicaremos la equivalencia del software que se va a implementar en cada una de las redes. Al mismo tiempo, debemos resaltar que se utiliza la misma infraestructura de clave pública llamada "OpenCA" para ambas redes, que será explicada antes de finalizar este capítulo. Conjuntamente, se configuró un servidor extra de DNS que nos sirvió para el reenvío de paquetes de una red a otra.

Servidor	Windows	GNU/Linux
Servidor firewall	ISA Server	Iptables
Servidor de directorio	Active Directory	OpenLDAP
Servidor de correo	Exchange Server	Exim
Servidor de clave pública	OpenCA	OpenCA

Tabla 1. Software Equivalente GNU/Linux/Windows

2.2 Definición de términos

Los términos que se van a definir en esta sección de capitulo dependerán de los servicios que se implementen en cada uno de los servidores, para lo cual tenemos la (Tabla 2) que relaciona a los servidores con los servicios que posee.

Servidores	Términos
Servidor firewall	Reglas para filtrar paquetes.
Directorio Activo	Servicio DNS (resolución de nombres, resolución reversa)
Servidor Correo	Spamassasim, Antivirus, DSAccess, DSProxy, MTA, SMTP, IMAP y POP.
Servidor OpenCA	Criptografía asimétrica, autoridad de certificación, certificados digitales, autoridad de registro.

Tabla 2. Servidores y Servicios GNU/Linux/Windows

2.2.1 Red Windows

La red de Windows será implementada sobre Windows server 2003, este sistema operativo basa su tecnología en Windows NT y es una evolución de la plataforma de servidores que presenta mejoras en rendimiento, ahorro de costos, conectividad, un elevado nivel de seguridad y calidad. Este servidor fue diseñado para empresas que deseen maximizar el valor de sus negocios, ofreciendo rapidez, escalabilidad, fiabilidad, y disponibilidad. Esto permite a los clientes ser más productivos ya que es un sistema poco complejo y fácil de gestionar, permitiendo mayor productividad empresarial. [1]

Uno de los mayores atributos de Windows server 2003 es la seguridad, que ahora es uno de los espacios más importantes en las empresas, porque de esta forma se puede garantizar la competitividad empresarial. Este sistema operativo puede man-

tener los sistemas informáticos conectados de forma eficiente y segura, se ha convertido en norma fundamental para el desarrollo de tecnología confiable afianzando al cliente gracias a todas las funcionalidades que se proveen.

Windows server 2003 hoy en día permite establecer infraestructuras de claves públicas mediante certificados y herramientas de gestión de los mismos, que permiten extender de forma segura la actividad de las empresas hacia el Internet, permitiendo entrar al mundo globalizado de forma competitiva y segura. Además esta plataforma permite encriptar la información para mantenerla segura dentro y fuera de la organización. [2]

Componentes de la red:

- Firewall = Isa Server
- Servidor de directorios = Active Directory Server
- Servidor de Mensajería = Exchange Server
- Servidor de claves Públicas, certificados digitales = OpenCA Server
- Usuarios = Linux, Windows

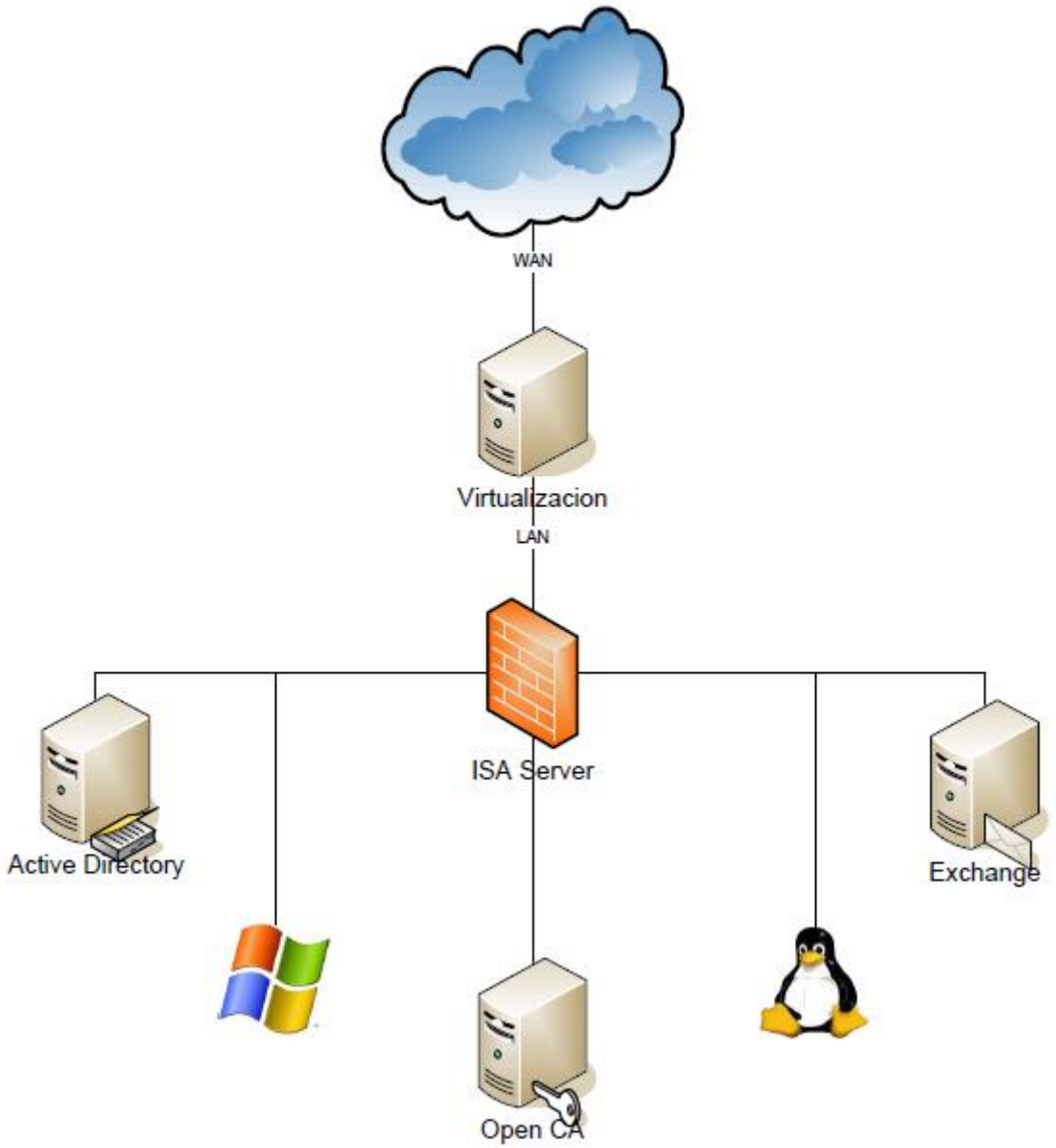


Figura 1. Diagrama de Red Windows

2.2.1.1 Internet Security and Acceleration ISA server 2006

Los riesgos frecuente de virus, ataques, y el uso del Internet han hecho necesario que organizaciones tanto grandes como pequeñas, evalúen estrategias de protección y seguridad. Hoy en día no es posible ignorar las desventajas de tener un sistema de seguridad vulnerable y los daños que pueden causar estos ataques a organizaciones. [5]

“Isa server es un Gateway integrado, provee seguridad perimetral que permite proteger su entorno de IT frente a las amenazas de Internet, además de proporcionar a los usuarios un acceso remoto seguro a las publicaciones y datos corporativos.” [6] El servidor de seguridad avanzado permite a las organizaciones obtener el máximo provecho de las inversiones tecnológicas para mejorar la seguridad y el rendimiento de la red.

2.2.1.2 Directorio Activo

La estructura jerárquica de un directorio o almacenamiento de datos nos permite almacenar información sobre objetos en la red, este ámbito es normalmente implementado como una base de datos optimizada posibilitando realizar diferentes operaciones como lectura, escritura y soporta búsquedas de grandes datos de información y con capacidades de exportación.

Windows server 2003 provee el servicio de directorio, almacena información acerca de los recursos de la red y permite el acceso a los usuarios y las aplicaciones de dichos recursos, convirtiéndose en un medio de organización, control, administración de una red centralizada, convirtiendo al directorio activo en una herramienta de administración de toda la organización. [3]

Sistema de Nombres de Dominio (DNS)

Sistema de nombres de dominio permite la administración de los nombres a equipos y servicios de red, este servicio constituye el mecanismo de asignación y resolución de nombres, es decir, la traducción de nombres simbólicos a direcciones IP en internet. Windows server 2003 utiliza DNS para localizar equipos y controladores de dominio en una red, la asignación de nom-

bres de dominio se utiliza en las redes basadas en el protocolo TCP/IP, como Internet, para localizar equipos y servicios con nombres sencillos. [13]

Funciones principales de DNS:

- Resolución de direcciones IP de otros host de una red TCP/IP.
- Definición de espacios de nombres.
- Búsqueda de los componentes físicos del directorio activo, es decir que ubica controladores de dominio y servidores de catálogo de un dominio de Directorio activo y ubica servidores de correo electrónico en otras organizaciones de mensajería. [12]

Resolución de Nombres

También conocidos como resolvers, son los encargados del proceso de traducción de un nombre en un objeto o información que lo representa, los resultados que retorna al programa que está solicitando la información es precisamente la resolución de nombres textuales a direcciones IP. [12]

Resolución Reversa

La resolución reversa como su nombre lo indica realiza el proceso inverso a la resolución de nombres, es decir, dado un número IP determinar el nombre principal asociado a ésta. Esta facilidad permite que los programas puedan producir la salida en formatos más fáciles y comunes. [12]

2.2.1.3 Exchange Server 2003

Exchange Server 2003 se relaciona con la infraestructura TCP/IP que ofrece Windows Server 2003 y el servicio de directorio activo, es útil conocer de que manera Exchange 2003 utiliza Directorio Activo para implementar la estructura de directorios deseada.

Exchange como plataforma de servidores de mensajería, tiene ciertas características como; transferir mensajes de correo electrónico a sus destinatarios de manera confiable, almacenar mensajes en un lugar específico destinado para almacenamiento, admite diferentes clientes al correo electrónico, permite conexiones internas o externas a la red, proporciona información de diferentes destinatarios de la organización. [4]

Directory Service Access (DSAccess)

Este componente controla el modo en que otros componentes de Exchange tienen acceso al Directorio Activo. DSAccess lee la topología del Directorio Activo, detecta los controladores de dominio y los servidores de catálogo global, y mantiene una lista de servidores de directorios válidos que son adecuados para ser utilizados por los componentes de Exchange.[12]

Directory Service Proxy (DSProxy)

Este componente proporciona un servicio de lista de direcciones de los clientes de Microsoft Office Outlook, tiene dos funciones:

- Emular un servicio de libreta de direcciones MAPI y las solicitudes proxy a un servidor de Directorio Activo.
- Proporciona un mecanismo de referencia para que los clientes de Outlook puedan contactar al Directorio Activo directamente.

Su nombre indica que proporciona solamente servicios proxy, sin embargo proporciona también servicios de referencia. [14]

Mail Transfer Agent (MTA)

Los agentes de transferencia de correo son los encargados de llevar el correo electrónico al usuario final, el protocolo que generalmente ocupa es el SMTP.

Los elementos importantes dentro de la transmisión de un correo electrónico son:

- Agentes de entrega de correo electrónico (MDA) que es el encargado de mover el correo dentro de un sistema.
- Los clientes de correo electrónico o también conocidos como Mail User Agente (MUA) es un programa que se usa para leer y enviar mails, además se los debe mencionar a los clientes lectores de correo remoto como POP e IMAP. [16]

Protocolo Simple de Transferencia de Correo (SMTP)

Es un protocolo estándar que permite la transferencia de correos de un servidor a otro mediante una conexión punto a punto. SMTP es un modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste en líneas de texto compuestas por caracteres ASCII. [15]

Protocolos IMAP y POP

El funcionamiento de los protocolos IMAP y POP es proporcionar un acceso remoto a los buzones de los usuarios.

- Internet Messaging protocol Access (IMAP), permite al usuario acceder remotamente a su correo electrónico como si fuera local, además permite crear, renombrar y borrar los buzones. El acceso y la administración puede ser de más de un ordenador.
- Post Office Protocol (POP) fue diseñado para soportar el procesamiento de correo fuera de línea, su funcionamiento se basa en que el cliente del mail se conecta periódicamente a un servidor de correo y se baja todo el correo pendiente a la maquina local del usuario. [16]

Antivirus y Antispam (ESET)

Es un software que sirve como seguridad en mail, para la detección proactiva de amenazas para Microsoft Exchange provee del servicio de antispam con tecnología de huellas digitales, análisis de contenidos, filtrado bayesiano y detección máxima de amenazas informáticas distribuidas a correo electrónico. Provee servicio de antivirus contra amenazas informáticas en constante evolución. [17]

2.2.2 Red GNU/Linux

En la red de GNU/Linux usualmente utiliza herramientas del sistema GNU, es decir herramientas de software libre, en donde el código fuente puede ser utilizado, modificado, redistribuido libremente por cualquiera, bajo los términos de licencia publica general de GNU GLP y otras licencias libres. [7]

Componentes de la red:

- Firewall = Iptables
- Servidor de directorios = OpenLDAP Server
- Servidor de Mensajería = Exim Server

- Servidor de claves Públicas, certificados digitales = OpenCA Server
- Usuarios = Windows, Linux

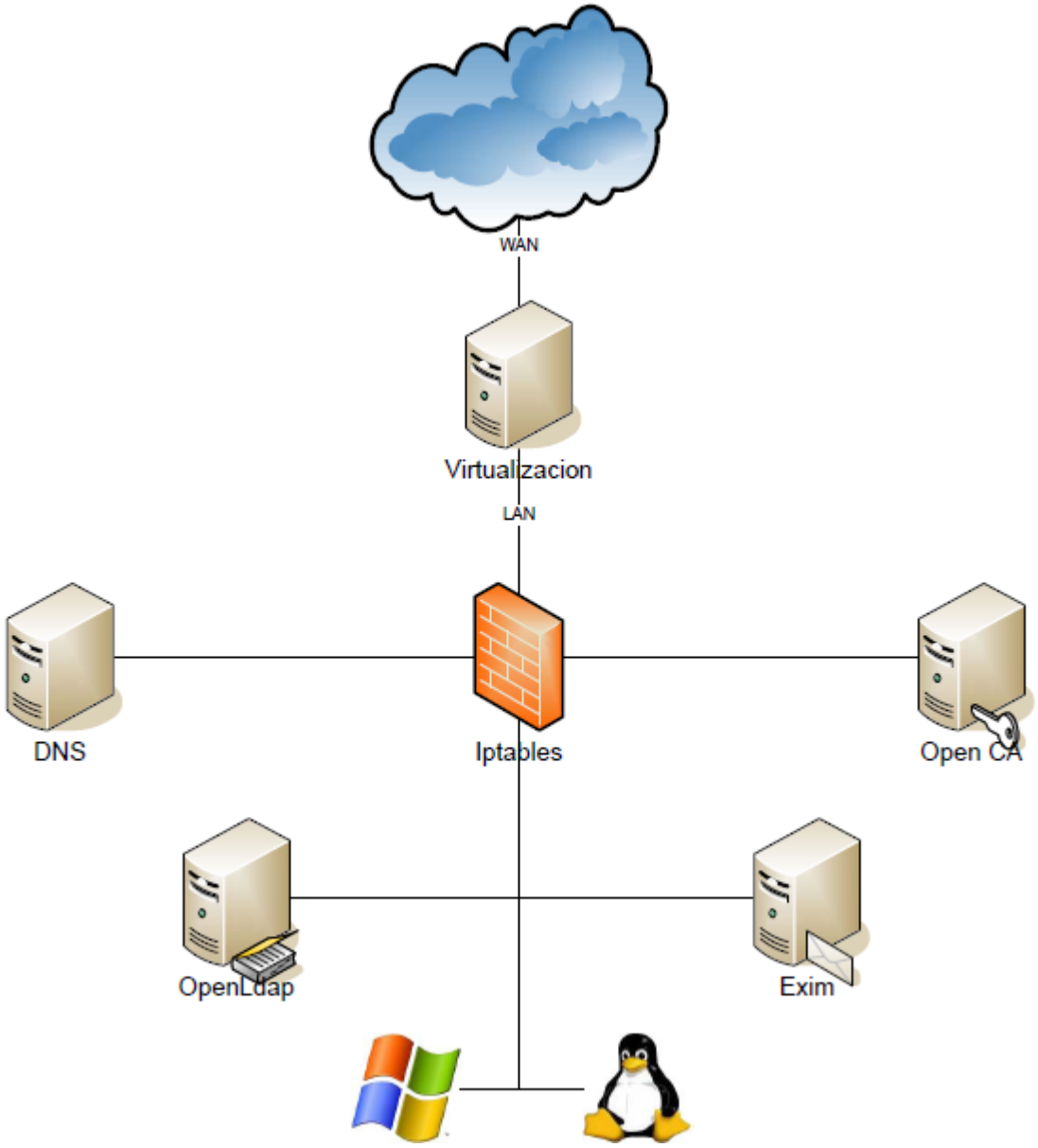


Figura 2. Diagrama de red GNU/Linux

2.2.2.1 Firewall

El firewall es una herramienta preventiva contra ataques, que realiza una inspección de tráfico entrante como saliente. Esto impide que servicios o

dispositivos no autorizados accedan a ciertos recursos y de esta forma proteger a la organización contra ataques degenerativos de servicios. El firewall es excelente para seguridad de contra ataques desde el Internet, ya que cualquier ataque que se presente, tendrá que filtrarse primero por el firewall, e impedirá o permitirá el paso al equipo o red. [10]

El firewall que se va a ocupar para nuestra red GNU/Linux es Iptables, una herramienta que nos permite configurar las reglas de filtrado de paquetes del kernel de Linux, permitiéndonos crear firewalls de acuerdo a nuestras necesidades. Su funcionamiento es simple, ya que un paquete debe cumplir reglas específicas, además se especifica para esa regla una acción o target. [22].

2.2.2.2 Servicio de directorios Open LDAP

En un sistema operativo Unix el servicio de directorios se basa en LDAP (Lightweight Directory Protocol) que es un modelo cliente-servidor, en donde se mantienen los datos que conforman el árbol de directorios LDAP o la base de datos troncal; en donde el cliente se conecta al servidor y hace una consulta, el servidor contesta con la respuesta correspondiente, o bien con una indicación de donde puede el cliente hallar más información.

El servicio de directorios proporciona una respuesta rápida a operaciones de búsqueda o consulta y tiene la capacidad replicar información de forma amplia con el fin de aumentar la disponibilidad y confiabilidad, y a la vez reducir el tiempo de respuesta; para evitar inconsistencias en las réplicas de directorios debe existir una sincronización entre las mismas. [8]

2.2.2.3 Servicio de correo (EXIM)

Los servidores de correo son utilizados a menudo con diferentes funciones según la planificación de la organización o persona. El correo electrónico es probablemente la aplicación TCP/IP más usada, los protocolos básicos de correo proporcionan intercambio de mensajes entre hosts TCP/IP. Para lograr el intercambio de correo electrónico se definen una serie de protocolos como SMTP, POP, IMAP; estos protocolos tienen la finalidad concreta de trasferir los correos de un lugar a otro. [9]

El software para el servidor que se propone es Exim que es un agente de transporte de correo MTA, tiene una gran flexibilidad en la elección de caminos que pueden seguir de acuerdo al origen y funcionalidad que se desee implementar; tiene facilidades para controlar usuarios, dominios virtuales,

spam, lista de bloqueo por DNS, todas estas opciones son configurables en este servidor de correo. [18]

Asimismo se propone implementar spamassasin para el control de spam y antivirus ClamAV, para proporcionar seguridad equivalente a lo que se realizará en la red Windows.

Spamassassin

Spamassassin lee el encabezado y el cuerpo de un correo electrónico entrante o saliendo, determinando mediante una serie de pruebas asignado una puntuación para realizar la comprobación de si es o no Spam. El encabezado del correo electrónico es reescrito, agregando líneas indicando las pruebas positivas, la suma total de las puntuaciones y una bandera, indica Spam o no, si la suma total sobrepasa un límite determinado. [19]

ClamAV antivirus

Es una herramienta de antivirus open source para Unix, diseñado específicamente para escanear correos electrónicos, su principal objetivo es la integración con servidores de correo. Este antivirus dispone de un paquete con herramientas para actualización automática a través del Internet, escáner de línea de comandos, un demonio multi-hilo flexible y escalable, actualizador de base de datos con soporte para actualizaciones programadas y firmas digitales, análisis según accesos, soporte embebido para casi todos los formatos de ficheros de correo. [20]

2.2.3 Servidor Open CA

La infraestructura de clave pública sirve para gestión de certificados digitales y aplicación de firma digital o cifrada, esta infraestructura tiene una autoridad res-

ponsable de crear y expedir certificados a los usuarios, asociando consigo la identidad del usuario. La Autoridad de Certificación es responsable de administrar todos los aspectos del ciclo de vida del certificado después de su expedición, es por eso que almacena de forma pública los certificados autorizados como revocados.

La infraestructura de clave pública en sistemas operativos Windows o GNU/Linux proporcionan los mismos servicios que son:

Autenticidad: la firma digital tendrá la misma validez que la manuscrita.

Confidencialidad: De la información transmitida entre las partes.

Integridad: Debe asegurarse la capacidad de detectar si un documento firmado ha sido manipulado.

No repudio: De un documento firmado digitalmente.

Para la implementación de esta infraestructura se ocupará OpenCA que es una herramienta de software libre que permite realizar la gestión de certificados, firmas digitales etc. [11]

Criptografía Asimétrica

La clave pública se utiliza para codificar y la clave privada se utiliza para decodificar. Dependiendo de la aplicación que se le dé al algoritmo, la clave pública puede ser de cifrado o viceversa, resultando completamente difícil calcular una clave a partir de otra ya conocida, esto intensifica la seguridad en estos criptosistemas. [23]

La criptografía de clave publica permite entre otras cosas, implementar el sistema de firmas digitales con tiene el propósito de validar el contenido y probar que no se ha falsificado un mensaje durante su envío. Las firmas digitales respaldan la autenticidad del mensaje, basándose en el hecho de que dos grupos pueden autenticarse

el uno con el otro para el intercambio de información seguro. Cubriendo una gama de vulnerabilidad en la seguridad de un sistema. [24]

Autoridad de Certificación

Una autoridad certificadora es una entidad de confianza que emite y revoca certificados, este servicio de certificación asegura que los certificados tengan relación entre el usuario y su clave pública, esto se lo realiza mediante un cifrado de la clave pública, cada usuario tiene una clave privada que se mantiene en secreto y solo la debe conocer el usuario, por lo tanto esta nunca se envía a través de la red, a diferencia de la clave pública que puede ser distribuida al público. Además el cifrado que nos provee la autoridad certificadora se utiliza para proteger los mensajes de datos, ya que son transmitidos a través de la red. Las firmas digitales sirven para verificar la identidad de los remitentes de los mensajes que se transmiten. [24]

La Autoridad de Certificación se encarga de verificar las condiciones que constan en sus políticas públicas de seguridad, y se encarga también de emitir y seguir el ciclo de vida de los certificados que emite. [25]

Certificados digitales

El certificado digital está constituido por la clave pública, identidad del usuario, periodo de validez del certificado, identidad de la autoridad certificadora, y la firma digital del certificado. Esta información se encapsula en un formato estándar, definido por la norma ISO X.509 versión 3. El repositorio en el que se publican todos los certificados que se encuentran en gestión y pueden ser consultados por los usuarios que quieran enviar información cifrada o verificar firmas digitales es la Autoridad Certificadora. [24]

Atención de Solicitud de certificados

Para atender solicitudes es importante un reconocimiento previo de elementos característicos y únicos propios de los usuarios o solicitantes. La Autoridad Certificadora puede requerir información como carnet personal para hacer la constatación de que los datos coinciden como foto entre otros; en caso de equipos electrónicos, computadores, servidores, podríamos hacer la verificación constatando las características del equipo como números de serie, etc.

Generación y registro de claves

Cualquiera que desee firmar digitalmente mensajes y recibir mensajes cifrados o firmados tiene que generar su propio par de claves y registrarlo ante la autoridad de certificación a través de una autoridad de registro aceptada dentro de la red planteada, para esto es necesario solamente el envío de la llave pública y el documento digital en donde consta los datos de solicitud de registro, firmados con dicha clave.

Para completar el proceso de inscripción el solicitante deberá: Enviar otro certificado digital de identidad expedido por alguna otra autoridad de certificación autorizada, o enviar un documento físico válido en donde se asume la responsabilidad del compromiso indicado en la solicitud digital enviada. [25]

Emisión de certificados

Satisfechas las condiciones anteriores y cumpliendo con las políticas de emisión de certificados y de seguridad, la Autoridad de Registro envía todos los documentos a la Autoridad Certificadora, la cual se encarga de generar el certificado correspondiente y devolver al solicitante un certificado digital que atestigua la validez de su clave pública para actuar dentro del sistema. Certificados a utilizar X.509 versión 3.

Estados de un certificado

Válido.- Es un certificado digital que está válido o en uso, por lo tanto la fecha cae dentro del intervalo de vigencia de un certificado.

Suspendido.- Certificado anulado temporalmente, es decir que se procede a cancelar la validez del certificado por cierto periodo de tiempo y la Autoridad de Certificación pasa al certificado al estado de suspendido, sin embargo, este estado no es irreversible y puede levantarse la suspensión dentro del periodo de validez del certificado.

Revocado.- Cuando un certificado ha sido rechazado, bien por la Autoridad de Certificación que lo emite o por el usuario; esta revocación depende de lo estipulado en las políticas y procedimientos.

Caducado.- Este es el estado final del certificado y se produce cuando se ha superado la fecha de vigencia del certificado. El estado de caducado no le resta valor histórico, ya que mientras estuvo activo, las operaciones en las que participó eran perfectamente válidas. [25]

Servicios de certificación

Los mecanismos de certificación con clave asimétrica son los más utilizados, es por eso que la firma digital representa uno de los mecanismos seguros que se manipulan hoy en día. El manejo de una firma digital implica la verificación de su llave pública correspondiente para proporcionar un servicio de confidencialidad, implicando a su vez, la validación de una cadena de certificados que garantice el establecimiento de confianza entre dos entidades.

El proceso de validación o certificación se puede realizar de la siguiente manera:

- Obtención del certificado a validar o certificar.
- Determinación de la posibilidad de establecer la confianza entre las entidades implícitas.
- En caso de establecer la confianza, identificación de los certificados necesarios en el proceso.
- Obtención de los certificados identificados.[24]

Autoridad de Registro

En las infraestructuras de claves públicas deben establecerse los mecanismos para que los usuarios soliciten su propio certificado, asegurando la identidad del usuario. Este proceso se llama proceso de registro y esto se lo realiza mediante la autoridad de registro. [24]

CAPÍTULO 3: ANÁLISIS Y DISEÑO DEL SISTEMA

En este capítulo vamos a conocer el diseño de los sistemas que van a ser utilizados, por eso es importante conocer la capacidad y las limitaciones del software y hardware en los que el sistema se va a integrar, necesitamos además, conocer la infraestructura de red y la capacidad del sistema operativo que va a ser utilizado en el desarrollo de esta tesis.

3.1 Descripción del diseño de la red.

Para la creación e implementación de la red usaremos un software que funciona en diferentes sistemas operativos como Linux, Windows y Mac. Este software nos permite realizar virtualizaciones, esto quiere decir que permite ejecutar varios ordenadores dentro de un mismo hardware de manera simultánea, y nos proporciona un ambiente de ejecución similar a todos los efectos a un computador físico con todos sus componentes correspondientes. [26] Esta herramienta se la conoce como VMware Server y sirve para manejar, gestionar y arbitrar los recursos principales de una computadora, que son el CPU, memoria, red y almacenamiento, reparte dinámicamente dichos recursos entre todas las máquinas virtuales definidas en el computador central. De modo que nos permite tener varios ordenadores virtuales ejecutándose sobre uno el mismo computador físico. En la figura a continuación se puede observar que la virtualización se encuentra divida en dos redes. La red 172.21.1.1/24 para la implementación de los servidores en Windows y la red 172.21.2.1/24 para la implementación de los servidores en GNU/Linux. La integración de las redes se la realizó por medio de un DNS-master que permite hacer el reenvío de mensajes de una red a otra, la configuración de este DNS-master es únicamente para cumplir con la comunicación entre las plataformas híbridas.

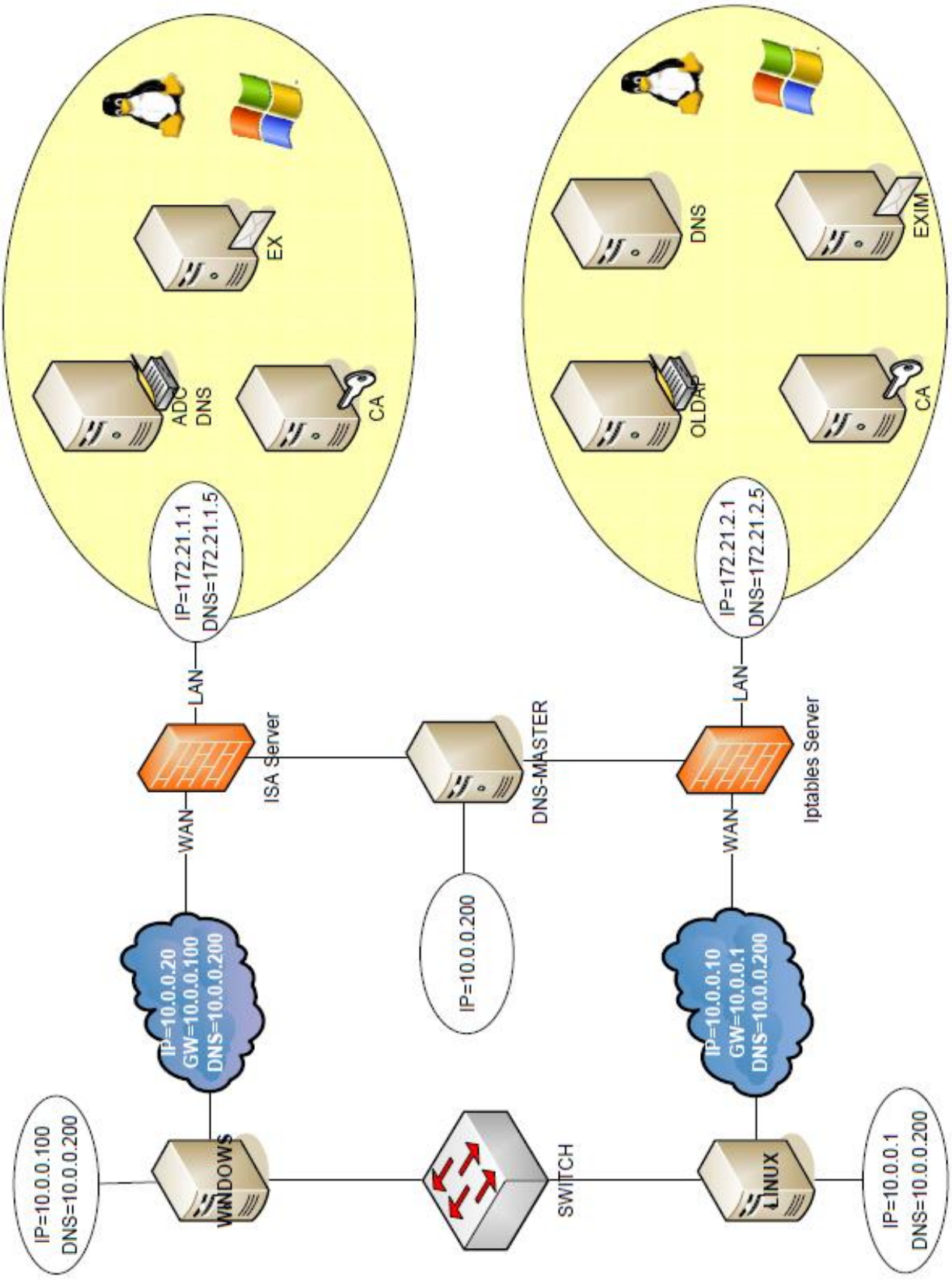


Figura 3. Virtualización de la red

3.2 Descripción básica del entorno de trabajo de los servidores Windows.

Especificación del software en cada una de las máquinas.

3.2.1 Servidor Isa (UIO-ISA-01)

Este servidor va a ser configurado ISA server.

Diseño y análisis del ambiente de ISA server

Este servidor puede asumir múltiples roles en la organización, en nuestro caso vamos a utilizarlo como firewall para establecer una metodología de seguridad dirigida tanto para el tráfico interno como externo a la red.

Las necesidades de nuestra red son:

- Asegurar el acceso y fiabilidad a la red.
- Autenticar a los usuarios para garantizar el control de acceso.
- Mantener la confidencialidad e integridad de la información transmitida.
- Acceso seguro y rápido a los servidores internos.
- Permitir a los usuarios tener acceso a los recursos de la red de forma remota.

Para satisfacer nuestras necesidades este servidor va a estar ubicado entre el internet y los servidores de la organización como lo muestra la (figura 3); este servidor va a tener dos interfaces de red, una llamada WAN que va a estar dando la cara al internet y la otra se llama LAN que va a manejar la red interna de servidores.

El rango de IP que vamos a utilizar para esta red es del 172.21.1.0/24, a continuación se va a especificar las IP y nombres correspondientes a cada servidor.

Isa Server = UIO-ISA-01 = 10.0.0.5 y 172.21.1.1

Directorio Activo = UIO-ADC-01 = 172.21.1.5

Exchange = UIO-EX- 01 = 172.21.1.10

OpenCA Server = UIO-CA-01 = 172.21.1.15

WIN = UIO-WIN-01 = 172.21.1.20

LNX = UIO-LNX-01 = 172.21.1.25

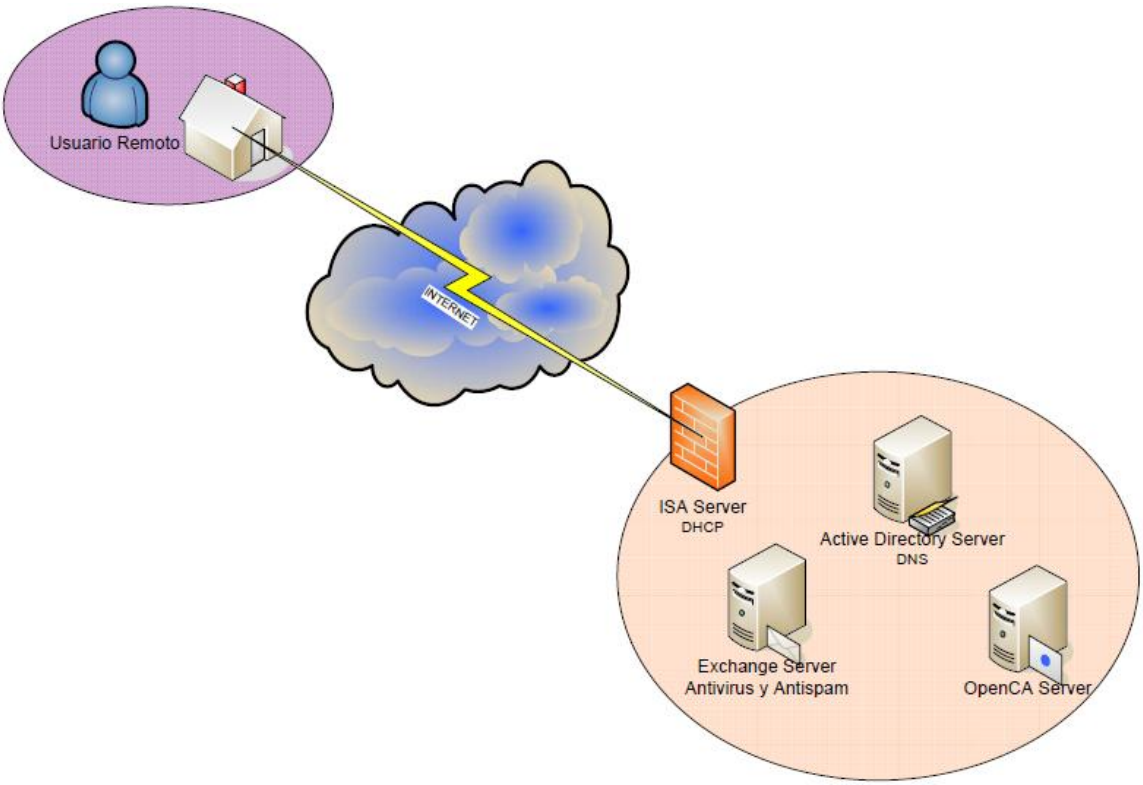


Figura 4. Ambiente de ISA Server

3.1.2 Servidor Directorio Activo (UIO-ADC-01)

Este servidor va a ser configurado Active Directory y servicio de DNS.

Diseño y análisis del ambiente de Directorio Activo

El servidor de directorio Activo nos va a permitir crear la estructura lógica bajo la cual nuestra red va a trabajar. En este caso se creará un dominio que actuará a su vez como controlador de dominio y será llamado *tesis.com*, este dominio compar-

tirá la base de datos de directorios en común, administrando procesos de inicio de sección de usuario, autenticación y búsqueda del directorio.

Dentro del dominio tenemos la jerarquía de objetos en el directorio, está constituida por:

- Dos unidades organizativas de Computadores y Usuarios
- Cuatro unidades organizativas de servidores, administrativos, y clientes.
- Dos Grupos que son Sistemas y Finanzas.

Las directivas de seguridad son las que ayudan a delimitar la confianza de un dominio, estableciendo las políticas bajo las cuales los recursos del dominio van a ser usadas y configuradas, por ejemplo la unidad organizativa de *usuarios*, posee unidades organizativas de *Administrativos* y *Clientes* se les aplica diferentes permisos, como su nombre lo indica *Administrador* tiene permiso administrativos que indica amplios permisos y *Clientes* para usuarios con limitados permisos como solo escritura, etc.

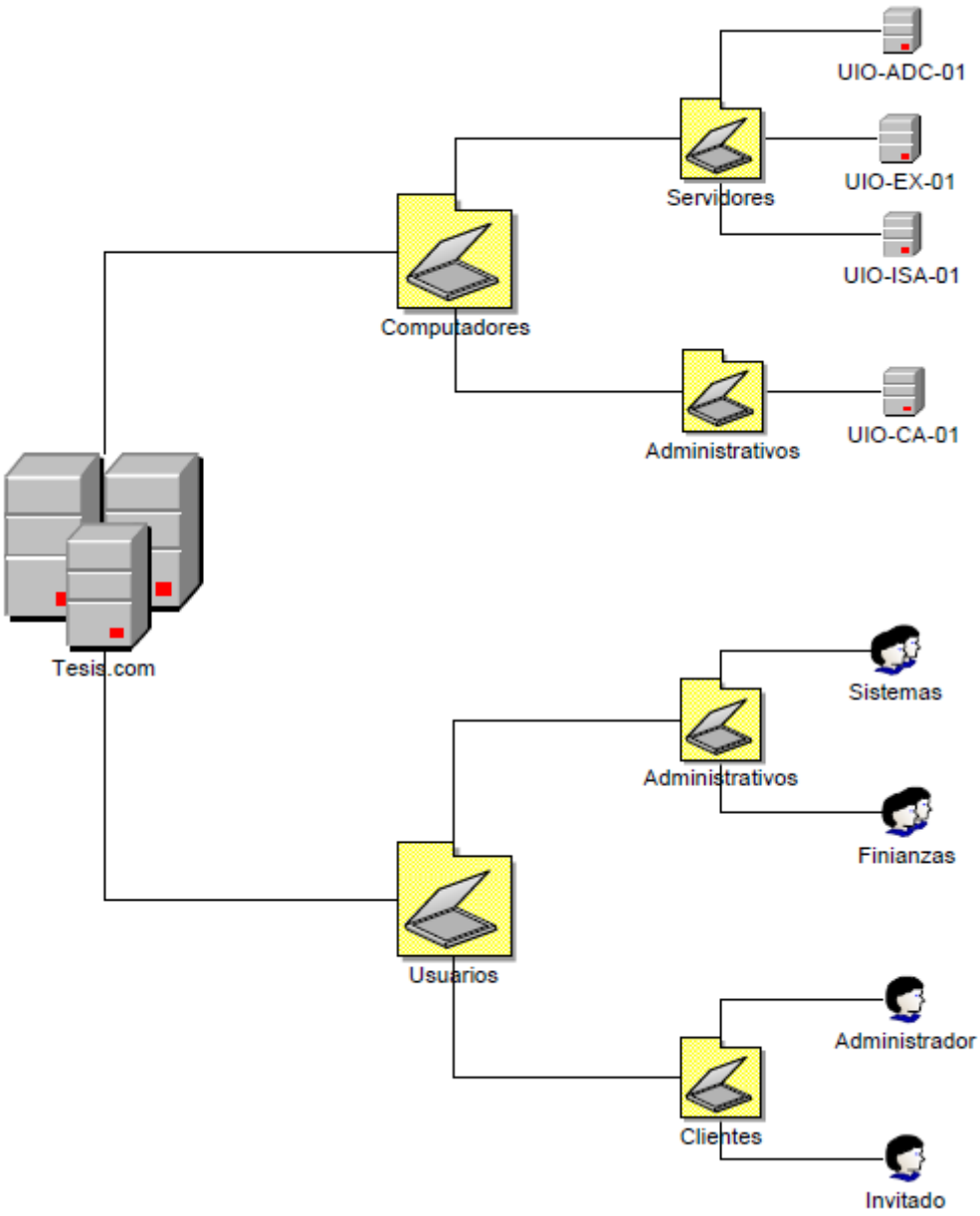


Figura 5. Esquema de jerarquías de Active Directory

Conjuntamente, este servidor se configuró el servicio de DNS para generar una base de datos en donde se almacene la información asociada de nombres simbólicos a direcciones IP, y así recordar la IP y el nombre de cada servidor de la red. La estructura del DNS es la siguiente:

ISA01.tesis.com = 172.21.1.1

ADC01.tesis.com = 172.21.1.5

EX01.tesis.com = 172.21.1.10

CA.tesis.com = 172.21.1.15

3.2.3 Servidor Exchange (UIO-EX-01)

Este servidor va a ser configurado Exchange Server, con servicios de antivirus y antispam.

Diseño y análisis del ambiente de Exchange

El servidor de Exchange 2003 depende completamente del servicio de Directorio Activo, para realizar operaciones de directorio. El Directorio Activo provee toda la información acerca de buzones, servicio de listas de direcciones, e información relacionada con el destinatario. Por lo que, la mayor parte de información sobre la configuración de Exchange se encuentra almacenada en el Directorio Activo.

El encargado de administrar el acceso a los directorios es el componente de Exchange, se lo denomina operador del sistema que además de encargarse de la administración, posee diversos componentes internos como DSAccess y DSProxy, que se encargan de comunicarse con el Directorio Activo y almacenan en cache la información para aumentar la velocidad a la cual se recupera la misma, consiguiendo disminuir la carga de trabajo en los controladores de dominio y los servidores de catalogo globales.

Se uso además ESET para control de virus y spam, este software nos permite filtrar la información antes de que llegue a los buzones de los clientes, evitando las amenazas informáticas.

Para los propósitos de esta tesis se utilizó las siguientes características de configuración:

- Dos controladores de domino, en el caso de que se caiga uno, el otro sirva de respaldo, es por eso que se tiene configurado dos computadoras la primera está configurada con directorio activo y controlador de domino. La segunda está configurada con Exchange y controlador de dominio.
- Versión de Exchange estándar ya que cumple con los propósitos básicos de este prototipo de prueba, la diferencia básicamente entre el Estándar y Enterprise son los grupos de almacenamiento y cluster, es por eso que si se desea ampliar las capacidades se recomienda la versión Enterprise, para mayor capacidad de almacenamiento y disponibilidad.
- Instalación de NNTP que es un protocolo de transporte de noticias, y SMTP para transporte de correos.
- Instalación de sp2 que nos permite hacer la extensión de la capacidad de la base de datos hasta de 75 GB.
- Se limitan el tamaño de la bases de datos de 50 GB para tener un aviso previo en el caso de que crezca desmesuradamente y colapsen los servicios, el límite de la base de datos es de 75 GB, por lo tanto va a enviar una alerta cuando llegue a 50 GB, para poder sacar respaldos y hacer mantenimiento de cuentas.

Para el caso de disponibilidad se configuro el RPC para poder ingresar a los correos fuera de la red interna de la compañía.

3.2 Descripción básica del entorno de trabajo de los servidores GNU/Linux.

Especificación del software de cada una de las maquinas.

3.2.1 Servidor Firewall (UIO-IPT-01)

Este servidor va a ser configurado con iptables.

Diseño y análisis del ambiente de Iptables

Este servidor trabaja con dos tarjetas, WAN para la red externa con la IP 10.0.0.10 y otra LAN para la red interna con la IP 172.21.2.1. Las reglas iptables que se van a aplicar para asegurar la red interna como externa son las siguientes:

- Vaciar las reglas, para asegurarnos de que no exista ninguna regla aplicada con anterioridad.
- Aplicar las políticas por defecto, rechazamos los paquetes de entrada, salida o forward.
- Permitir todas las conexiones en un interfaz local.
- Negar las conexiones del exterior a la interfaz local.
- Permitir el tráfico a la interfaz interna.
- Permitir el tráfico interno.
- Permitir la salida al web externo.
- Hacer enmascaramiento de la red externa a la interna y viceversa.
- Permitir acceso desde LAN a WAN por los siguientes puertos.

  Puerto HTTP www

  Puerto FTP control

  Puerto FTP datos

  Puerto SSH, SCP, SFTP

  Puerto HTTPS/SSL para transferencia segura

  Puerto POP3 e-mail

  Puerto NTP sincronización de tiempo

Puerto IMAP4 internet message access protocol e-mail

Puerto POP3 sobre SSL

Puerto SMTP sobre SSL

- Permitir la salida de LAN a WAN por los siguientes puertos

Puerto HTTP www

Puerto DNS

Puerto SSH, SCP, SFTP

Puerto NTP

Puerto SMTP

El rango de IP que vamos a utilizar para esta red es 172.21.2.0/24, a continuación se va a especificar las IP y nombres correspondientes a cada servidor.

Iptables = UIO-IPT-01 = 10.0.0.10 y 172.21.2.1

OpenLDAP = UIO-OLDAP-01 = 172.21.2.5

Exim = UIO-EXI-01 = 172.21.2.10

OpenCA = UIO-CA-02 = 172.21.2.15

DNS = UIO-DNS-01 = 172.21.2.20

WIN = UIO-WIN-02 = 172.21.2.25

LNX = UIO-LNX-02 = 172.21.2.30

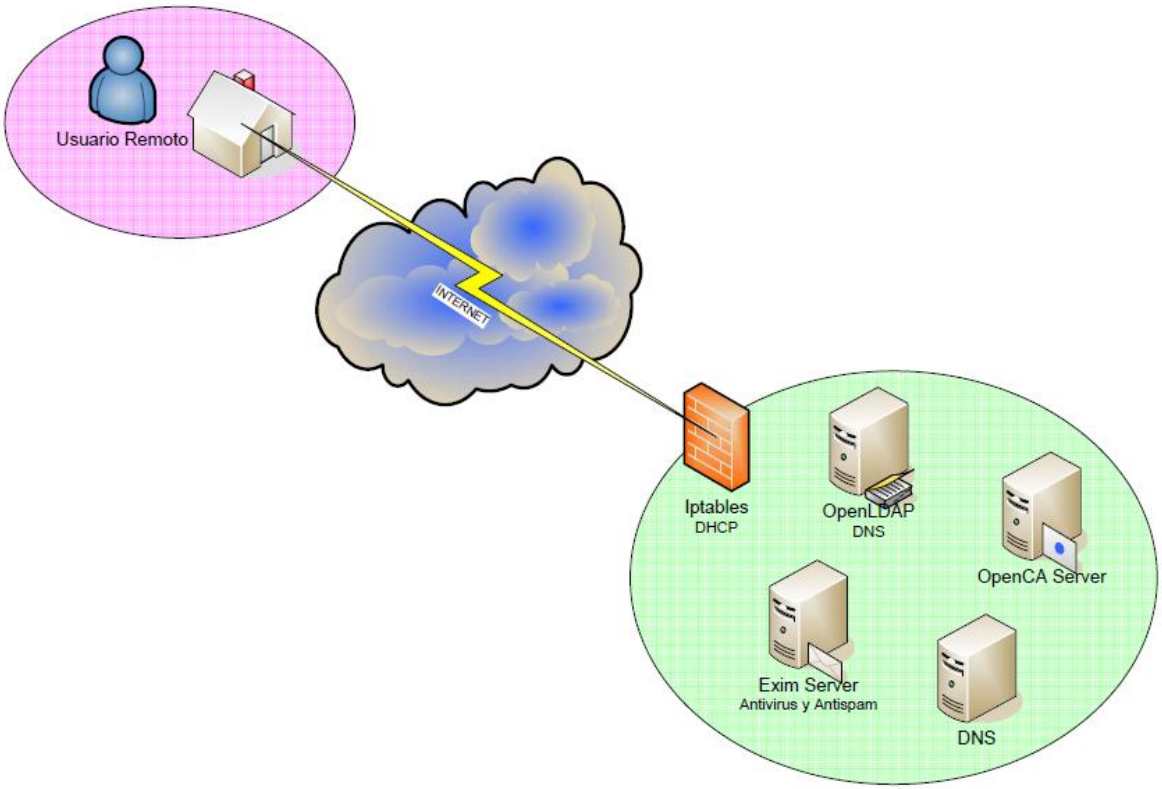


Figura 6. Ambiente Iptables

3.2.2 Servidor Open LDAP (UIO-OLDAP-01)

Este servidor va a ser configurado con OpenLDAP y servicio DNS.

Diseño y análisis del ambiente de directorios

Para realizar el diseño de directorios en Linux es necesaria la utilización de OpenLDAP que nos permite crear el dominio *estudiante.com* y generar una jerarquía de objetos similar a la que se utilizó en el directorio activo de Windows. Así mismo, se implementó el servicio DNS para la resolución de nombres. En el caso interno la resolución de nombres tiene la siguiente estructura:

fw.estudiante.com = 172.21.2.1

dns1.estudiante.com = 172.21.2.5

mail.estudiante.com = 172.21.2.10

ca.estudiante.com = 172.21.2.15

ldap.estudiante.com = 172.21.2.20

3.2.3 Servidor Exim (UIO-EXI-01)

Este servidor será configurado con Exim, spamassasim y clamAV antivirus.

Diseño y análisis del ambiente de Exim

El servidor de Exim trabaja como un agente de transporte de correo electrónico, para una optima protección de spam y virus se implemento los servicios de spamassassin y ClamAV para la protección de virus. En la (figura 7) se puede observar como es escaneado el correo tanto entrante como saliente para mantener la seguridad de los buzones de los usuarios y evitar cualquier amenaza o ataque. Ademas, se configuraron los archivos de Exim para que se autentiquen con el OpenLdap y pueda realizar la importación de los recursos de la red para los diferentes usuarios.

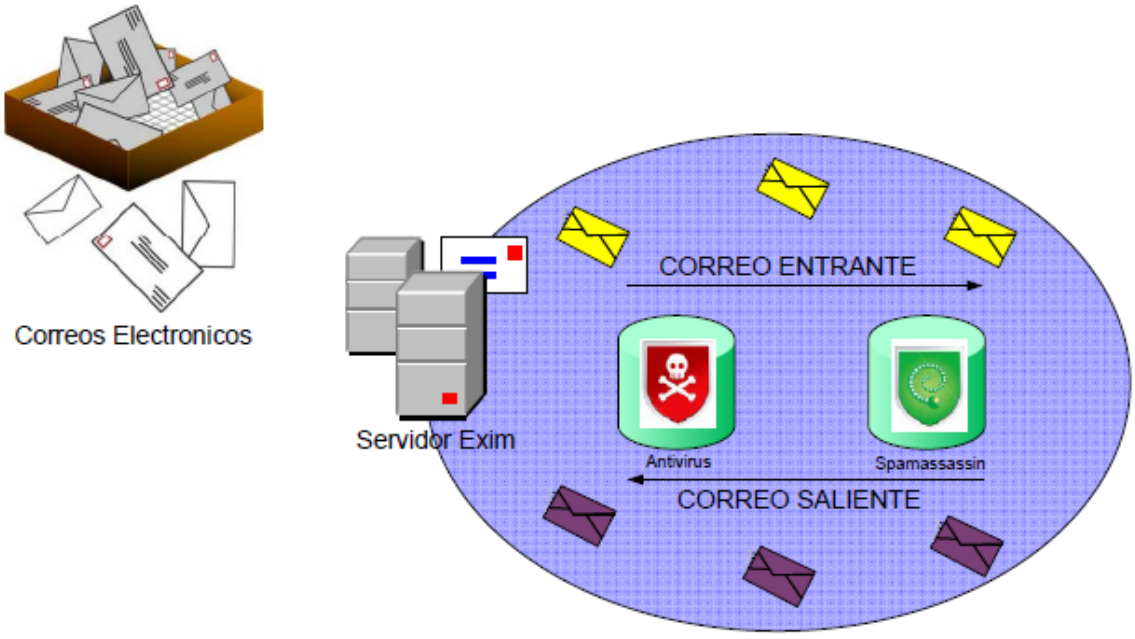


Figura 7. Ambiente del servidor de correo Exim

3.3 Descripción del Servidor Open CA (UIO-CA-01)

Este servidor será configurado con OpenCA constituido por una autoridad de registro y una autoridad de certificación.

Diseño y análisis del ambiente de Clave Pública

Se propone un modelo de infraestructura de Clave Pública, basado en el uso de certificados X.509 versión 3, el modelo está formado por una Autoridad certificadora que es el nodo principal y que define las políticas de certificación para la organización, para definir la ruta de certificación se utilizan los certificados X.509 versión 3, es decir desde el certificado hasta la raíz de su árbol que es la Autoridad de Certificación, facilitando el proceso de verificación.

Función del proceso de certificación

La (Figura 8) muestra el proceso interno de certificación que realiza OpenCA server, se cumplen los pasos enumerados a continuación.

1) Verificación y validación
2) Datos del usuario
3) Clave pública
4) Certificado
5) Publicación
6) Certificado de clave pública

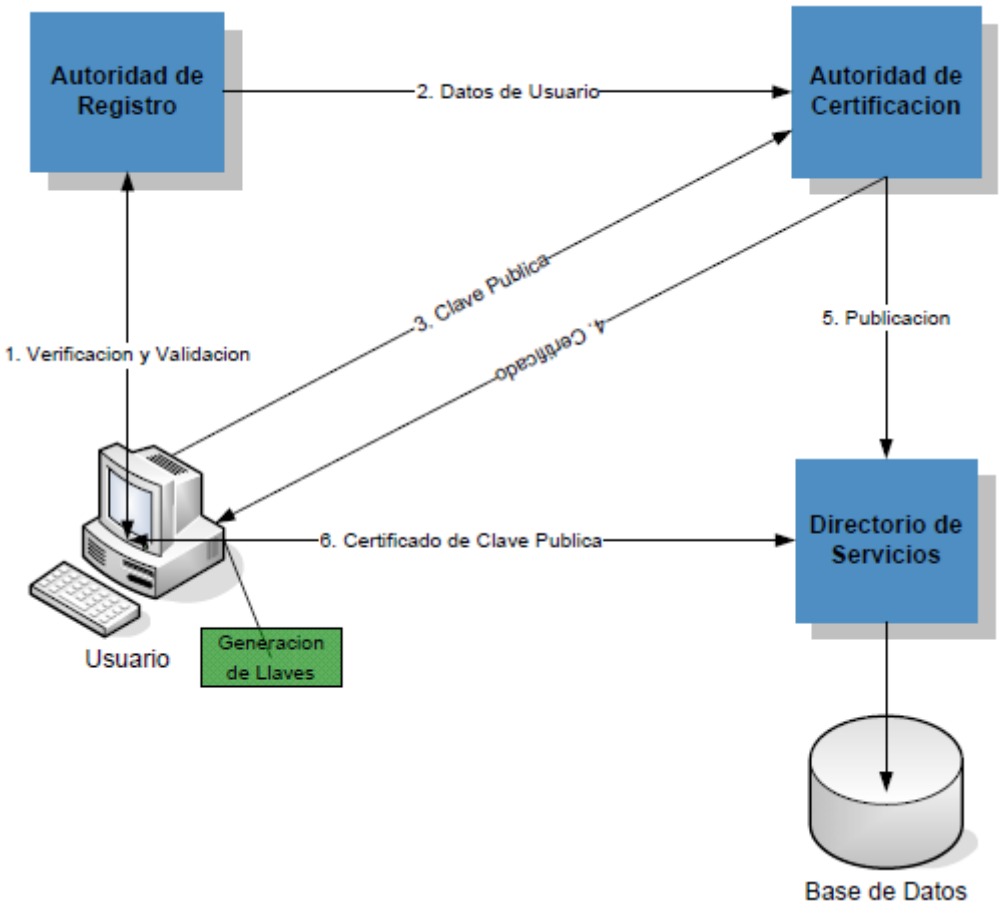


Figura 8. Proceso de certificación interno en el servidor de OpenCA

3.4 Descripción de clientes.

En diferentes sistemas operativos existe un control de las personas que pueden ingresar al sistema y de las acciones que dichas personas están autorizadas a ejecutar. Se los denominara *usuarios* y para controlar las acciones y entradas de cada uno se crearan *cuentas de usuario* en donde se almacenará toda la información y configuración personalizada de cada usuario. [27]

Los procesos de unificación de los clientes en los sistemas operativos varían según la plataforma bajo la que se trabaje.

3.4.1 Cliente Linux (UIO-LNX-01)

Integración al directorio

Para poder integrar los usuarios GNU/Linux al Active Directory usaremos una herramienta llamada “Likewise”, es un software que permite realizar la autenticación al directorio activo con solo instalar el software.

Para poder autenticar a un usuario Linux en un directorio Linux sólo necesitamos ingresar en los archivos de configuración el nombre de hostname que hemos configurado en nuestro ordenador cliente y verificar la configuración de red que es asignada por el DHCP automáticamente.

3.4.2 Cliente Windows (UIO-WIN-01)

Integración al directorio

Para realizar la integración al Active Directory requerimos autenticar el usuario al dominio tesis.com y verificar la configuración de la red ya que el DHCP nos asigna una automáticamente.

[ANEXO 8]

CAPÍTULO 4: IMPLEMENTACIÓN Y PRUEBAS DEL SISTEMA

4.1 Proceso de implementación y pruebas de los equipos.

La implementación de este proyecto varía según la organización en donde se efectúe, debido a que la infraestructura dependerá del número de trabajadores, localización geográfica, capacidades económicas, necesidades tecnológicas de la empresa, etc.

La metodología conocida como modelo cascada, es la que se va a utilizar durante el desarrollo de esta tesis; este modelo da un enfoque metodológico que ordena rigurosamente las etapas del ciclo de vida de un proyecto, es decir que cualquier error en una de las etapas nos conduce necesariamente al rediseño de la infraestructura afectada. Esto se debe al estricto control que se debe mantener durante la vida del proyecto y a su vez de una amplia documentación escrita.

4.1.1 Servidor ISA (UIO-ISA-01)

Proceso de implementación y pruebas de ISA server [ANEXO 1]

- Configuración de tarjetas de red.
- Implementación de ISA Server.
- Pruebas de configuración de tarjetas de red, autenticación al directorio y dominio, funcionamiento del filtrado de paquetes por la aplicación de las reglas.

4.1.2 Servidor Directorio Activo (UIO-ADC-01)

Proceso de implementación y pruebas de Directorio Activo server [ANEXO 2]

- Implementación de Active Directory y DNS.

- Pruebas de configuración de red y autenticación al directorio activo con el usuario creado, funcionamiento del DNS y resolución de nombres internos como externos a la red.

4.1.3 Servidor Exchange (UIO-EX-01)

Proceso de implementación y pruebas de Exchange server [ANEXO 3]

- Implementación de Exchange Server, antivirus y antispam
- Pruebas de configuración de red e integración al dominio, pruebas de envió y recepción de mensajes mediante SMTP, revisión de usuarios con mail y la cola de mensajes, comprobar la aplicación de firmas digitales y certificados.

4.1.4 Servidor OpenCA (UIO-CA-01)

Proceso de implementación y pruebas de OpenCA server [ANEXO 4]

- Implementación de OpenCA
- Pruebas de configuración de red e integración al directorio activo, probar la emisión de certificados y firmas digitales, probar los estados de los certificados.

4.1.5 Servidor Firewall (UIO-IPT-01)

Proceso de implementación y pruebas de Iptables server [ANEXO 5]

- Configuración de tarjetas de red.
- Implementación de ISA Server.
- Pruebas de configuración de tarjetas de red, autenticación al directorio y dominio, funcionamiento del filtrado de paquetes por la aplicación de las reglas.

4.1.6 Servidor Open LDAP (UIO-OLDAP-01)

Proceso de implementación y pruebas de OpenLdap server [ANEXO 6]

- Implementación de Active Directory y DNS.
- Pruebas de configuración de red y autenticación al directorio activo con el usuario creado, funcionamiento del DNS y resolución de nombres internos como externos a la red.

4.1.7 Servidor Exim (UIO-EXI-01)

Proceso de implementación y pruebas de Exim server [ANEXO 7]

- Implementación de Exchange Server, antivirus y antispam
- Pruebas de configuración de red e integración al dominio, pruebas de envió y recepción de mensajes mediante SMTP, revisión de usuarios con mail y la cola de mensajes, comprobar la aplicación de firmas digitales y certificados.

CAPÍTULO 5: ANÁLISIS DE RESULTADOS

5.1 Análisis comparativo de los sistemas operativos.

Para realizar un análisis comparativo debemos considerar las características que hacen a cada uno de los sistemas relativamente mejor que otro. Iniciaremos mencionando que la gratuidad de GNU/Linux se basa en modos de licenciamiento que no involucran transferencia monetaria alguna, sin embargo existen restricciones, debido a la existencia de un contrato que limita y especifica las obligaciones de las partes. La primera de las restricciones y la más importante es la distribución del código fuente, o en algunos casos la prohibición de guardar las modificaciones y no dar a conocer a la comunidad. Por otro lado Microsoft, también tiene software de uso libre, sin embargo, la mayor parte del software para el prototipo que implementamos en esta tesis es software con costo monetario, sin dejar de lado que Microsoft, no libera el código fuente todavía. Es necesario reconocer que montar una infraestructura de red que sea Microsoft representa una inversión alta con una ventaja muy importante que es la de soporte técnico, mientras de GNU/Linux se debe hacer el soporte mediante la comunidad y a expensas de ayuda gratuita; es por eso que se analiza los recursos monetarios y las facilidades que representa cada uno de los sistemas que se desean implementar y se deja opcional de acuerdo a los recursos y capacidades de cada empresa. Cabe recalcar tanto en sistemas GNU/Linux como en Microsoft Windows cumplen con la misma funcionalidad y nos brindan servicios similares, sin embargo, tanto la implementación como la administración varían según el sistema operativo bajo el cual se está trabajando.

Un segundo aspecto a identificar entre las diferencias para la implementación de ambas redes son las características de hardware requeridas, es así que fue necesaria la virtualización de sistemas operativos, con características comparables de hardware para realizar la

implementación. Fue necesario, una mínima capacidad de memoria y disco duro, en el caso de Windows Server 2003 se recomiendan las siguientes características, memoria de 256 MB, 1.2 GB para la instalación de red y 2.9 GB para la instalación del software; mientras que para la infraestructura GNU/Linux es necesario al menos 256 MB de memoria y 4GB de disco disponible para la implementación.

Un tercer aspecto a comparar, son las implementaciones de los servidores, en el caso de Isa Server y un servidor con Iptables, la implementación y la administración es completamente diferente ya que para Isa server se puede configurar reglas mediante un panel que especifica paso a paso la regla que se desea; mientras que Iptables es un archivo que cumple un orden y tiene un formato definido, por lo que resulto más complicado la configuración ya que tomó tiempo estudiar cada una de las reglas y formularlas de acuerdo a nuestras necesidades. Otro caso fue la implementación del Active Directory y OpenLdap, ya que en cuestión de configuración OpenLdap resultó ser poco intuitiva porque es necesario la modificación de archivos específicos con formatos determinados, para lo cual es necesario tener conocimientos más profundos de GNU/Linux y poder realizar estas configuraciones.

5.2 Análisis de resultados de ambos sistemas operativos.

En esta sección podremos analizar la facilidad de implementación, el proceso de comunicación y la seguridad que existe en el prototipo implementado. Además, se analizará la fiabilidad y seguridad de correos electrónicos gracias a la implementación de firmas digitales, autenticación de usuarios y encriptamiento de certificados digitales.

5.2.1 Factibilidad de integración de sistemas híbridos.

Existe factibilidad para integrar diferentes plataformas (Windows o GNU/Linux), ya que los servicios y protocolos que se utilizaron son aplicables en ambas, por lo

que su funcionamiento posee las mismas características pero la administración e implementación diferirán en ambos sistemas. Es necesario mencionar que la conectividad en ambas redes es posible, ya que existen los medios para integrar clientes tanto Windows como GNU/Linux, por lo tanto existe alta disponibilidad de datos e información de la empresa.

Para la integración de las infraestructuras, fue necesario la creación de un DNS externo que se comunique con ambas redes y puede realizar el reenvío de paquetes entre las infraestructuras, mientras que los DNS internos resuelven las direcciones y nombres de su propia red, cumpliendo con una conectividad completa y segura de las redes.

5.2.2 Administración de la red.

La administración de los equipos es algo que va a depender directamente del diseño de la infraestructura de la organización y de la cantidad de centros de datos y sucursales, es decir del tamaño de la organización.

Existen dos tipos de administración, la primera conocida como administración centralizada que es la que ocupamos en nuestro prototipo, en donde un único grupo de IT es responsable de todas las tareas de administración, centralizando los datos y recursos de la red y permitiendo un acceso local como remoto a los usuarios. Una segunda administración es conocida como distribuida, en donde la administración se distribuye en regiones o grupos de la organización, cada grupo administrativo contiene servidores de correo, de directorio, y de certificación, haciendo responsable a cada grupo de controlar su propio sistema.

5.2.3 Seguridad de una infraestructura híbrida.

Los niveles de seguridad se encuentran distribuidos en cada uno de los servidores de la red, descritos a continuación:

Servidor de Firewall.- representan la protección a información valiosa y confidencial de la empresa y también la protección de ataques a la red; así mismo se aplicaron diferentes reglas para el filtrado de paquetes para tener la información y los datos de la organización seguros.

Servidor de correo.- cuenta con reglas de spam y antivirus integrado en cada una de las infraestructuras para filtrar información antes de llegar a los buzones de los clientes, que además se sincroniza con el directorio para asegurar los permisos de usuarios a cada una de las cuentas asignadas.

Servidor de directorio.- cuenta con usuarios con determinados permisos y políticas que limitan sus acciones y el manejo de información, es necesario mencionar que la protección de las claves de los usuarios para acceso al directorio depende de la discreción y manipulación del propio usuario.

Servidor de claves públicas.- cuenta con autoridades que almacena certificados y firmas digitales, permitiendo cifrar y descifrar los datos, la clave pública encripta los datos en un formato ilegible o codificado que solamente la clave privada, correspondiente a este par de claves, puede descifrar el mensaje en un formato legible; cada entidad dentro de este servidor cuenta con diferentes tipos de almacenamiento para la protección de información.

5.2.4 Escalabilidad de la red.

La escalabilidad de la red dependerá exclusivamente del ambiente bajo el cual implemente este prototipo, ya que administrara un número de clientes e información

de acuerdo al tamaño de la organización. También se puede escalar este prototipo para redes wireless, ya que al mejorar el esquema actual del directorio se puede realizar un sistema de autenticación de clientes wireless con openLdap.

CAPÍTULO 6: CONCLUSIONES Y RECOMENDACIONES

6.1 Resumen de actividades

Este trabajo de tesis se realizó con el objetivo de implementar un prototipo con un sistema de seguridad a nivel de correo electrónico integrando sistemas operativos GNU/Linux y Windows permitiendo que el emisor formulase mensajes firmados digitalmente además de la encriptación de los mismos.

Las actividades que se realizaron durante el desarrollo de esta tesis fueron: planteamiento del problema, diseño de la solución, investigación de las etapas dependientes, implementación, realización de pruebas y elaboración del documento.

Etapa de planteamiento del problema

Se dimensionó la red para un ambiente comercial y se estableció el número de servidores y servicios necesarios.

Etapa de diseño de la solución

Se diseñó las características de los servicios, la ubicación y dependencia de los servidores como servicios. Además se analizo la prioridad de cada uno dentro la red.

Etapa de investigación

Se investigó sobre los sistemas de seguridad para ambas redes y se recopilo información sobre la implementación, diseño y administración de cada uno de los servidores.

Se investigó la integración de clientes híbridos para ambas infraestructuras, es decir como autenticar a un usuario Linux a una red Windows y viceversa, para dar facilidades de acceso a los usuarios.

Etapa de implementación

Se implementó un prototipo de red que cumpliera con las necesidades propuestas en el planteamiento del problema, en la cual viabiliza la realización de pruebas.

Etapa de pruebas

Pruebas de autenticación, de envío de mensajes, de identificación de dominio, filtro de paquetes, de asignación de direcciones IP dinámicas, resolución de nombres DNS.

Realización de pruebas con usuarios locales y remotos.

Elaboración de documento

Se planteó una estructura que permita explicar de manera detallada y progresiva de la elaboración de esta tesis.

6.2 Conclusiones

Se concluye que la factibilidad de implementación, funcionamiento y comunicación de un sistema con características híbridas Windows, GNU/Linux son reales, ya que el prototipo que usamos, prueba la seguridad a nivel de correo electrónico mediante autenticación de usuarios híbridos, encriptación de información con certificados digitales y seguridad en las transacciones con firmas digitales dando fiabilidad a la información. Además, de probar la interconectividad de las plataformas hibridas.

La implementación de esta tesis se puede ajustar a la infraestructura de pequeñas y medianas empresas ya que cuenta con servidores y servicios de una red básica, siendo un aporte importante para las mismas. Cada uno de los servidores implementados aportó característi-

cas de seguridad en la red, ampliando el alcance de esta tesis y los niveles de seguridad dentro del ambiente que se realizaron las pruebas.

Tener una infraestructura de clave pública (OpenCA) centralizada constituida por una autoridad de certificación y registro, fue suficiente para satisfacer las necesidades de este prototipo y probar el funcionamiento de claves, certificados y firmas digitales. Se debe mencionar que el servidor de OpenCA sirvió para crear las firmas y certificados digitales, pero no se logro la administración de la misma dentro de las infraestructuras hibridas, por lo que se recomienda que las autoridades de certificación tienen que ser introducidas de forma reglamentada, ya que dan fe de los usuarios que poseen algunos atributos y calificaciones necesarias para realizar ciertas transacciones.

La implementación y administración de servidores en sistemas operativos GNU/Linux es más complicada, ya que para la configuración es necesario conocer la estructura de archivos, inicialización de servicios, comandos para monitoreo, etc. Los que no resultan ser intuitivos y es necesario tener conocimientos de sistemas operativos GNU/Linux. Asimismo, no todos los servidores bajo el sistema operativo GNU/Linux, cuentan con paneles administrativos, dificultando un poco más las tareas de control y verificación que se realizaron para probar la implementación de esta red.

La comunicación de las infraestructuras se lo consiguió debido a la implementación de un DNS-master que aseguró el reenvío de correos electrónico de una red a otra obteniendo la integración de las infraestructuras que se propuso para esta tesis.

6.3 Recomendaciones

- Se recomienda realizar un análisis previo a la implementación de este prototipo, para realizar el análisis de los requerimientos y de la organización o persona que la desee implementar, de esta manera se analizara

- Asimismo se invita a analizar los requerimientos mínimos de hardware de acuerdo a las mejores prácticas de cada uno de los sistemas operativos, y también considerar la implementación virtual como se lo realizó en este prototipo. De esta manera para poder probar los propósitos de esta tesis, las características básicas necesarias son; un servidor de claves públicas y un servidor de directorios con MTA; sin embargo para mayor seguridad se implemento un servidor firewall y un servidor de correo independiente, el cual probó su funcionamiento de manera correcta respecto a los objetivos de los objetivos de seguridad a nivel de correo electrónico, para este prototipo propuesto.
- Se recomienda además la actualización del software en Windows y la instalación de los service pack para mejor funcionamiento; en el caso de GNU/Linux la implementación del software con la última versión de la distribución que se vaya a utilizar.
- Cuando existen entornos numerosos con múltiples servidores y usuarios, se recomienda plantearse la necesidad de distribuir las tareas de certificación y registro y definir varias autoridades, con el propósito de especificar los procedimientos particulares que cada una tiene, mejorando la administración de las claves, certificados y firmas digitales en cada una de las áreas distribuidas.
- Para finalizar invito a incrementar el uso de seguridad a nivel de correo electrónico ya que los beneficios que representa tener información autentica, fiable y confidencial son incalculables.

BIBLIOGRAFIA

1) Ulloa, Héctor. *Microsoft Windows Server 2003* (Sep. 2007) Obtenido en línea el 12 de noviembre 2009. Disponible en: http://www.monografias.com/trabajos14/microsoftwindows/microsoftwindows.shtml

2) Microsoft Corporation. *Fundamentos Técnicos Windows Server 2003* (13 Sep. 2006) Obtenido en línea el 15 de noviembre 2009. Disponible en: http://www.microsoft.com/spain/windowsserver2003/techinfo/docs/fundamentos_tecni-cos.aspx#Fundamentos%20Empresariales%20de%20Windows%20Server%202003

3) Ferrer, Fernando y Terrasa, Andres. *Curso de Integración de Sistemas Linux/Windows* (Jun. 2006) Obtenido en línea el 15 de noviembre 2009 Disponible en: http://fferrer.dsic.upv.es/cursos/Integracion/html/index.html

4) Microsoft Corporation. *Guía de referencia técnica de Microsoft Exchange 2003* (12 Dic. 2006) Obtenido el 1 de diciembre 2009

5) Noel, Michael. *ISA Server 2004 UNLEASHED* (29 Ago. 2005) Obtenido en línea el 5 diciembre 2009. Disponible en: http://**xchm**.sourceforge.net

6) Microsoft Corporation. *Microsoft Internet Security and Accelerator Server* (11 Mar. 2009) Obtenido en línea el 8 diciembre 2009. Disponible en: http://www.microsoft.com/spain/isaserver/default.mspx

7) IBM. *Linux Network Administration, GNU*. Obtenido el 10 diciembre 2009.

8) Pinheiro Malere, Luiz Ernesto. *El LDAP-Linux-Como es* (1999) Obtenido en línea el 8 diciembre 2009. Disponible en: http://es.tldp.org/COMO-INSFLUG/COMOs/LDAP-Linux-Como/LDAP-Linux-Como-1.html

9) Hazel, Philip. *The Exim SMTP Mail Server* (19 Feb. 2009) Obtenido en línea el 11 diciembre 2009. Disponible en: http://www.uit.co.uk/exim-book

10) Linux Para Todos. *Servidor Firewall* (12 Nov. 2008) Obtenido en línea el 12 diciembre 2009. Disponible en: http://www.linuxparatodos.net/portal/staticpages/index.php?page=servidor-firewall

11) De la Fuente, Toni. *Intecna Soluciones. Infraestructura de Clave Pública con Software Libre (*2004) Obtenido el 15 diciembre 2009.

12) Garcia, Rafael. *Gestión y administración de Windows Server 2003*.Obtenido el 15 noviembre 2010.

13) IBM. *Linux Network Administration, LDAP*. Obtenido el 3 de enero 2010.

14) Microsoft Corporation. *Exchange Server 2003* (6 Dic. 2006) Obtenido en línea el 3 de enero 2010. Disponible en: http://technet.microsoft.com/en-us/library/bb123968(EXCHG.65).aspx

15) Creative Commons. *Simple Mail Transfer Protocol*. Obtenido en línea el 5 de enero 2010. Disponible en: http://es.kioskea.net/contents/internet/smtp.php3

16) Ferrer, Fernando y Terrasa, Andres. *Administracion Avanzada de Linux*. (Ene. 2004) Obtenido en línea el 8 de enero 2010. Disponible en: http://fferrer.dsic.upv.es/cursos/Linux/Avanzado/HTML/index.html

17) Antivirus. *ESET Mail Security para Exchange Server* (2010) Obtenido en línea el 28 de marzo 2010. Disponible en: http://www.antivirusgratis.com.ar/notas/8379/eset_lanza_eset_mail_security_para_microsoft_exchange_server

18) Exim Home Page. *Exim*. Obtenido en línea el 13 de enero 2010. Disponible en: http://www.exim.org/

19) Yanez, Ricardo. *Spamassassim con Exim4 en Debian* (13 Sep. 2009) Obtenido en línea el 13 de enero 2010. Disponible en: http://wiki.debianchile.org/EximSpamAssassinDebian#bayes

20) *ClamAV* (2009) Obtenido en línea el 13 de enero 2010. Disponible en: http://www.clamav.net/about/lang-pref/en/

21) Field, Julian. *What is MailScanner* (2006) Obtenido en línea el 13 de enero 2010. Disponible en: http://www.mailscanner.info/intro.html

22) *Firewall* (2008) Obtenido en línea el 15 de enero 2010. Disponible en: http://www.elrincondelprogramador.com/default.asp?pag=articulos/leer.asp&id=14

23) Tanenbaum, Andrew. *Computer Network, Criptografia* (Nov 2008) Obtenido el 3 de enero 2010.

24) EuroLogic Data Protection System. *Infraestructura de clave publica PKI* (2005) Obtenido en línea el 3 de enero 2010. Disponible en: http://www.eurologic.es/soluciones/que-es-pki.htm

25) Nist, National Institute of Standards and Technology. *Public Key Infraestructure Study* (Abr. 1994) Obtenido en línea el 3 de enero 2010. Disponible en: http://www.nist.com

26) Vmware. *Vmware* (12 Mar. 2010) Obtenido en línea el 5 de enero 2010. Disponible en: http://downloads.vmware.com/d/info/datacenter_downloads/vmware_server/2_0

27) Ferrer, Fernando y Terrasa, Andres. *Administracion Basica de Linux.* (Ene. 2004) Obtenido en línea el 20 de enero 2010. Disponible en: http://fferrer.dsic.upv.es/cursos/Windows/Avanzado/index.html

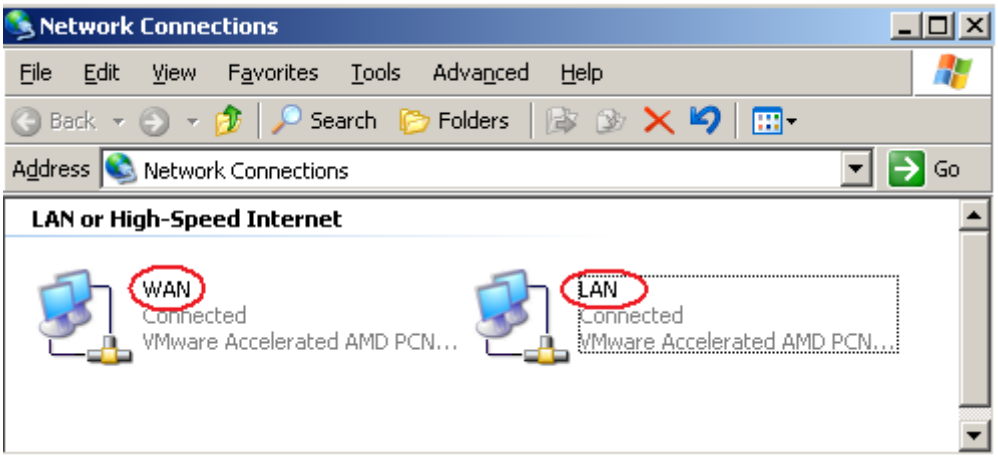
ANEXOS

ANEXO 1

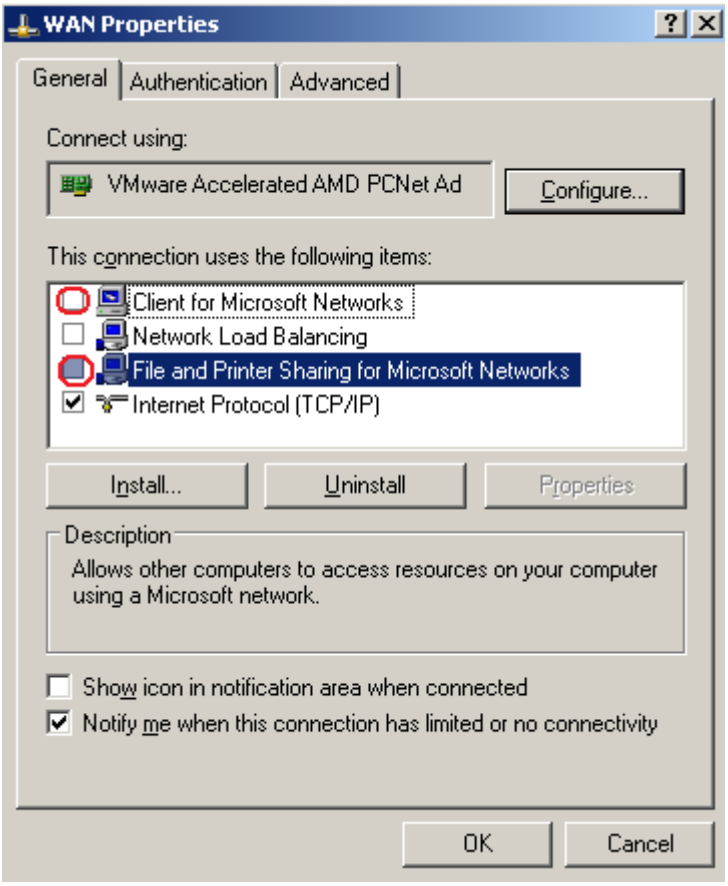
Proceso de implementación y pruebas de ISA server 2006

Para la implementación de ISA server es necesario tener dos tarjetas una que controle el tráfico interno y otra externo de la maquina.

1. Verificamos la existencia de dos tarjetas de red, en conexiones de red vemos dos tarjetas una llamada WAN y otra LAN, como se muestra en la figura a continuación.



2. Verificar las propiedades de la tarjeta WAN en donde deshabilitamos las opciones de clientes para la red de Microsoft y también para compartir las impresoras y archivos como se ve en la figura, esto se hace para tener más seguridad ya que no queremos que estas opciones estén habilitadas para los clientes externos.



3. En las opciones de TCP/IP verificamos la configuración de la tarjeta de red WAN.

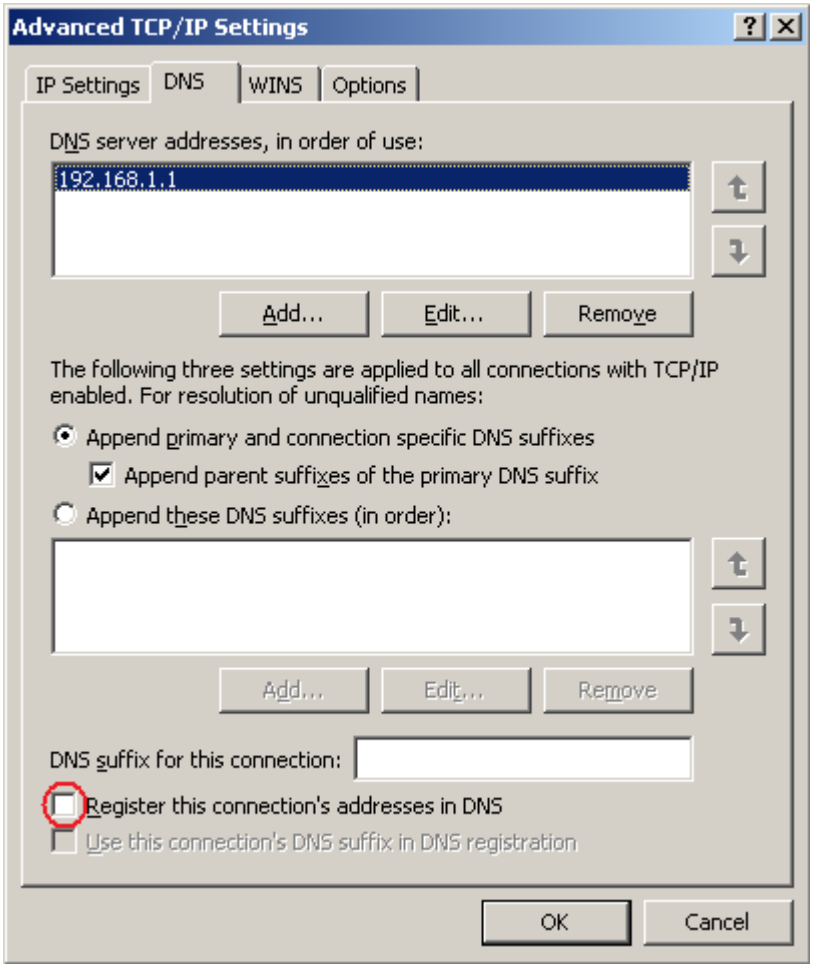
   Dirección IP: 10.0.0.5

   Mascara de subred: 255.255.255.0

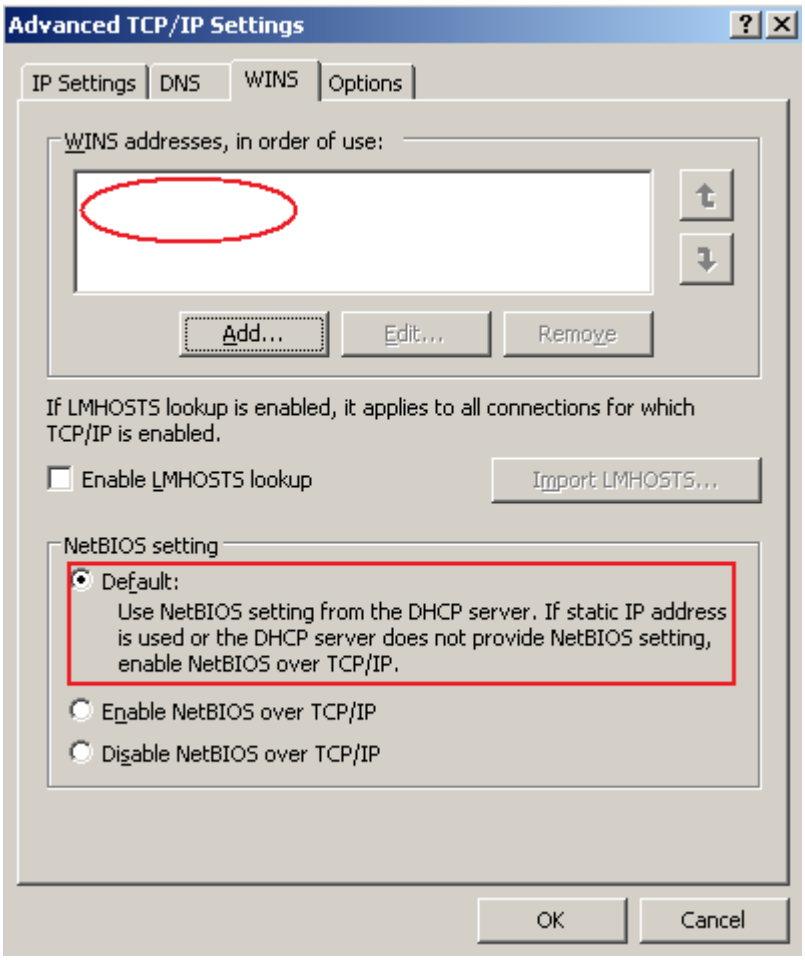
   Gateway: 10.0.0.1

   DNS server: 192.168.1.1

4. En configuraciones avanzadas, en la pestaña de DNS verificamos que el DNS sea 192.168.1.1 y quitamos el check del casillero que dice registrar esta conexión al DNS ya que no queremos que la conexión externa conste en nuestro registro de red interna.

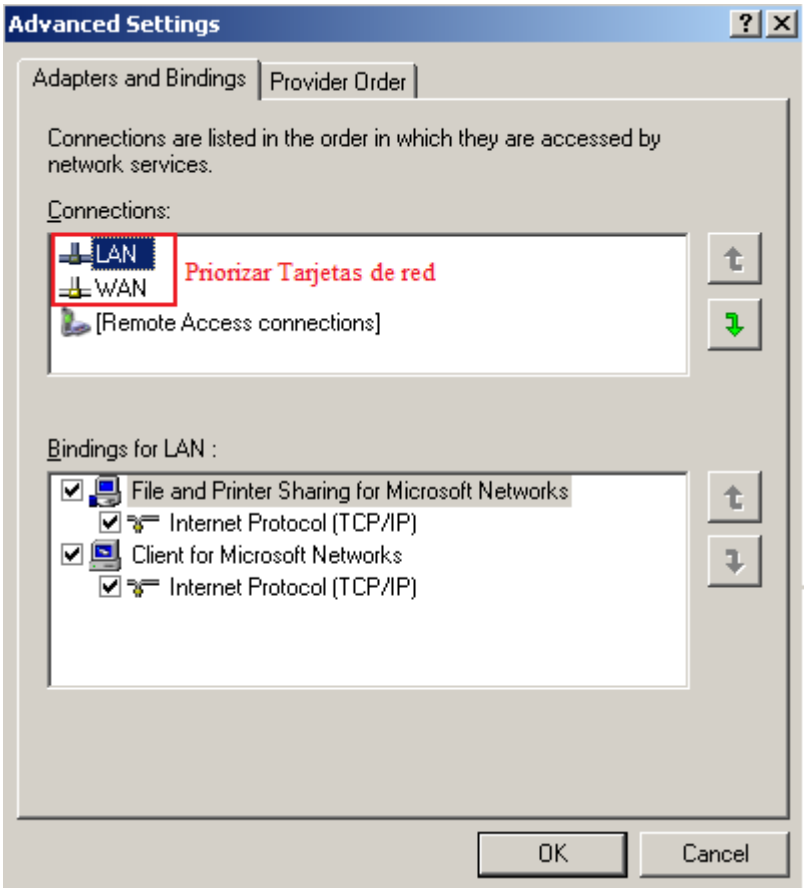


5. Además verificamos que el WINS este deshabilitado, vamos a la pestaña de WINS y verificamos que no exista ninguna dirección de WINS y que el NetBIOS este seleccionado el default.



6. Debemos configurar la prioridad de las tarjetas en conexiones de red, vamos a opciones avanzadas y en adapters and bindings, realizamos la priorización de las tarjetas como se muestra en la figura a continuación, la LAN esta sobre la WAN siendo esta mas prioritaria.

   Cabe recordar que para priorizar las tarjetas de red, debemos poner la LAN antes que la WAN ya que cuando haga la resolución de nombres pregunte al DNS interno y se autentique al Directorio Activo, sino va a preguntar el Internet externo y va a devolver error ya que no resuelve el nombre tesis.com porque no existe en el inter-net.



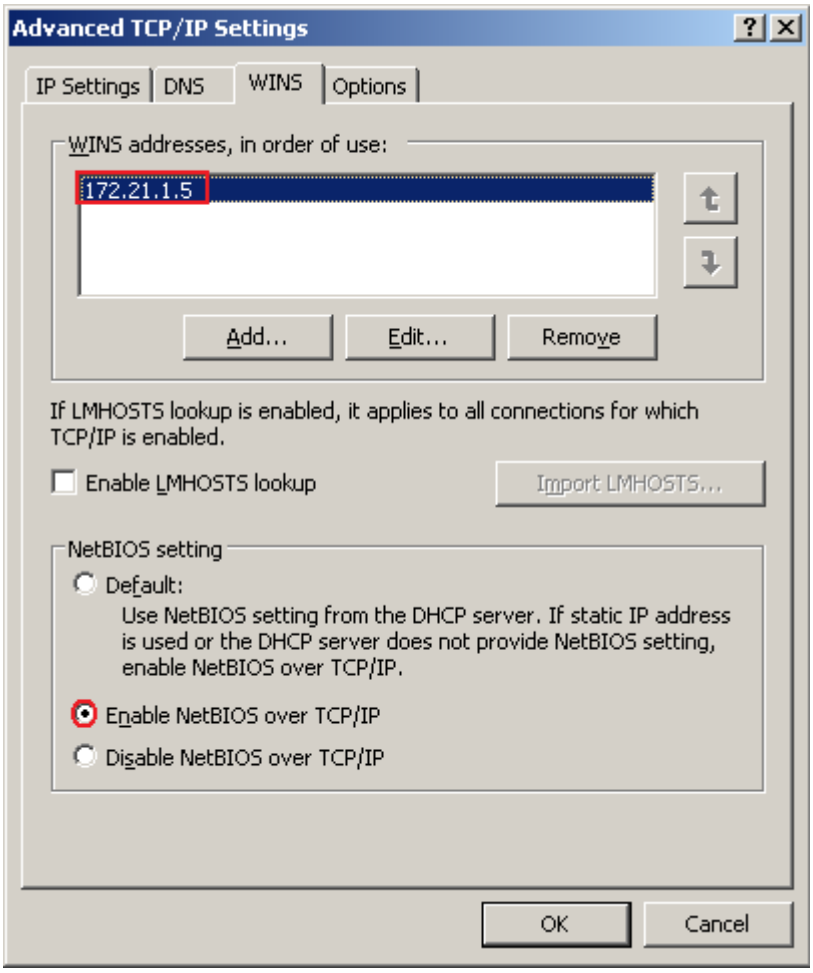
7. Configuramos la tarjeta de red LAN, debemos recordar que la tarjeta interna de un servidor ISA nunca lleva Gateway.

   Dirección IP: 172.21.1.1

   Mascara de subred: 255.255.255.0

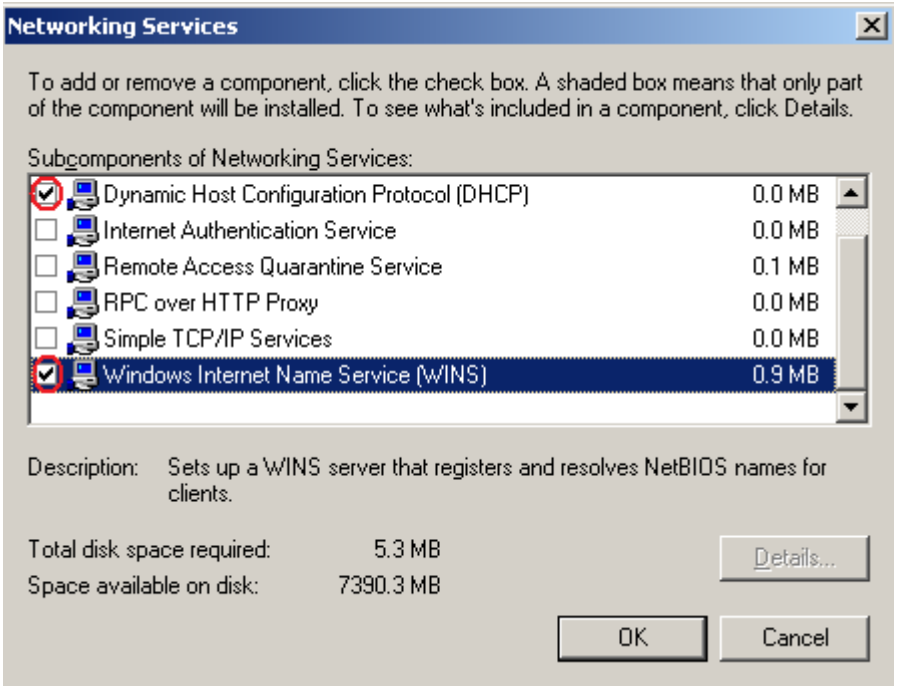
   DNS server: 172.21.1.5

8. En la pestaña de WINS. Se coloca la dirección del Directorio Activo 172.21.1.5 y se escoge la opción de habilitar el BIOS sobre TCP/IP, como se muestra en la figura.

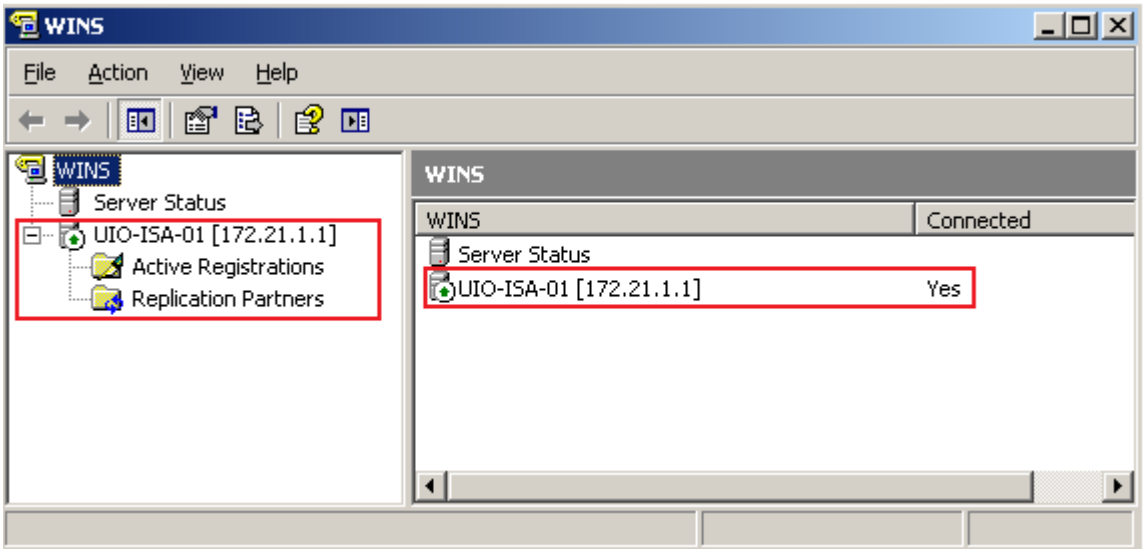


Configuración de WINS y DHCP

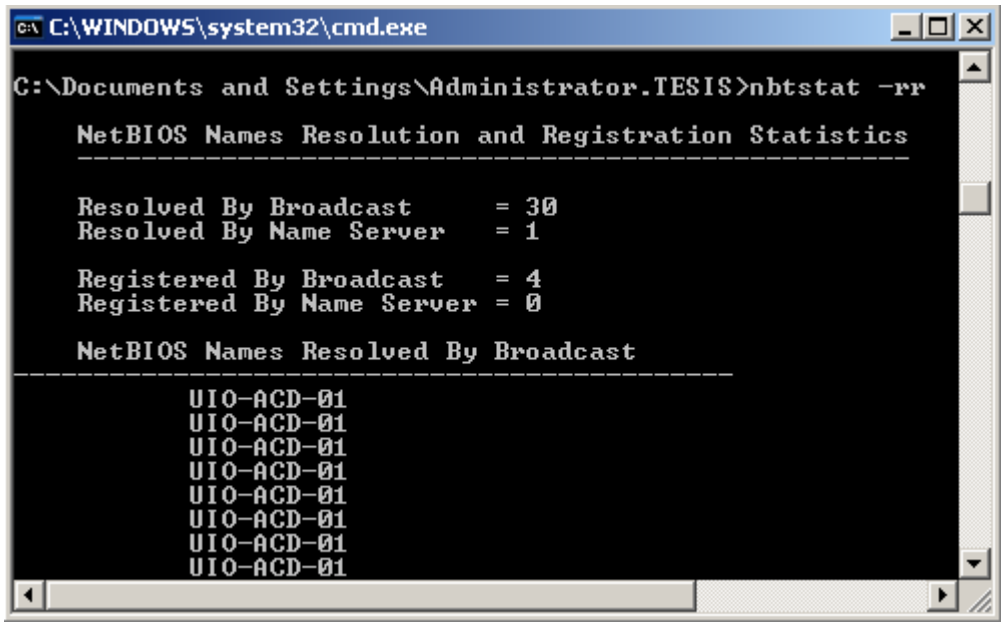
1. Instalar el servicio de WINS, ir a Panel de Control posteriormente a Agregar/ Quitar programas, después Agregar/Quitar componentes y habilitamos la opción de WINS y DHCP en los servicios de red, como se ve en la figura.



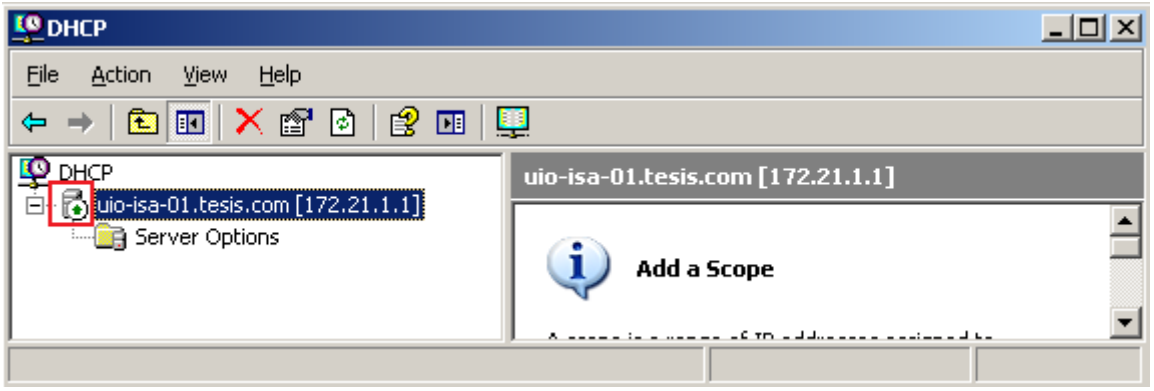
2. Una vez instalado WINS vamos a la consola en donde nos permite administrar los registros activos y las replicaciones y podemos ver como el ISA esta activado, WINS tiene el objetivo de proporcionar una base de datos distribuida en las que se registran y consultan asignaciones dinámicas de nombres NetBIOS a direcciones IP, esta configuración es necesario para configurar el ISA server, pero no la ocuparemos para demostrar ningún funcionamiento en esta tesis.



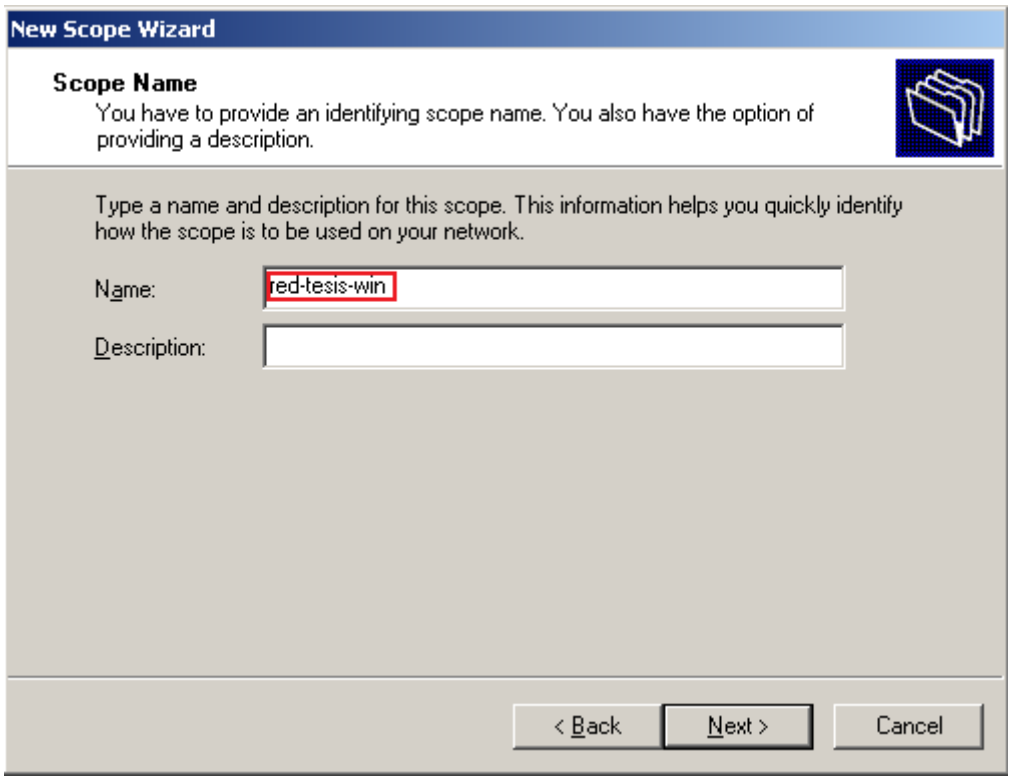
3. Para forzar el registro necesitamos hacerlo mediante consola para que se registre la red interna. Utilizando *nbtstat –rr* para iniciar una solicitud de liberación de nombre en el servidor WINS, en la figura siguiente nos muestra la resolución de nombres de Net-BIOS y vemos que es la de UIO-ADC-01 que es la máquina de directorio activo.



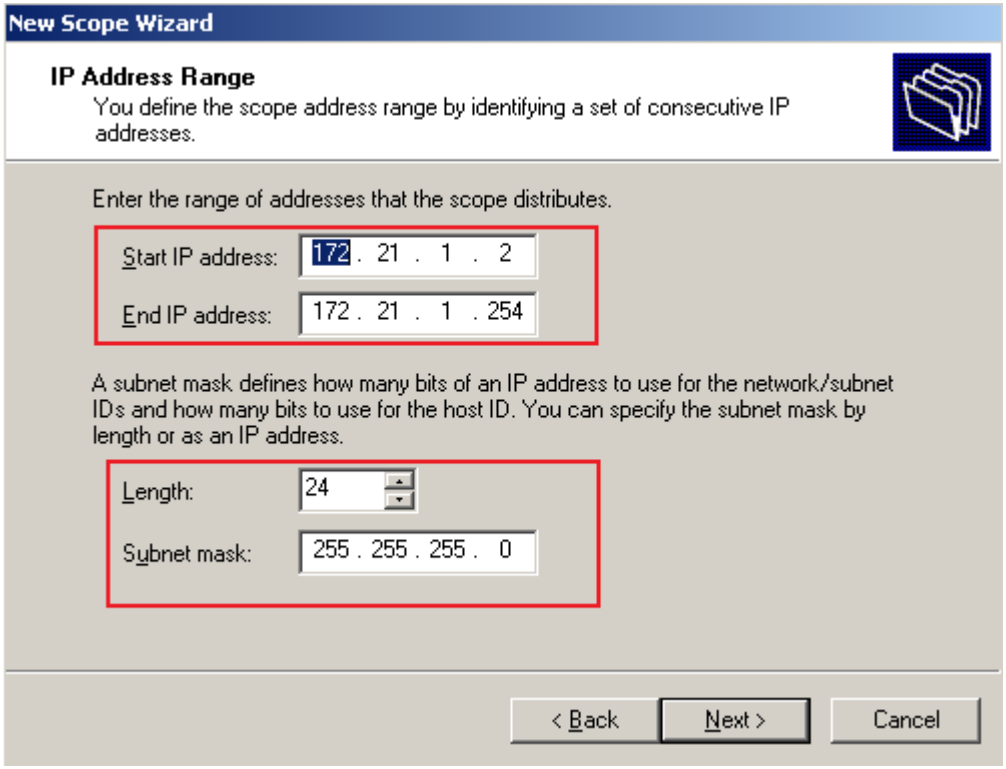
4. Verificamos la consola del protocolo DHCP, y vemos que el servicio esta iniciado y autorizado ya que esta en verde, para poderlo autorizar hacemos click derecho (Aut-horize), va al Directorio Activo y le dice que este servidor está autorizado para asignar direcciones IP



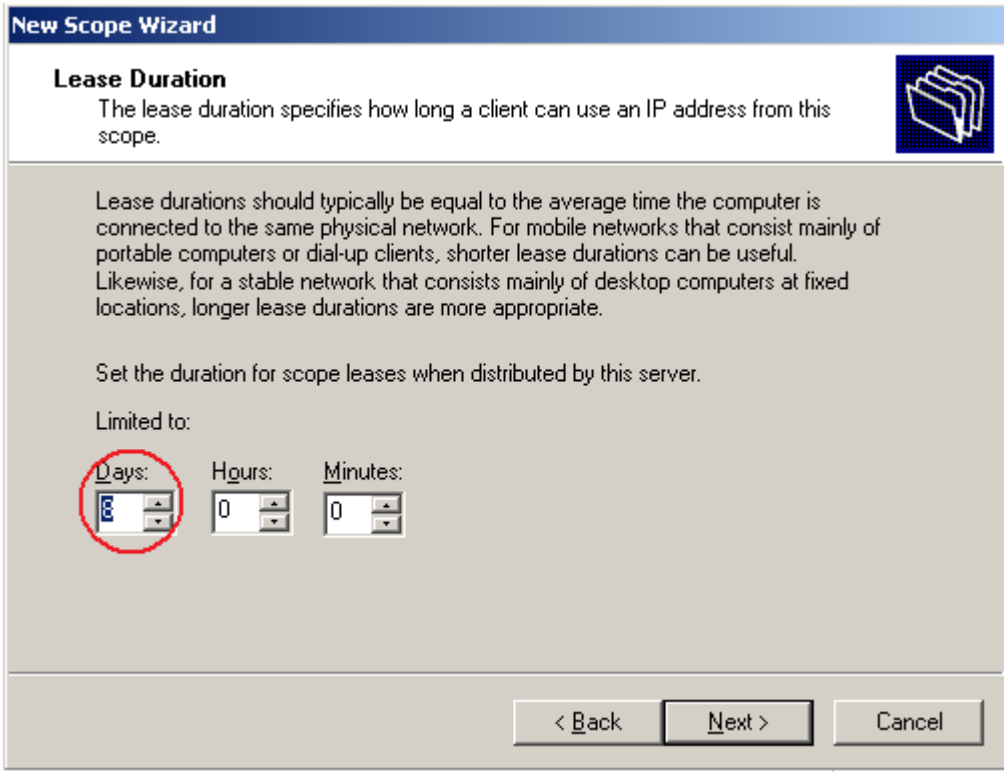
5. Creamos un nuevo scope es decir un rango para asignar direcciones IP dinámicamente a los usuarios que quieran formar parte de la red, hacemos click derecho seleccionamos new scope y asignamos el nombre



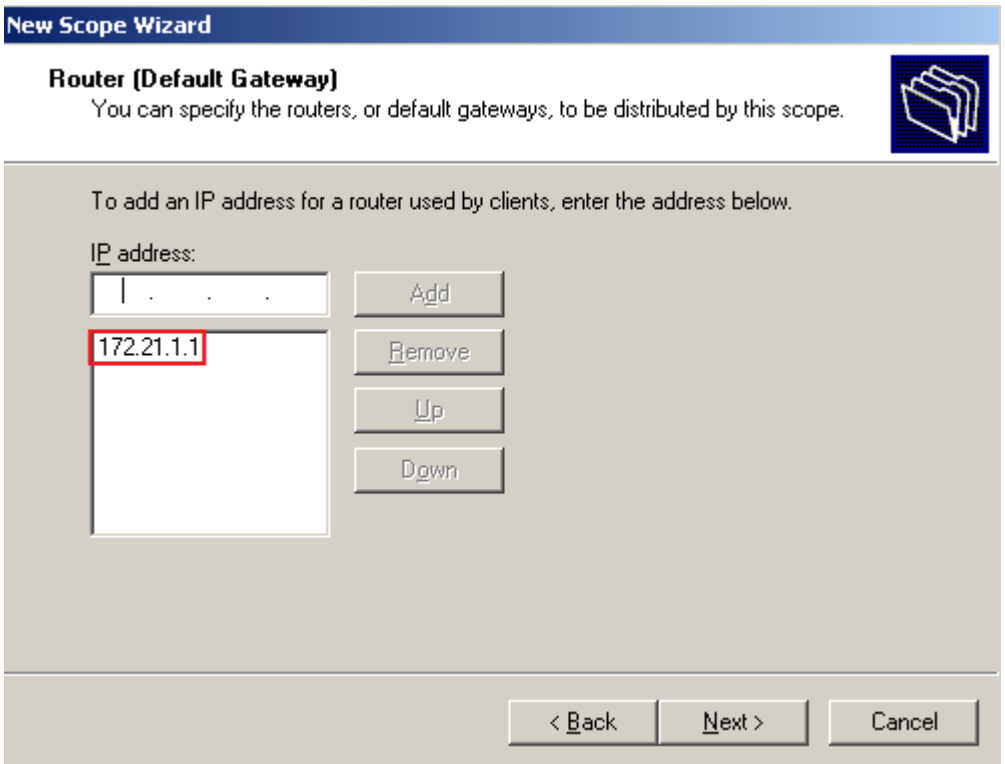
6. Especificamos el alcance de las redes como se señala en la figura a continuación y se designa la longitud de nuestra red y la máscara de red.



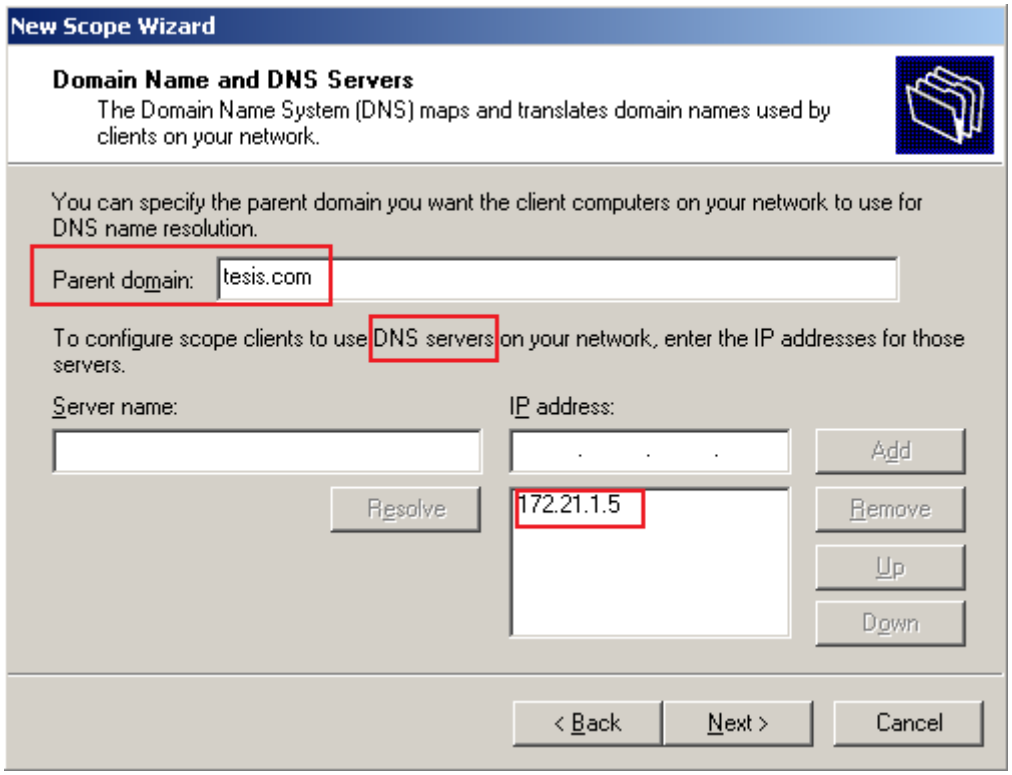
7. Colocamos siguiente en la opción para excluir a alguna maquina ya que no deseamos excluir a ninguna dentro de nuestra red.
8. Especificamos la duración de la IP en el cliente, y dejamos la que está por default que son 8 días.



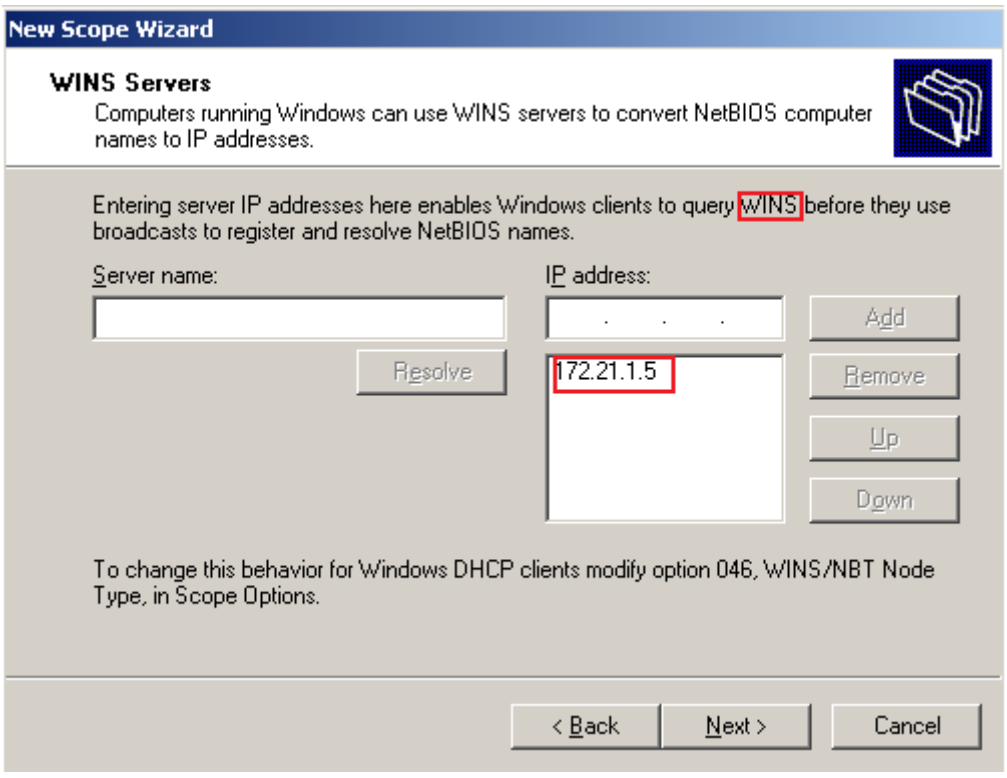
9. Configuramos opciones avanzadas. Asignamos el default Gateway en nuestro caso el ISA con la IP 172.21.1.1



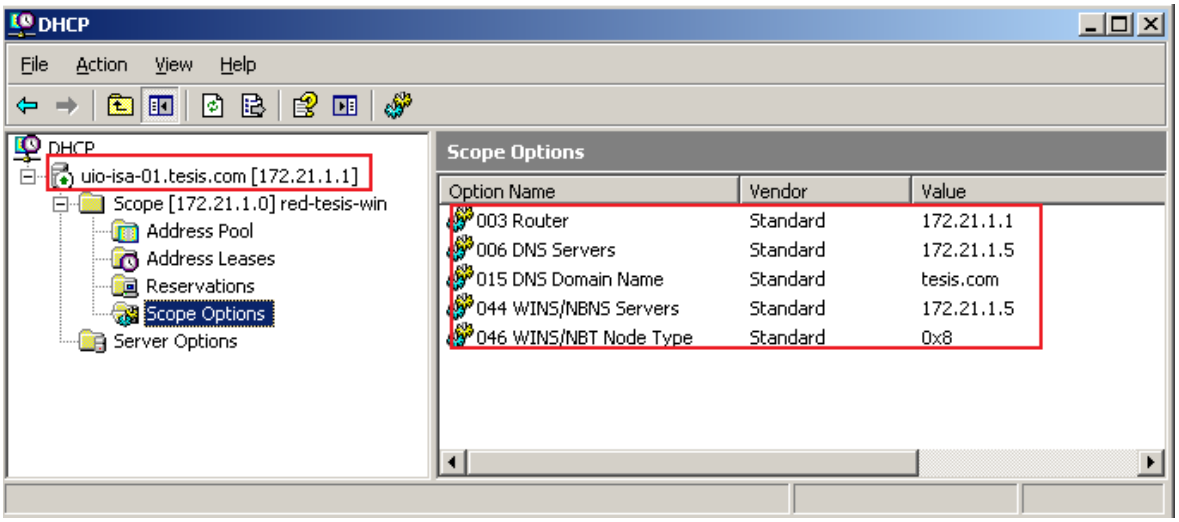
10. Configuramos además el dominio tesis.com y el DNS 172.21.1.5 bajo el que se va a trabajar.



11. Configuramos el WINS que va a utilizar en este caso 172.21.1.5

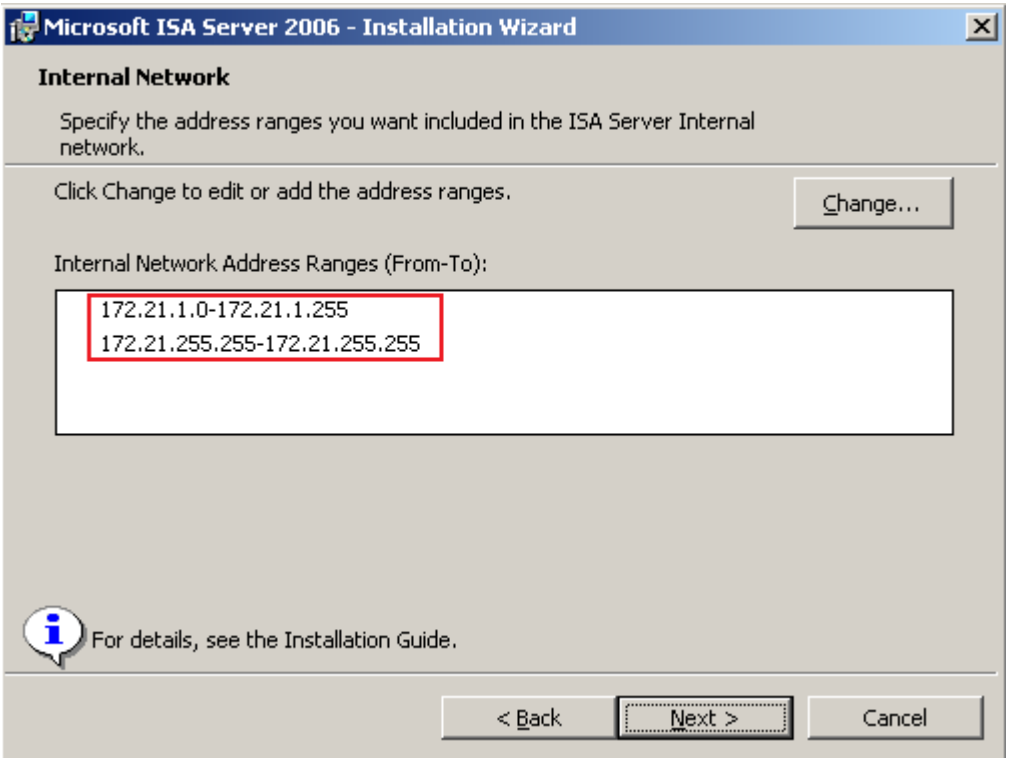


12. Para finalizar la instalación, aceptamos activar el scope ahora. Observamos la configuración del nuevo scope. El router nos especifica la máquina de ISA server, el DNS la maquina en donde está configurad, se especifica además el nombre del dominio en el que se trabaja que es tesis.com y la maquina que tiene WINS. Además se configura el tipo de nodo hibrido 0x8 que es una opción para hacer broadcast en el caso de que el WINS especificado anteriormente no está funcionando manda un broadcast para encontrarlo.

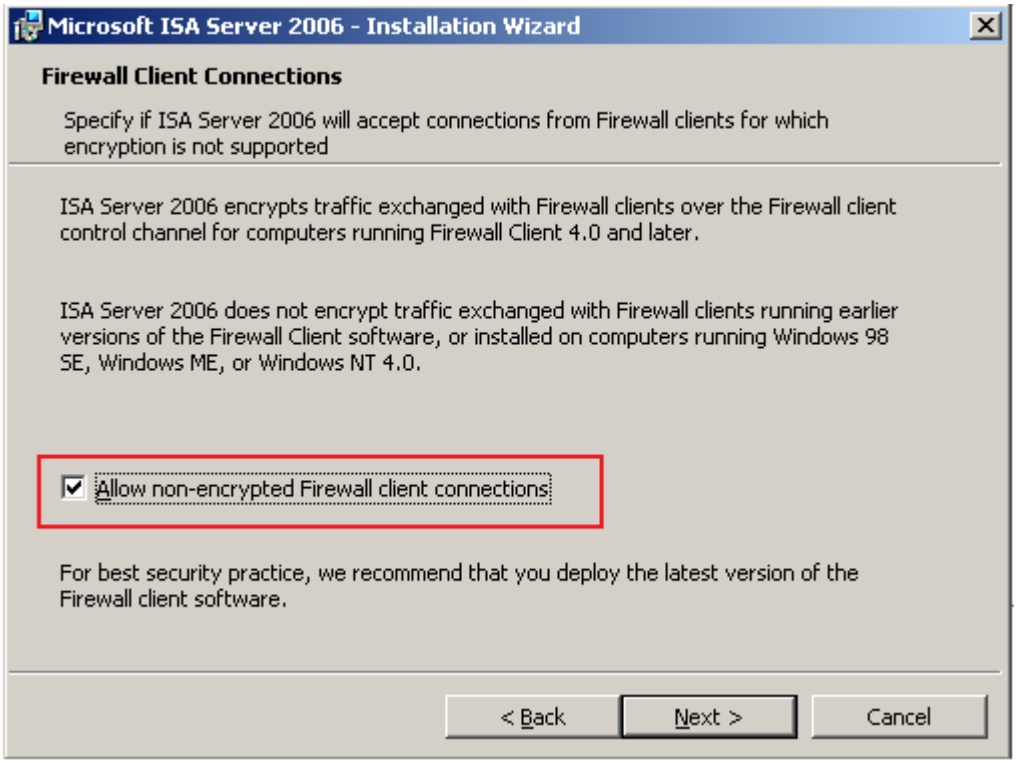


Configuración de ISA Server

1. Realizamos la instalación del ISA server con una instalación personalizada. Implementamos la configuración de la red interna 172.21.1.0 – 172.21.1.254



2. En la configuración habilitamos la opción para permitir al firewall los clientes no encriptados

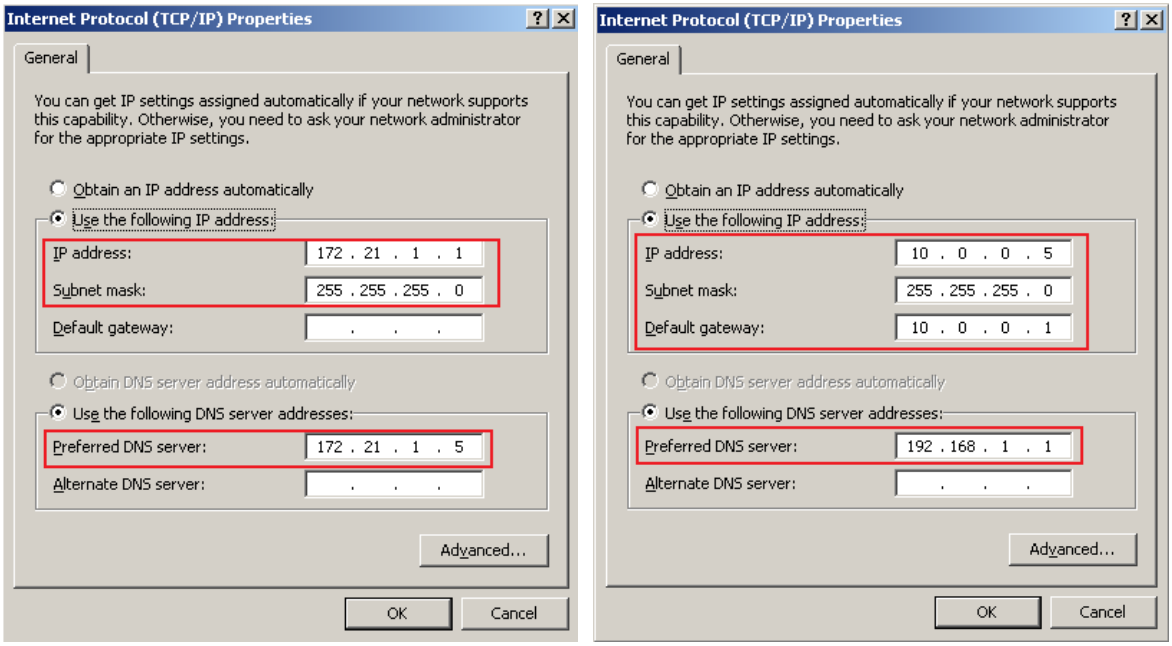


3. Hacemos la instalación del sp1 para ISA server. Finalizamos la instalación y reiniciamos el sistema.

Pruebas

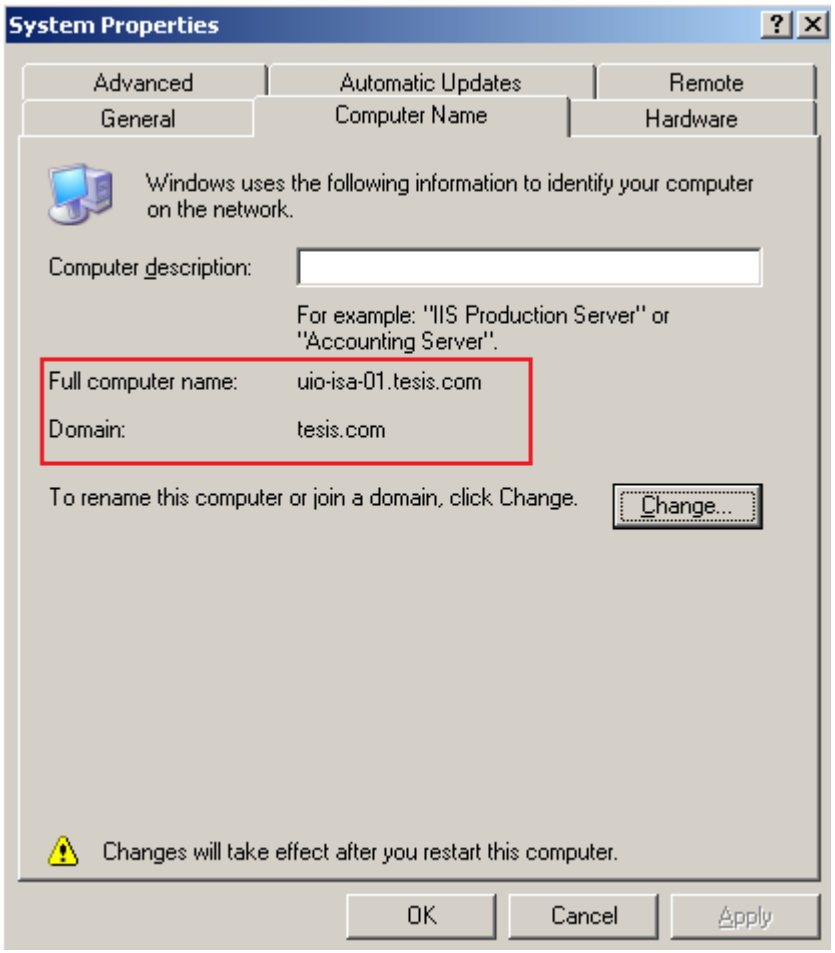
- Configuración de tarjetas de red.

Para probar la configuración de red, podemos revisar las propiedades de cada tarjeta de red y verificar las propiedades TCP/IP de las maquinas.

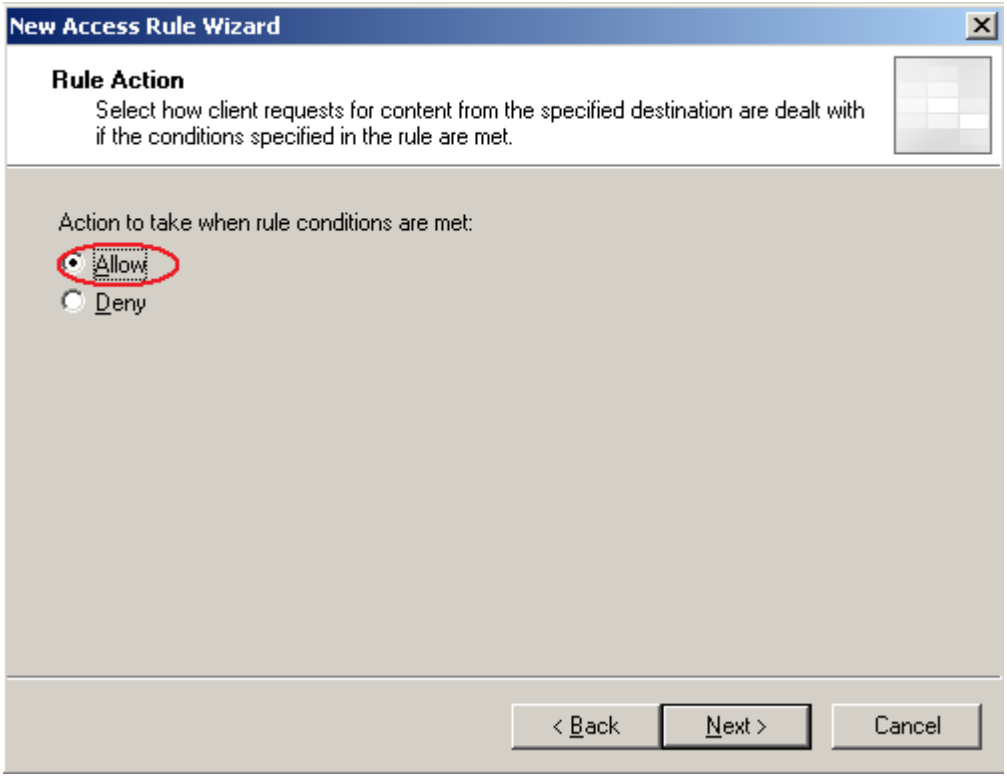


- Autenticación al directorio.

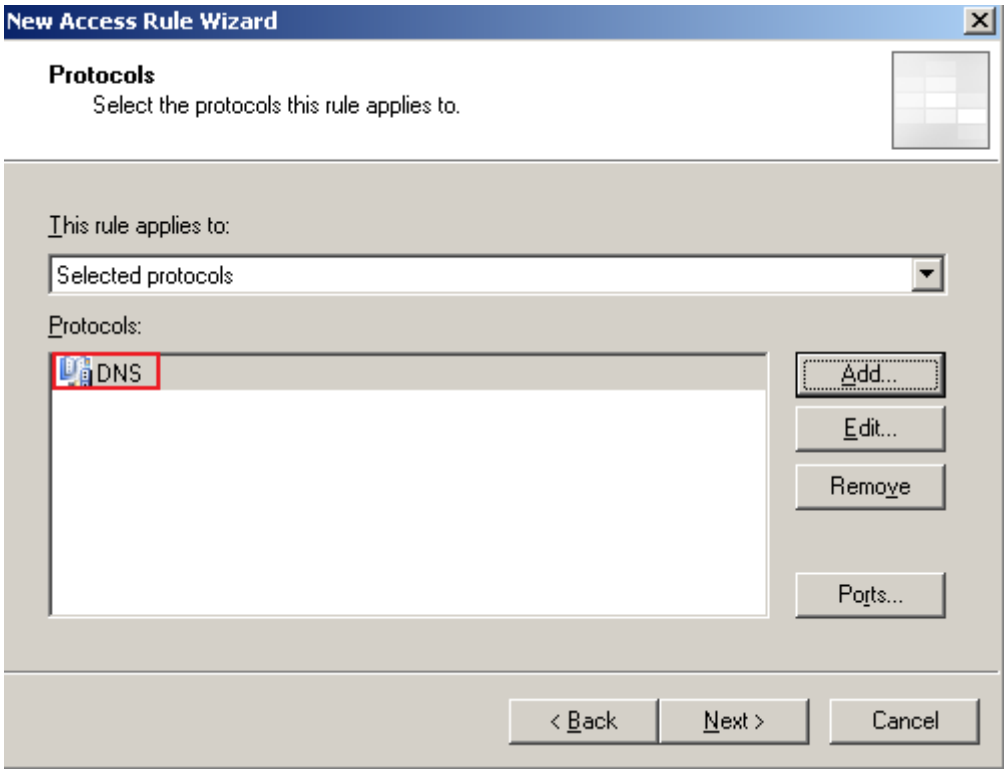
Para autenticarnos al directorio activo es necesario cambiar el nombre de nuestra maquina en este caso va a ser uio-isa-01.tesis.com y el nombre del dominio va a ser tesis.com como se muestra en la figura.



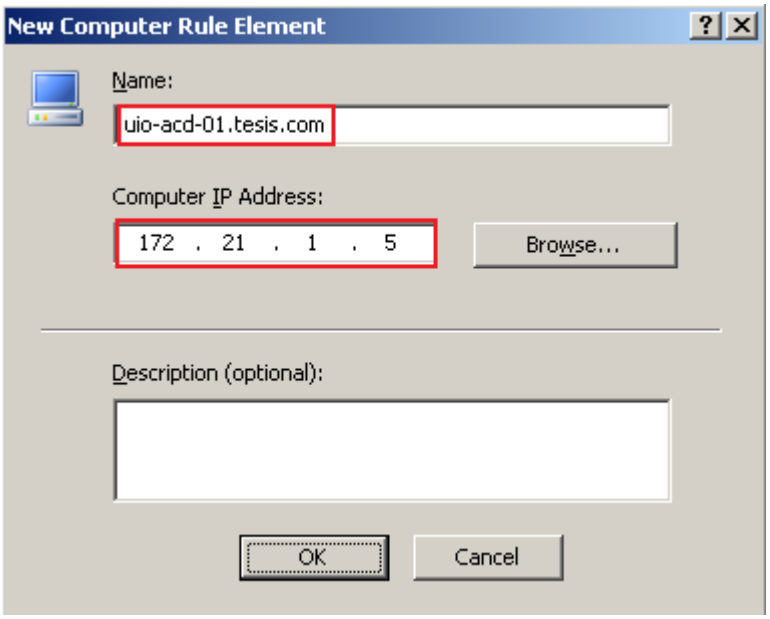
- Aplicamos una regla en el ISA server para verificar si funciona.
    - Abrimos la consola de administración del ISA server. Creamos una regla para permitir el tráfico de DNS, creamos una regla de acceso nueva. Le asignamos el nombre para identificarla.
    - Permitimos la regla



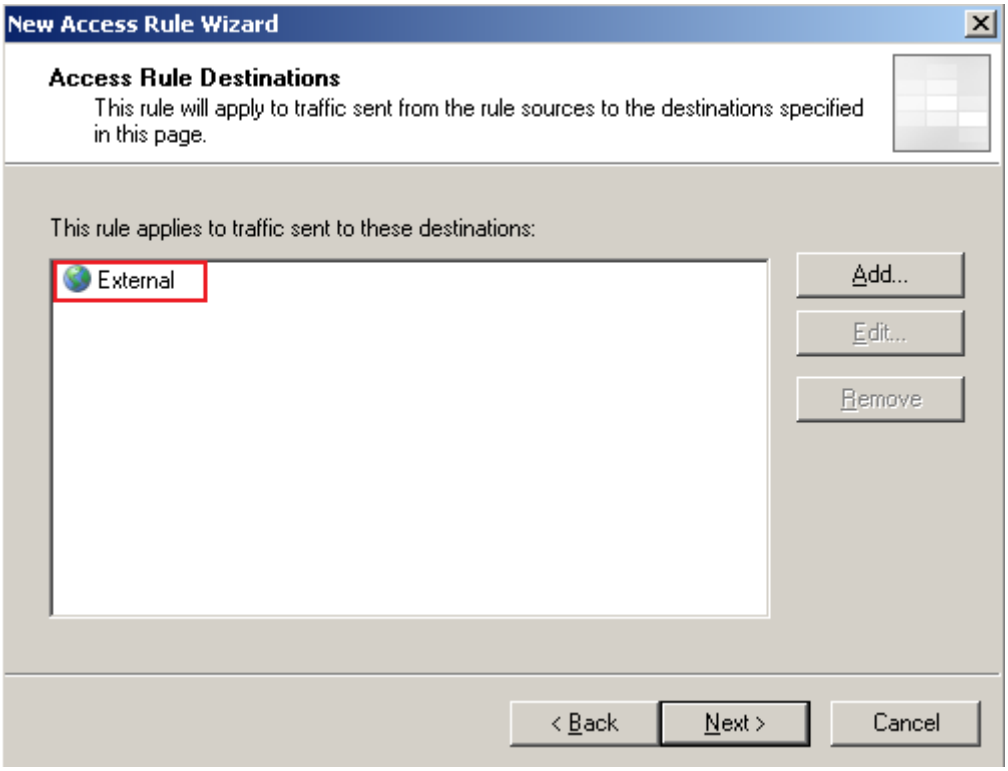
- Seleccionamos el protocolo que deseamos publicar, en este caso el de DNS.



- Configuramos el servidor en donde se encuentra el DNS para la regla

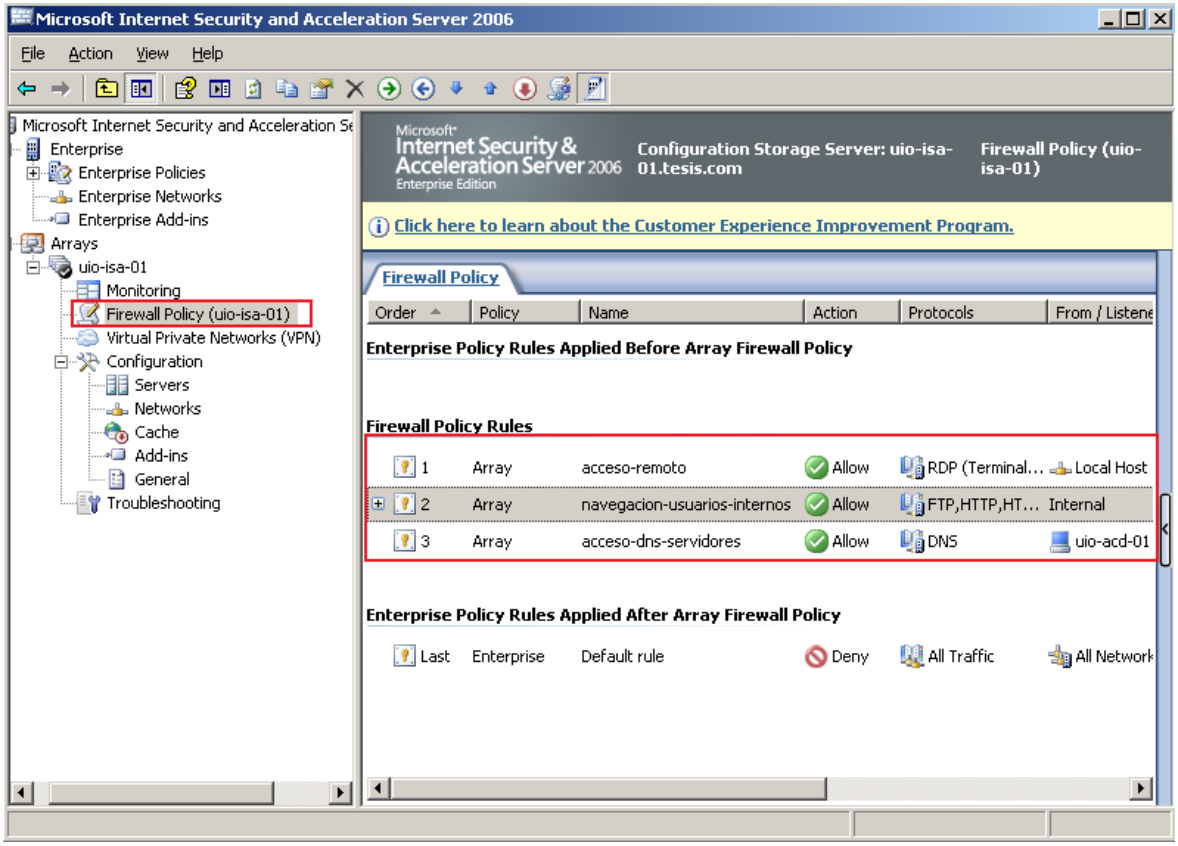


- El destino de las reglas va a ser para toda la red externa a la que se le proveerá el DNS



- Vamos a aplicar esta regla para todos los usuarios de la red. Y finalizamos.

- El mismo procedimiento se sigue si quieres crear otra regla con las necesidades que se presenten. En la siguiente figura se muestra el panel de administración de ISA y se puede ver las reglas que están aplicándose.



ANEXO 2

Proceso de implementación y pruebas del Directorio Activo

1. Configuración de TCP/IP para la maquina.

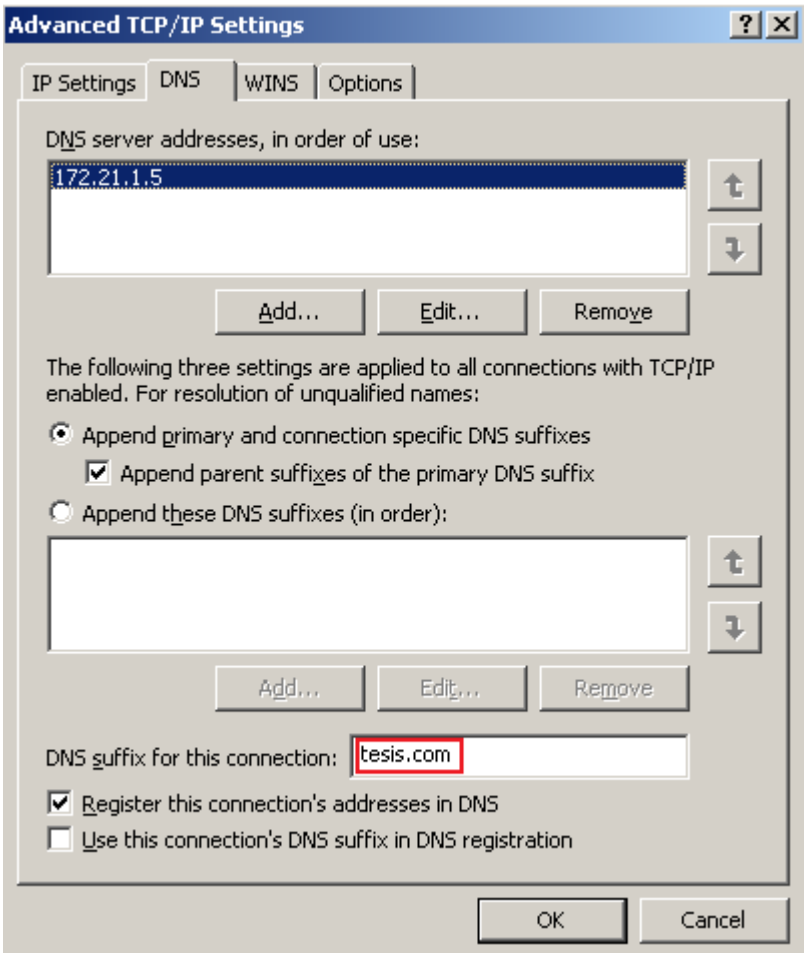
   Dirección IP: 172.21.1.5

   Mascara de subred: 255.255.255.0

   Gateway: 172.21.1.1

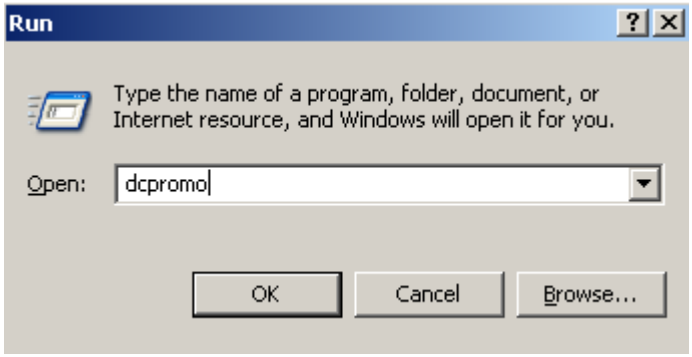
   DNS server: 172.21.1.5

2. Configuración de sufijo de DNS, en nuestro caso vamos a utilizar tesis.com como esta señalado a continuación, seleccionar la opción inferior “Register this connection’s addresses in DNS” que nos sirve para registrar el dominio al servidor de DNS.



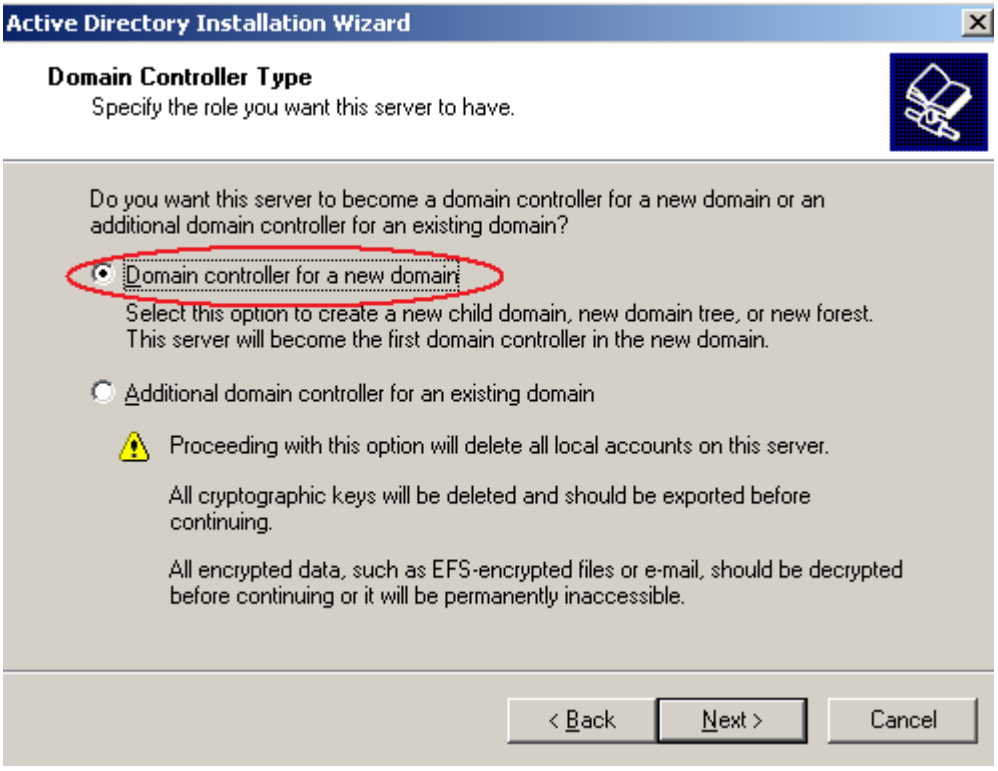
Configuración del Directorio Activo

1. Corremos el dcpromo para activar la herramienta de configuración del Directorio Activo

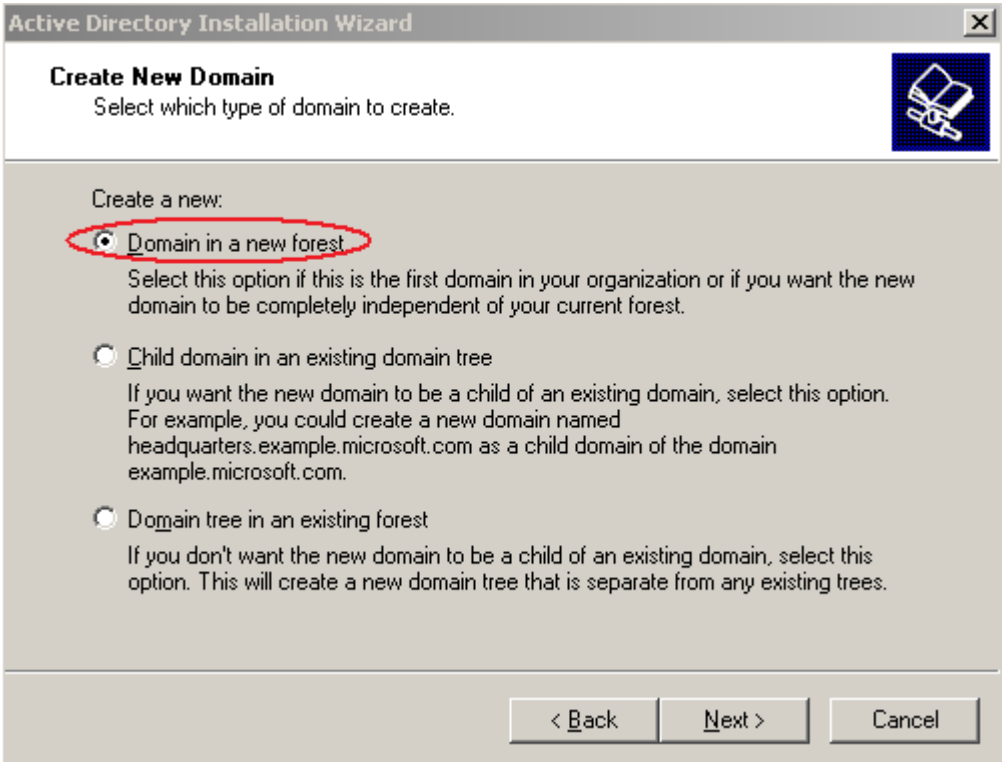


2. En las opciones nos va a salir la compatibilidad de nuestro sistema operativo, como estamos trabajando bajo Windows server 2003 no vamos a tener ningún problema.

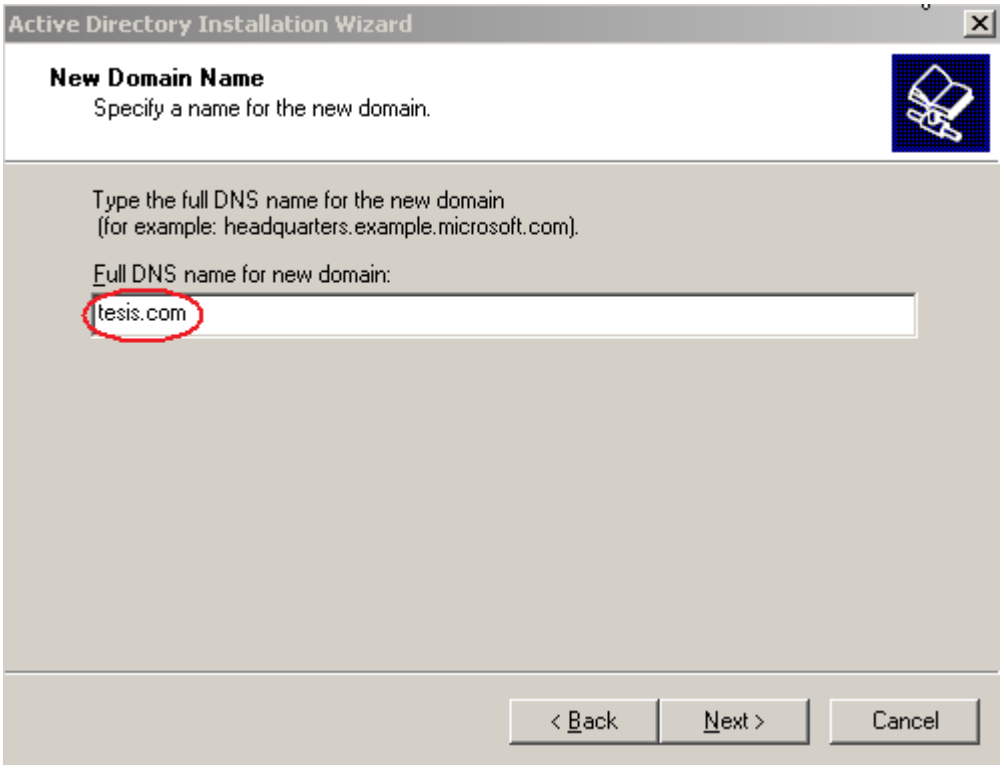
3. Creamos un controlador de dominio para un nuevo dominio.



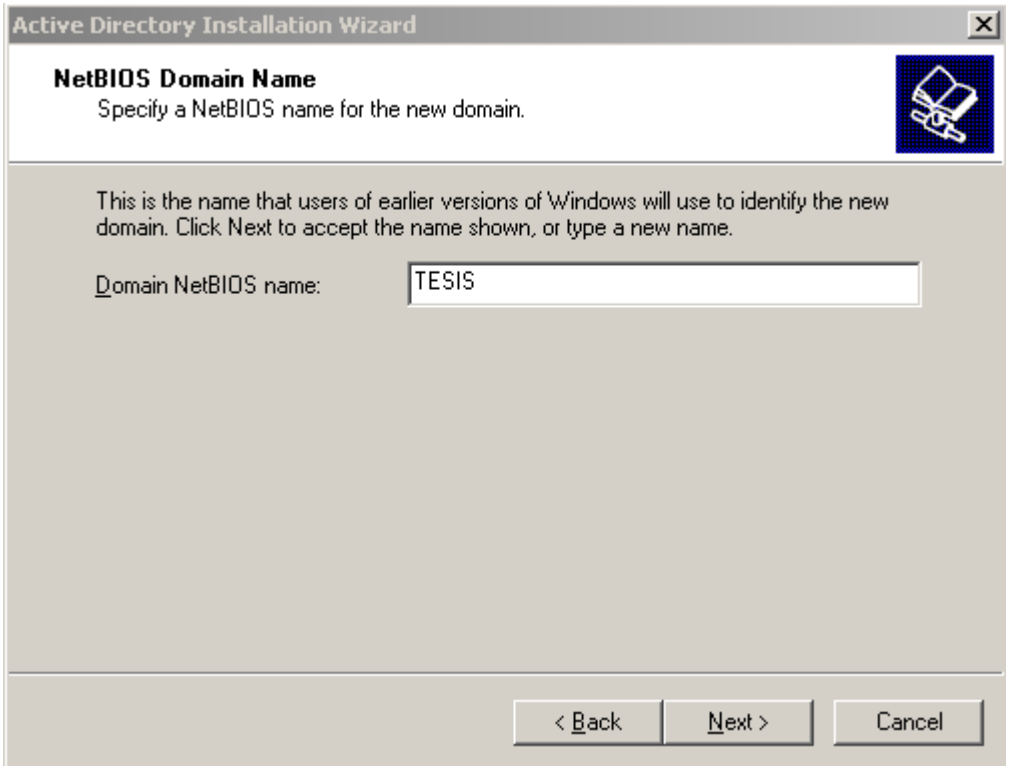
4. Como no existe nada aun vamos a seleccionar siguiente, creamos un nuevo forest.



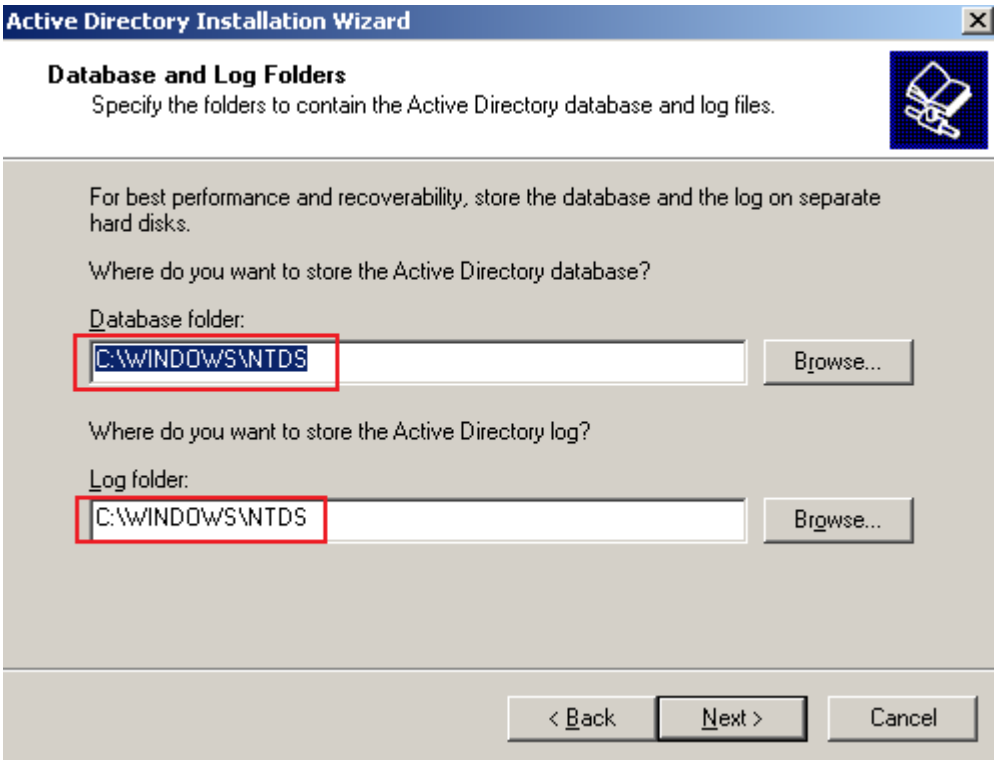
5. Asignamos el nombre del dominio, tesis.com



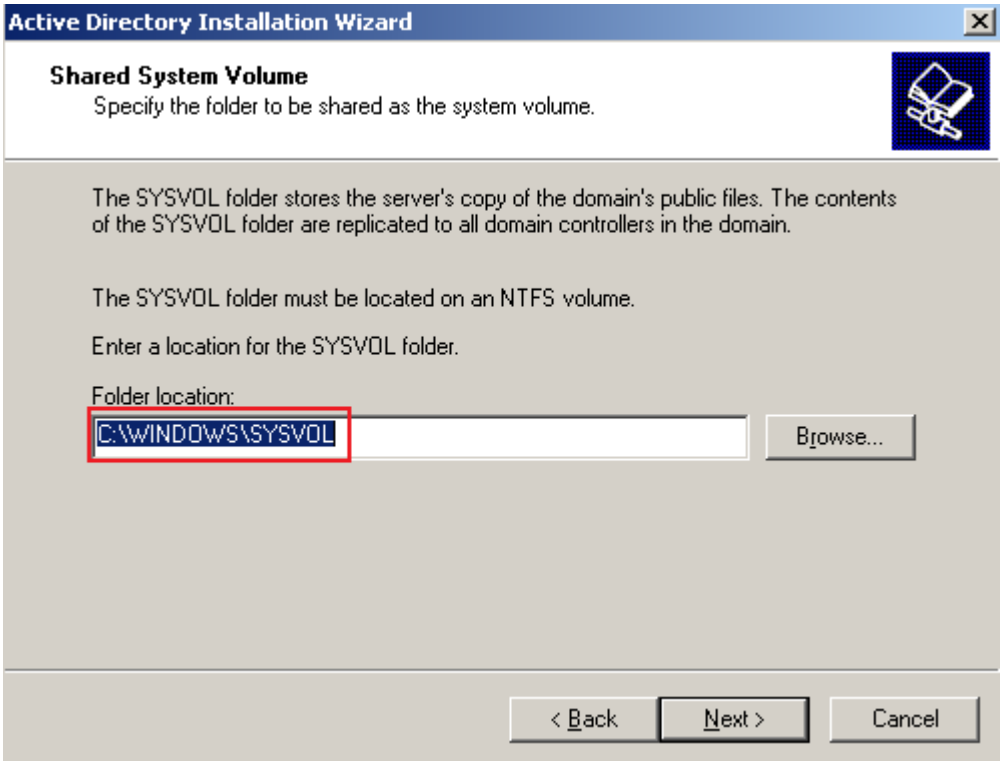
6. Asignamos el nombre al BIOS y lo dejamos el que viene por defecto que es el nombre sin .com



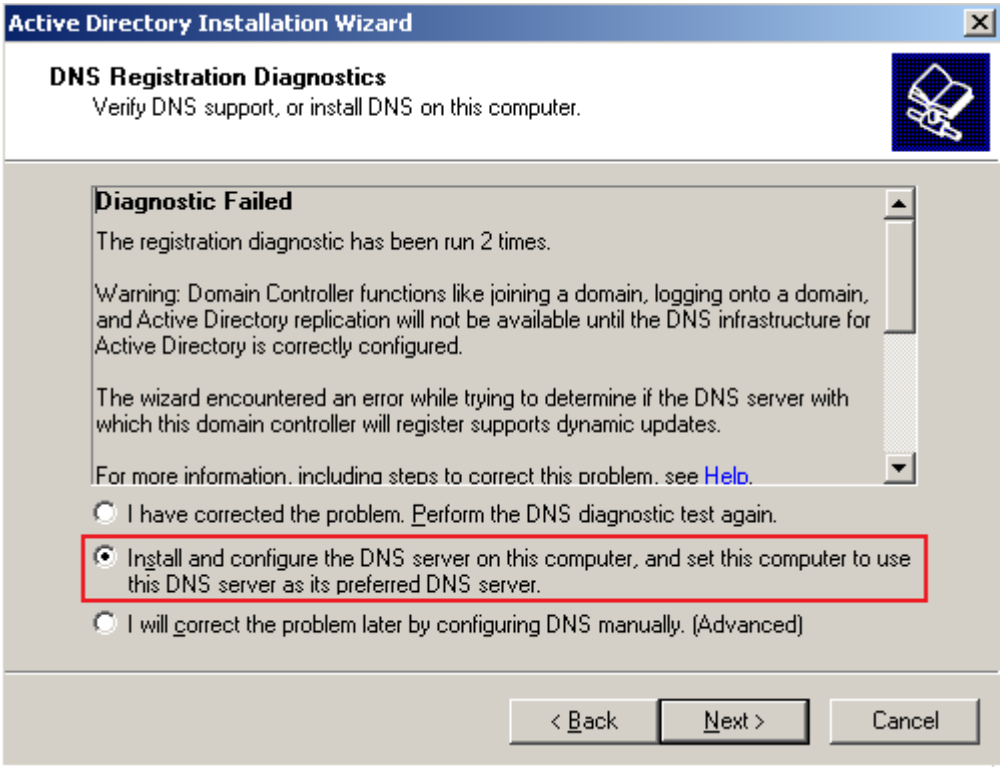
7. Seleccionamos los lugares en donde se van a almacenar los archivos de la base de datos y los logs, entonces si el controlador de dominio es pequeño podemos dejar las opciones que vienen por defecto, sino debemos asignar lugares de almacenamiento con más capacidad. En nuestro caso dejamos los que vienen por defecto.



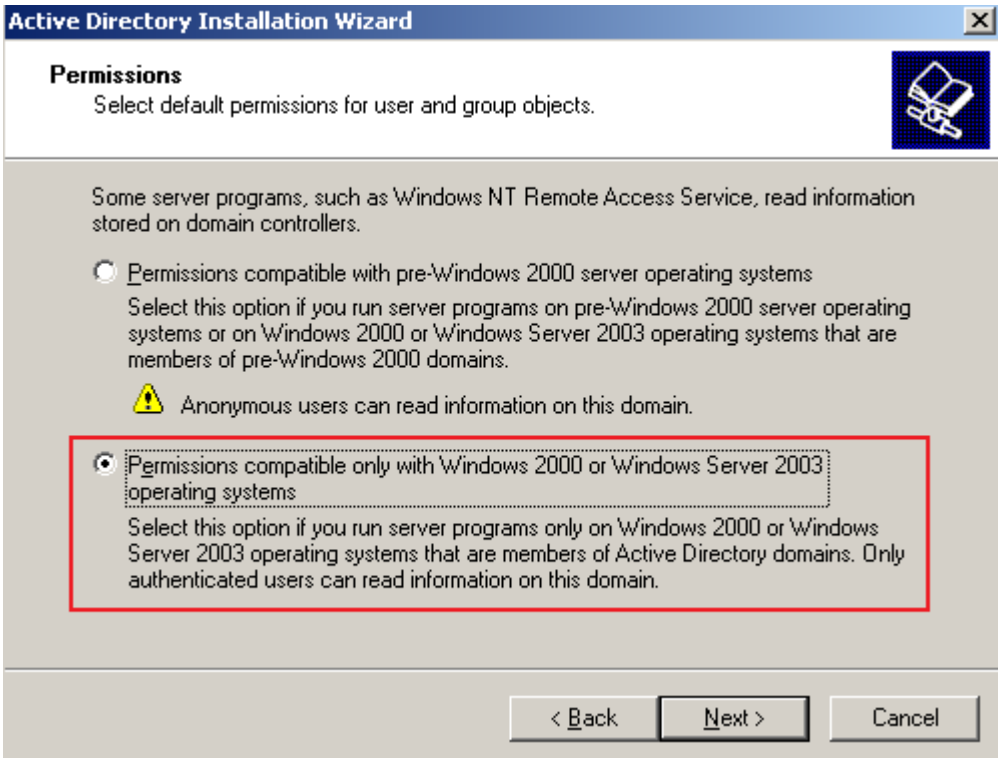
8. Creamos una carpeta que comparte en donde va a almacenar todas las carpetas del dominio y esa carpeta es la que va a replicar con los demás controladores



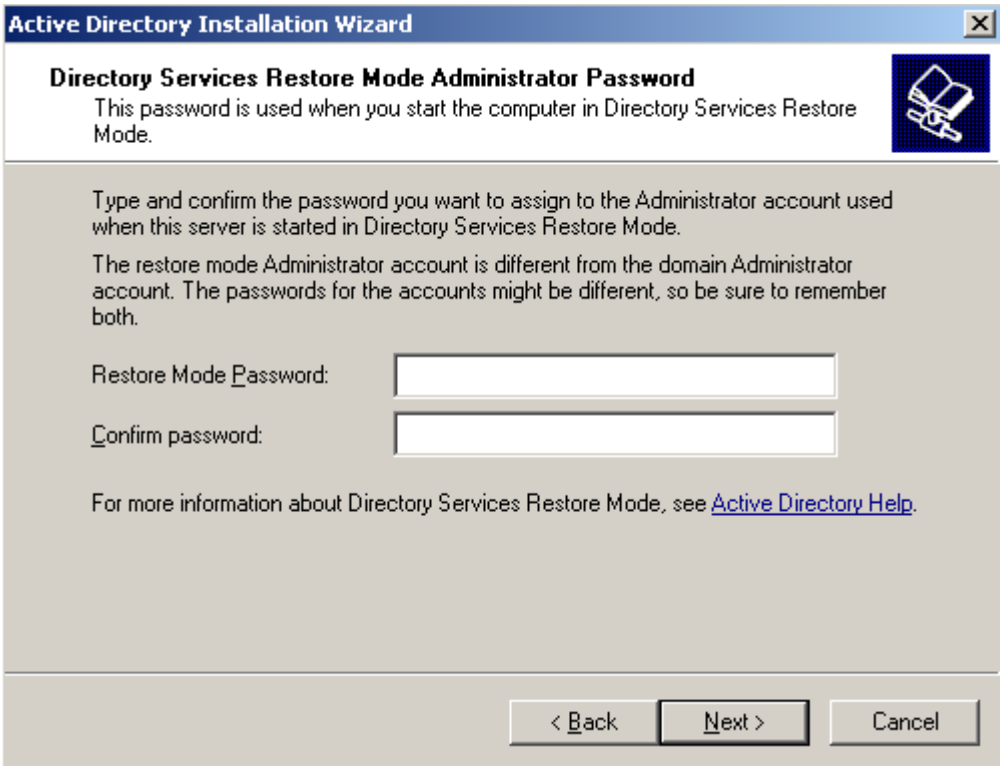
9. En la siguiente opción hace un chequeo de la existencia de un DNS, como no hemos instalado ninguna va a fallar, pero en las opciones inferiores nos da la opción para configurarlo e instalarlo en la misma computadora.



10. Seleccionamos los permisos que sean compatibles con Windows Server 2003 ya que el resto de nuestros ordenadores por montar están implementados bajo Windows Server 2003



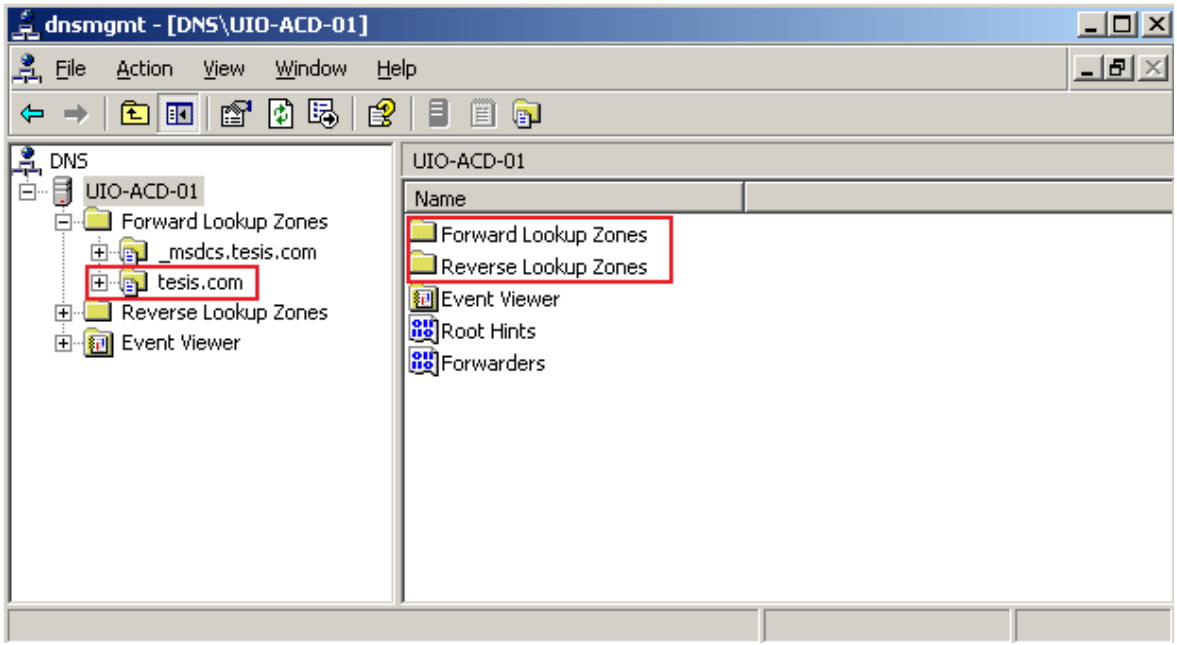
11. Ingresamos la clave para el directorio Activo, nos sirve para restaurar en el caso de que tuviéramos algún problema.



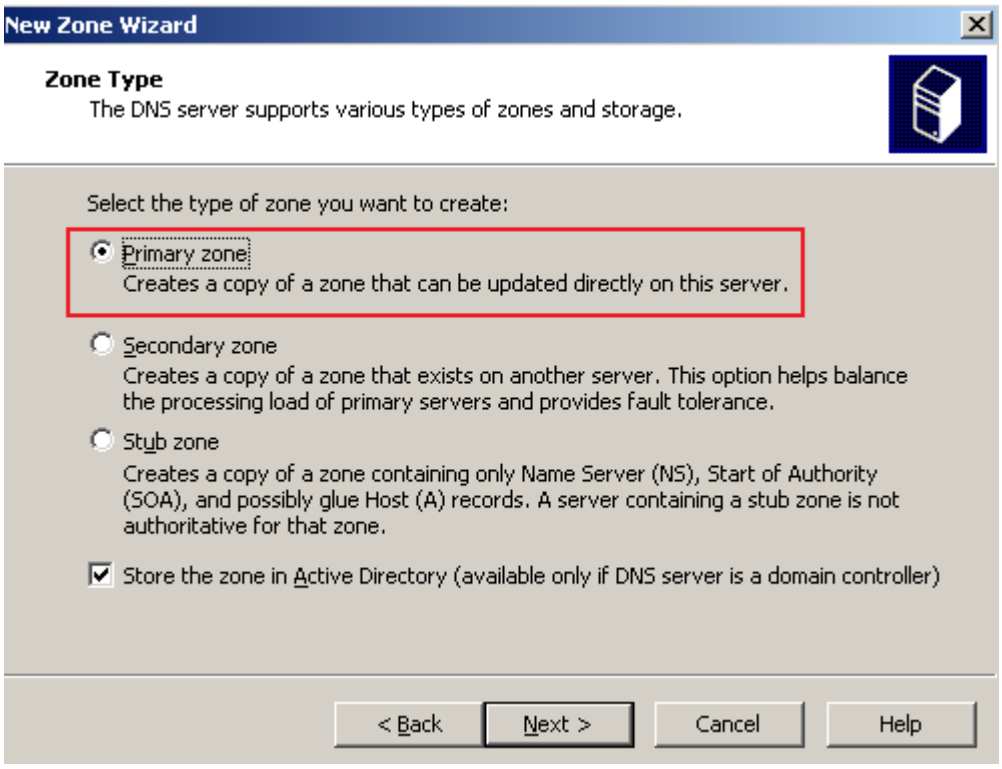
12. Después nos presenta un resumen con los cambios que se va a realizar y ponemos siguiente para que se realice la instalación, cuando finalice la instalación reiniciamos la maquina.

Configuración del DNS

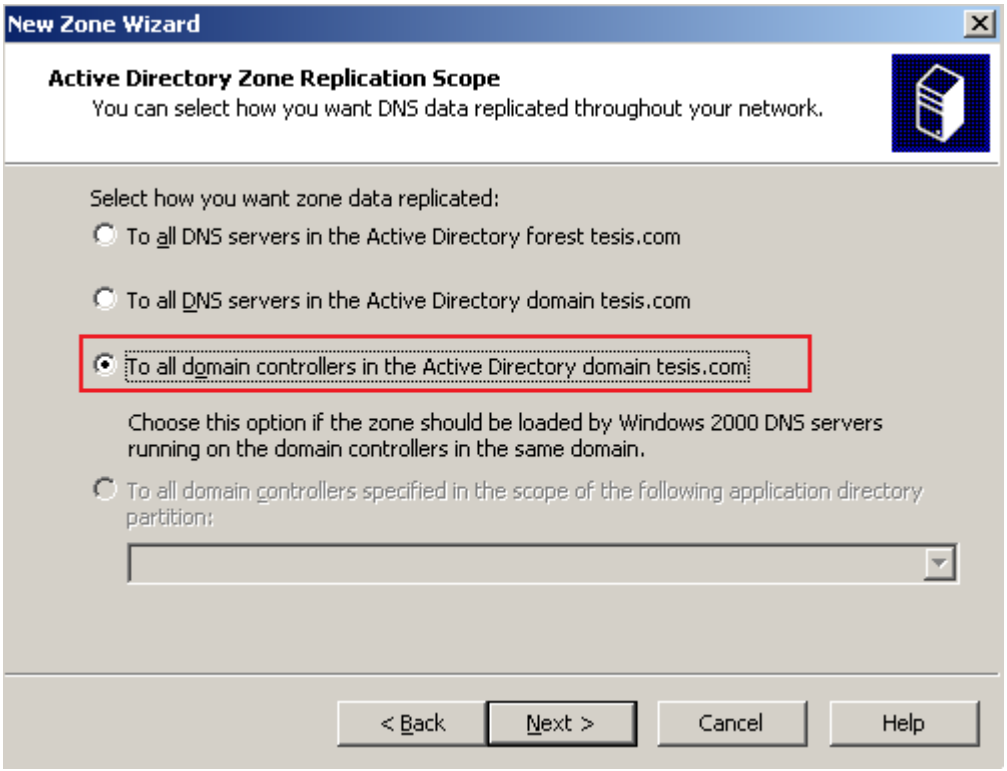
1. Servicio de DNS es importante dentro del directorio activo ya que se utiliza para resolver los servicios locales. Se crearon las zonas directas y las zonas reversas.



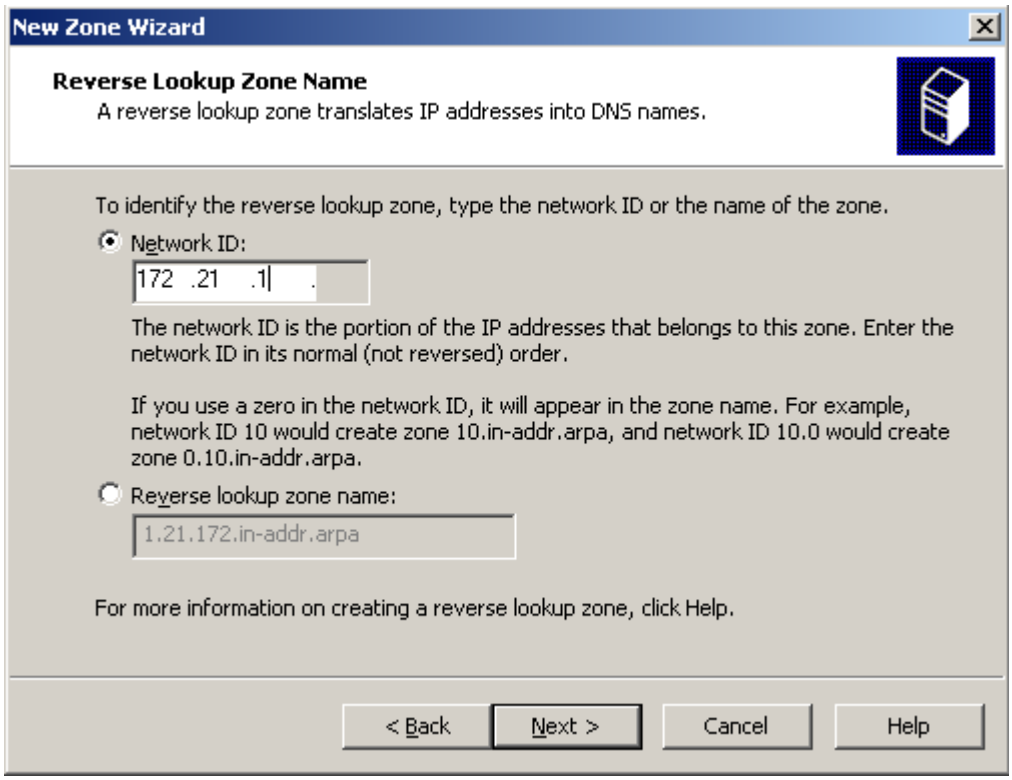
2. Para la creación de las zonas reversas, seleccionamos con el click derecho sobre el reverse lookup zone, aparece el wizard para la creación, seleccionamos zona primaria y hacemos que almacene en el directorio activo



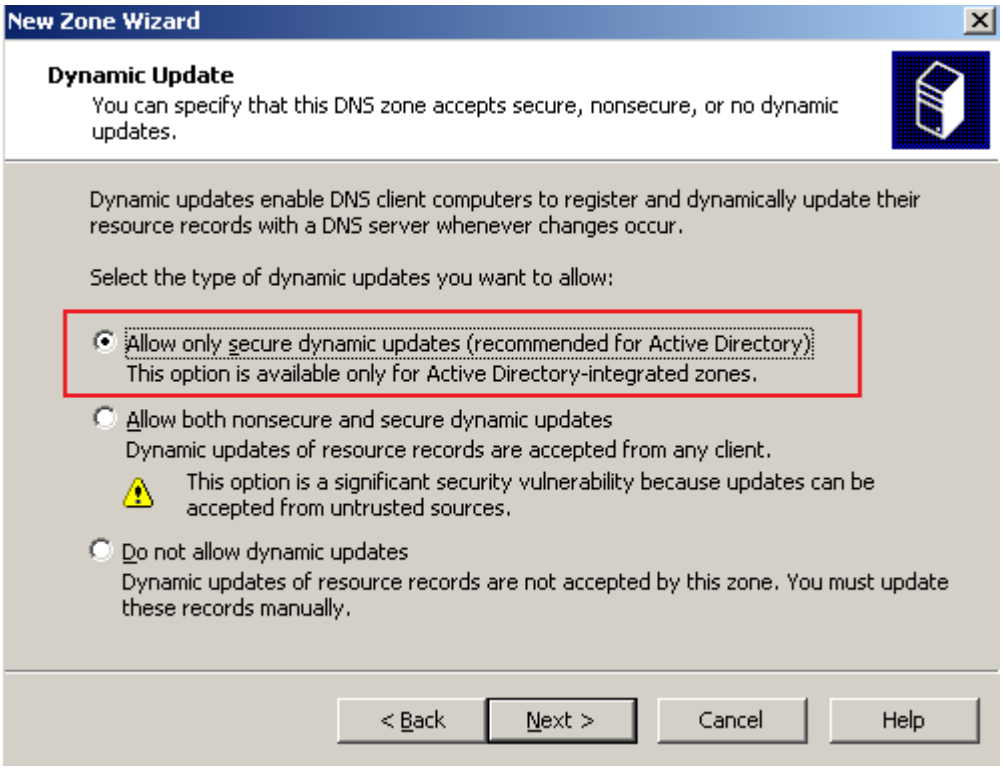
3. Seleccionamos para que se apliquen a todos los controladores de dominio



4. Ingresamos la IP de la que se va a crear la zona reversa, en nuestro caso ponemos 172.21.1. Existe la posibilidad de dejar el último digito libre esto se puede hacer cuando se tiene varias subredes y no se quiere crear una zona reversa para cada red.

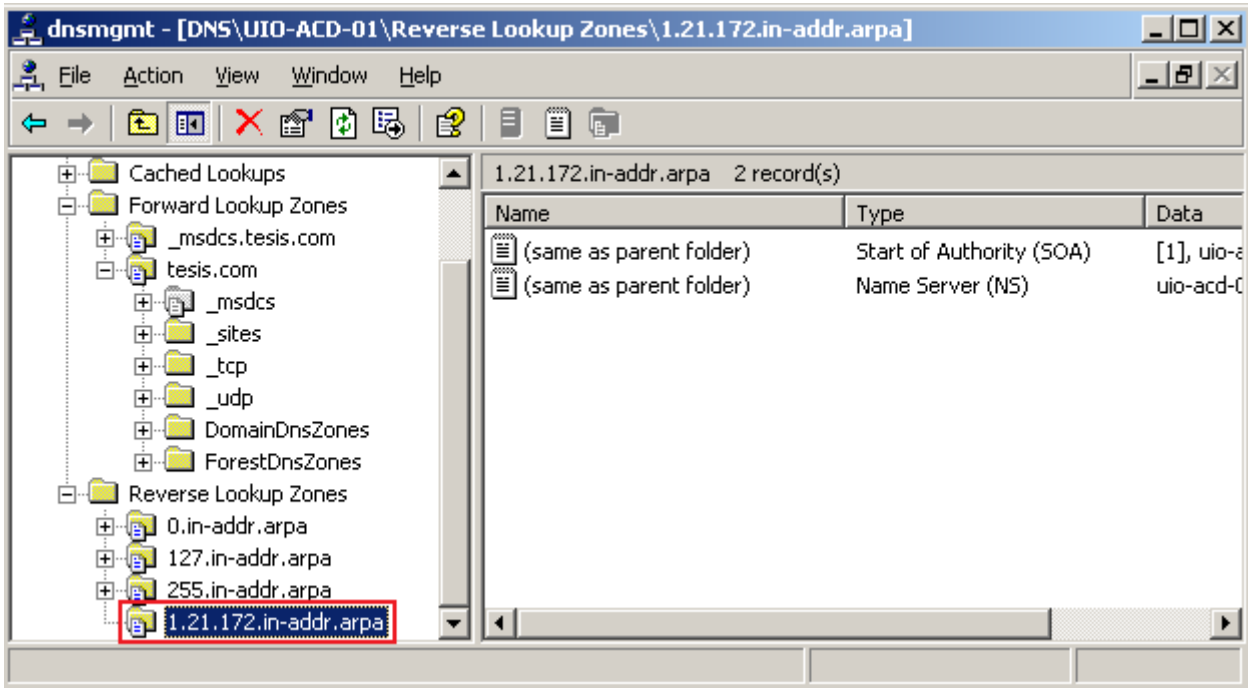


5. Escogemos la primera opción para realizar las actualizaciones dinámicas, esto quiere decir los ordenadores que estén dentro del dominio realicen sus actualizaciones correspondientes.



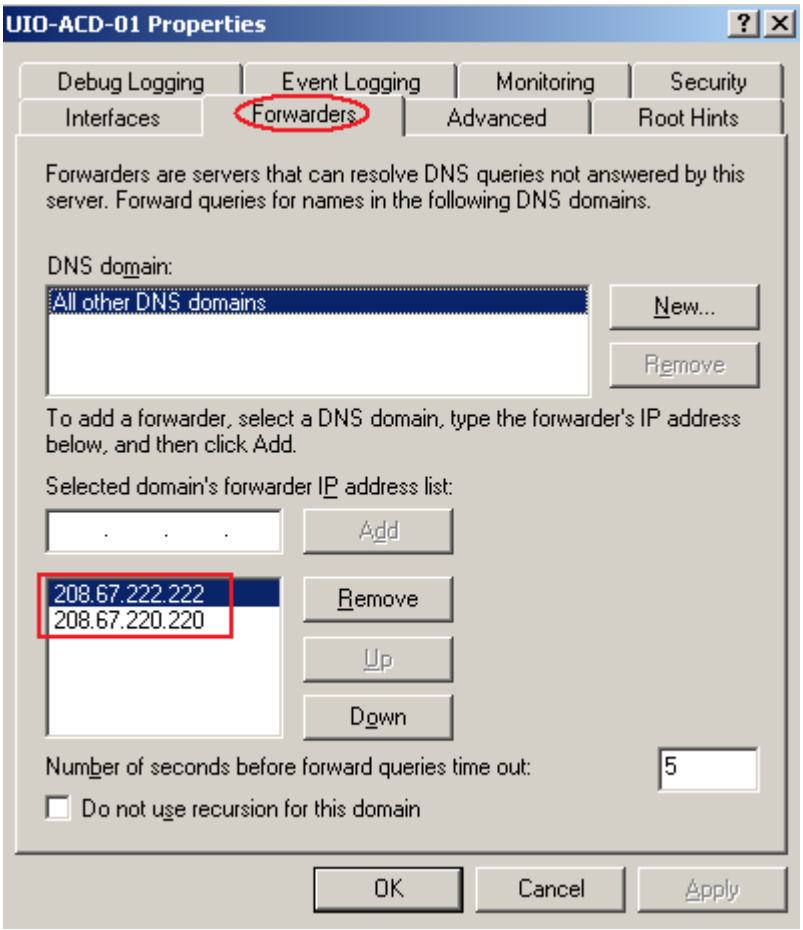
6. Después damos siguiente y completamos la creación de la zona reversa.

7. Se verifica que ya ha sido creada la zona reversa

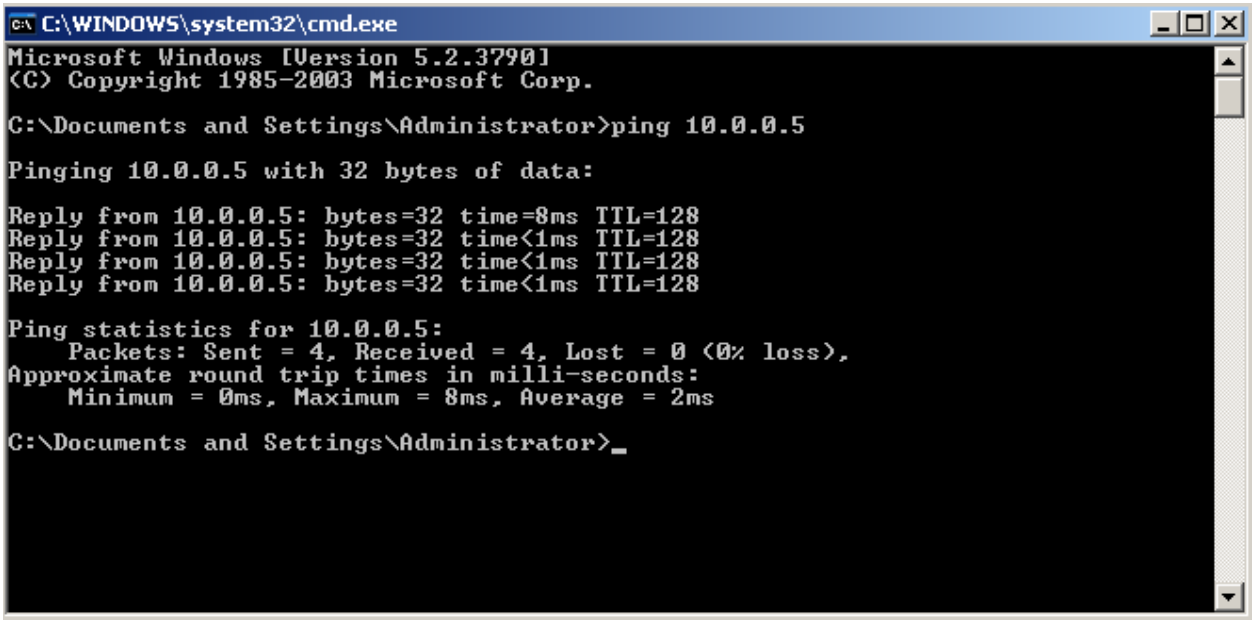


8. Para la resolución de los nombres de dominio de internet, se puede utilizar reenviadores llamados *opendns*, estos servidores respondes a las solicitudes de nombres de dominio que yo no tengo creadas.

9. Para esto utilizamos propiedades, seleccionamos forwarders. Las IP que responden para los dominios de internet son 208.67.222.222 y 208.67.222.220



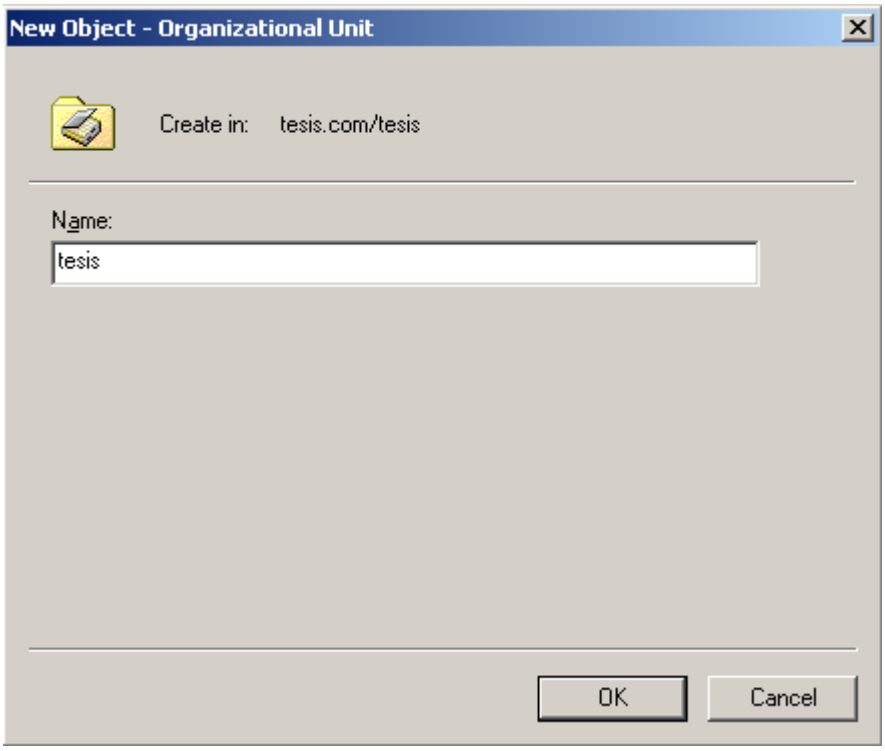
10. Para comprobar esto vamos a resolver un nombre como google.com



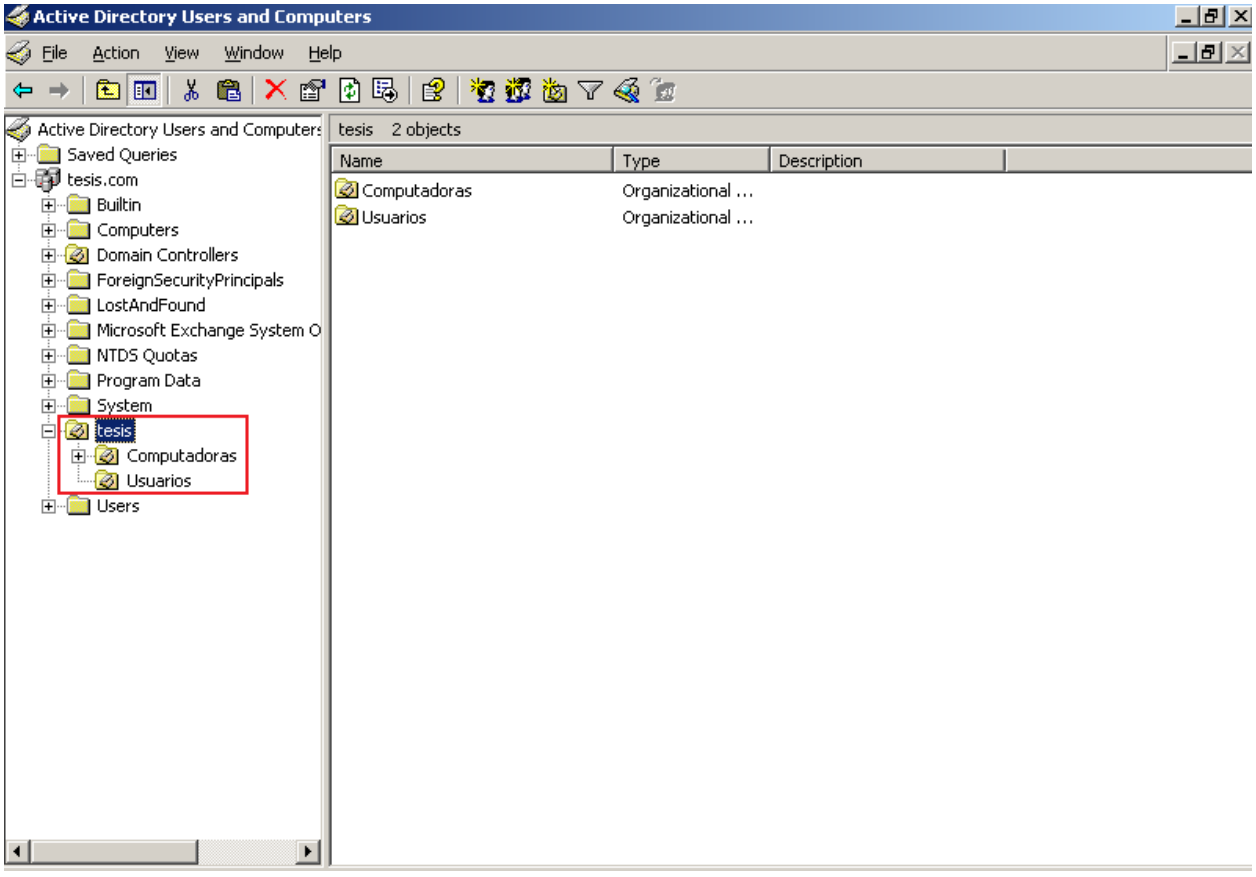
11. Estas consultas quedan en el cache del servidor, si seleccionamos las opciones avanzadas podemos ver las consultas que hemos realizado, esto nos sirve para que las respuestas sean más rápidas. Y si existe algún error con una página se puede borrar el cache

12. Vamos a crear una estructura de directorio activo básica, para esto vamos a “Active Directory Users and Computers” para ingresar una computadora y un usuario al dominio.

13. Creamos una nueva Unidad Organizacional que se llame tesis



14. Dentro de esta unidad vamos a crear dos Unidades Organizacionales mas, una que sea de usuarios y otra de computadoras.

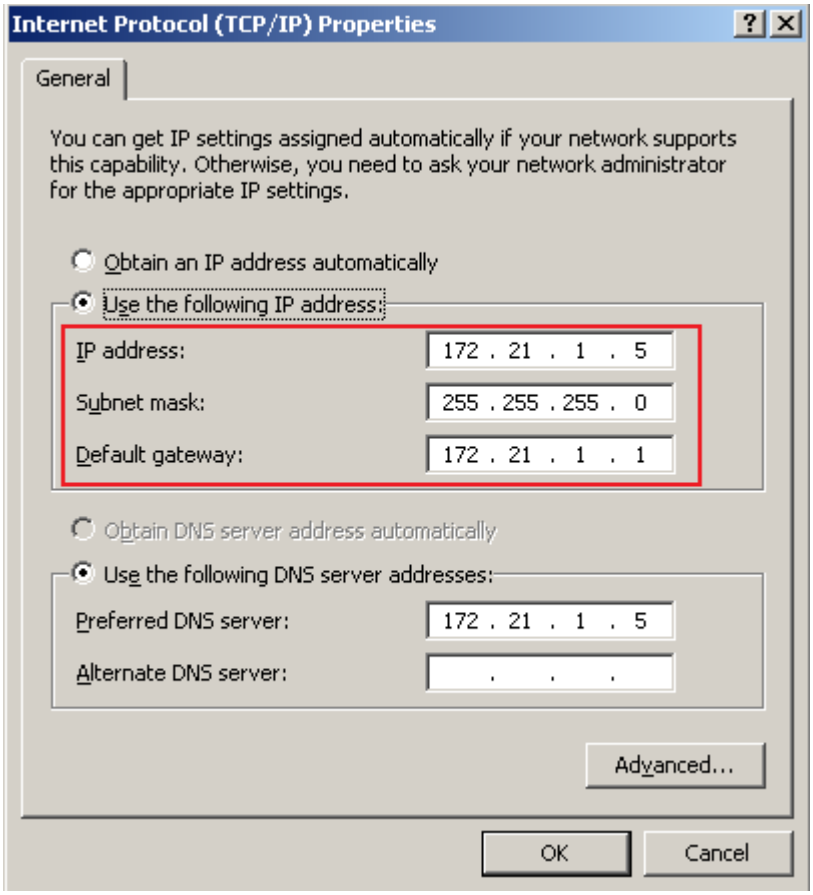


15. Dentro de usuarios podemos crear usuarios, haciendo click derecho, nuevo, usuario. Y completamos los campos vacios necesarios para la creación del usuario. Estos usuarios pueden ser utilizados para realizar la autenticación en diferentes maquinas que se encuentren en el dominio.

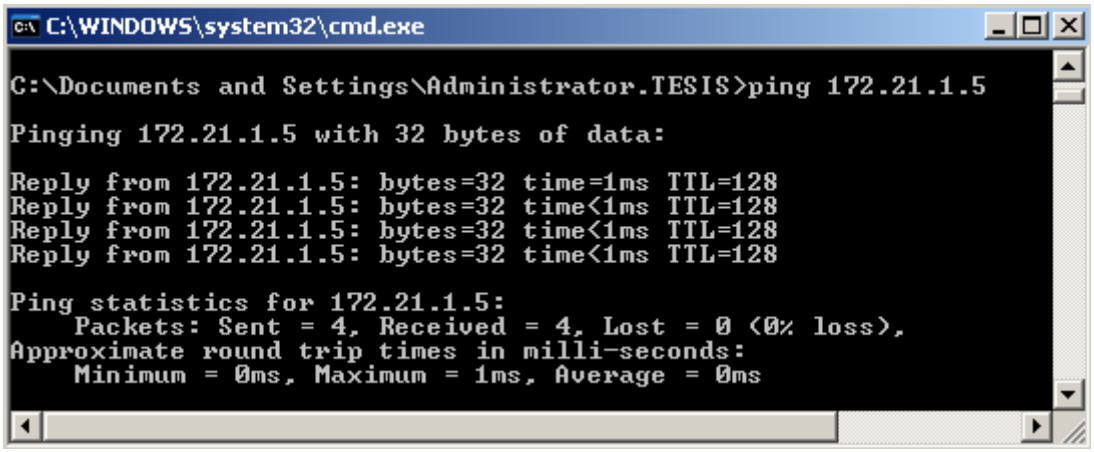
Pruebas

- Configuración de tarjeta de red.

Ir a las propiedades de la tarjeta y comprobar la configuración.

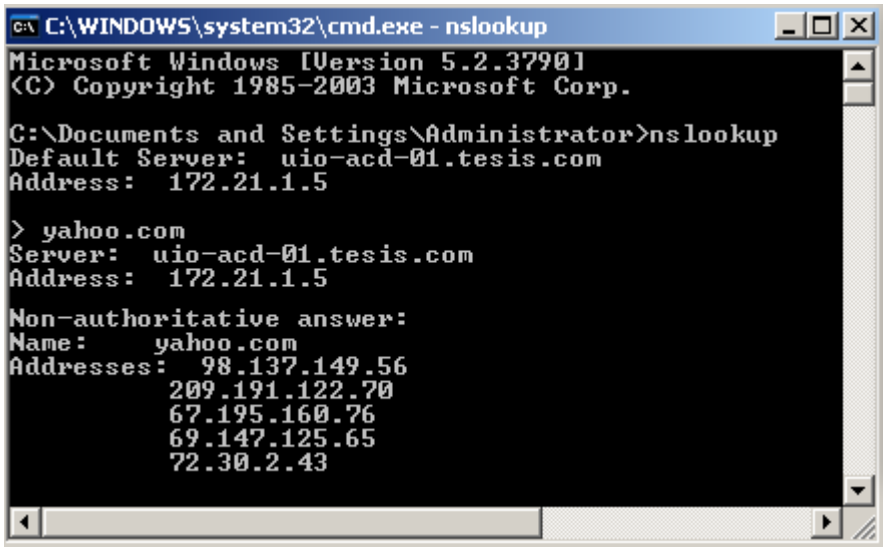


- Probar la configuración de red haciendo ping desde el ISA server a esta máquina para verificar la conectividad.

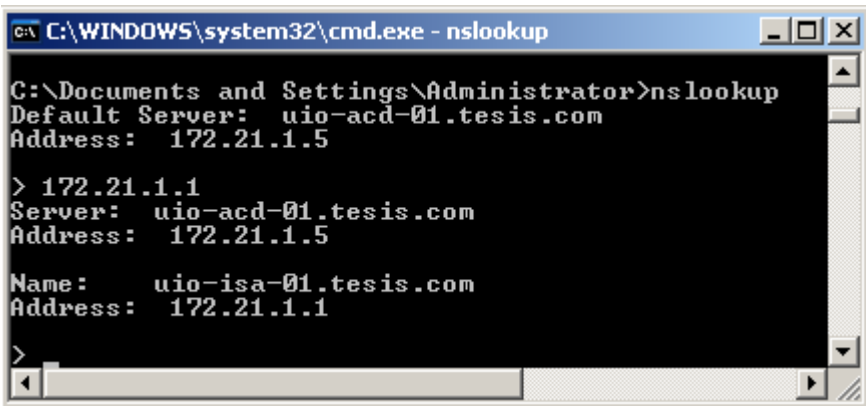


- Probar el funcionamiento del DNS con nslookup y resolución de nombres internos como externos a la red.

  Externo



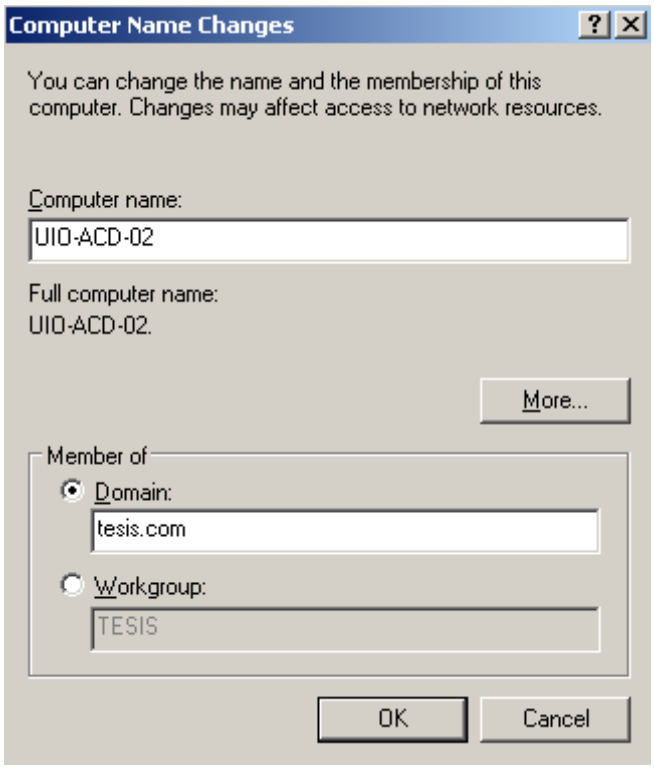
  Interno



- Autenticación al directorio activo y el dominio con el usuario creado.

  Para que la maquina sea parte del dominio, vamos a My Computer, hacemos click derecho en properties y en la pestaña de Computer Name

  Vemos el nombre de la maquina y hacemos click en Domain, colocamos el nombre de nuestro dominio.

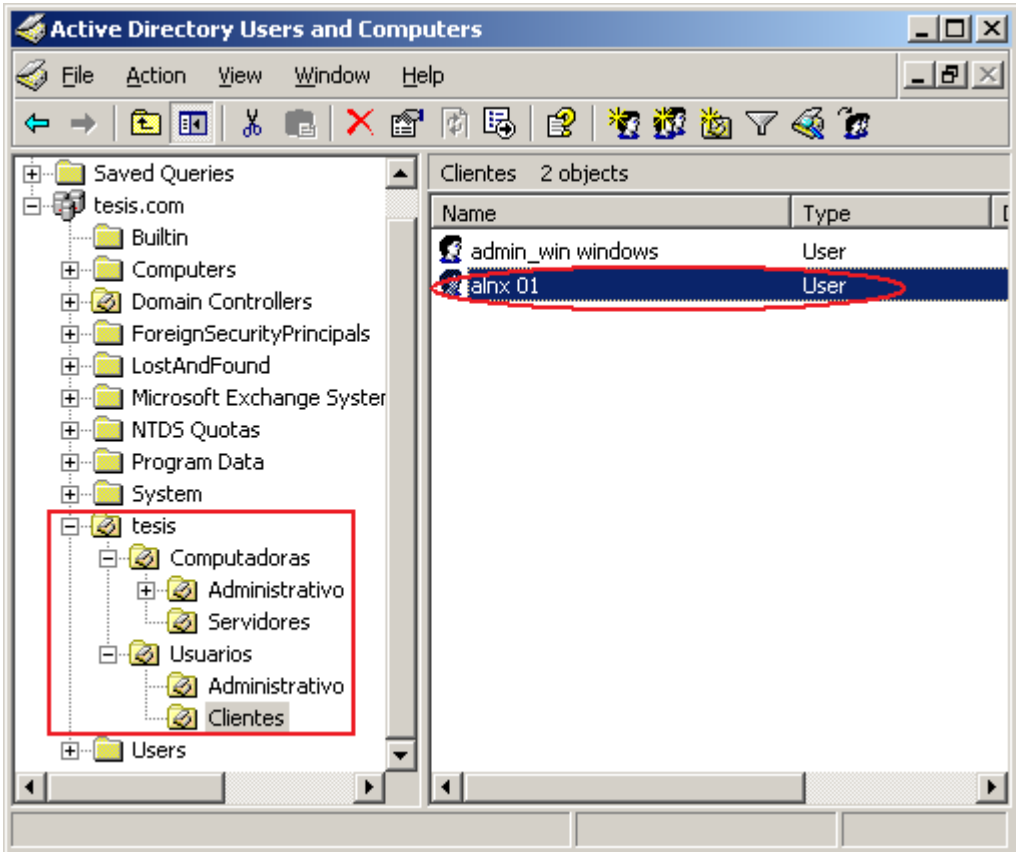


- Sale una pantalla de autenticación para poner el usuario y la contraseña, de esta forma se autentica al directorio y listo.

- Verificación de políticas a los usuarios según las creadas en el directorio.

  En el directorio creamos una Unidad Organizativa (OU) de usuarios en donde nos permite dar permisos a cada uno de los clientes de acuerdo a los consentimientos que se les desee dar, para probar esto es necesario autenticarse desde un usuario y realizar tareas que no le correspondan por ejemplo, modificar o borrar archivos en el momento que se les niegue estas acciones, se pueden comprobar los permisos

que se crearon. En la figura siguiente se puede ver la estructura de nuestro directorio.



ANEXO 3

Proceso de implementación y pruebas de Exchange Server 2003

Lo que se recomienda es que se instale Exchange en un ordenador que no sea controlador de dominio, lo ideal es que existan dos controladores de dominio para que se puedan tener respaldos en caso de perder uno de ellos. Sin embargo no se recomienda tener todo en un solo ordenador ya que si perdemos el ordenador perderíamos todo.

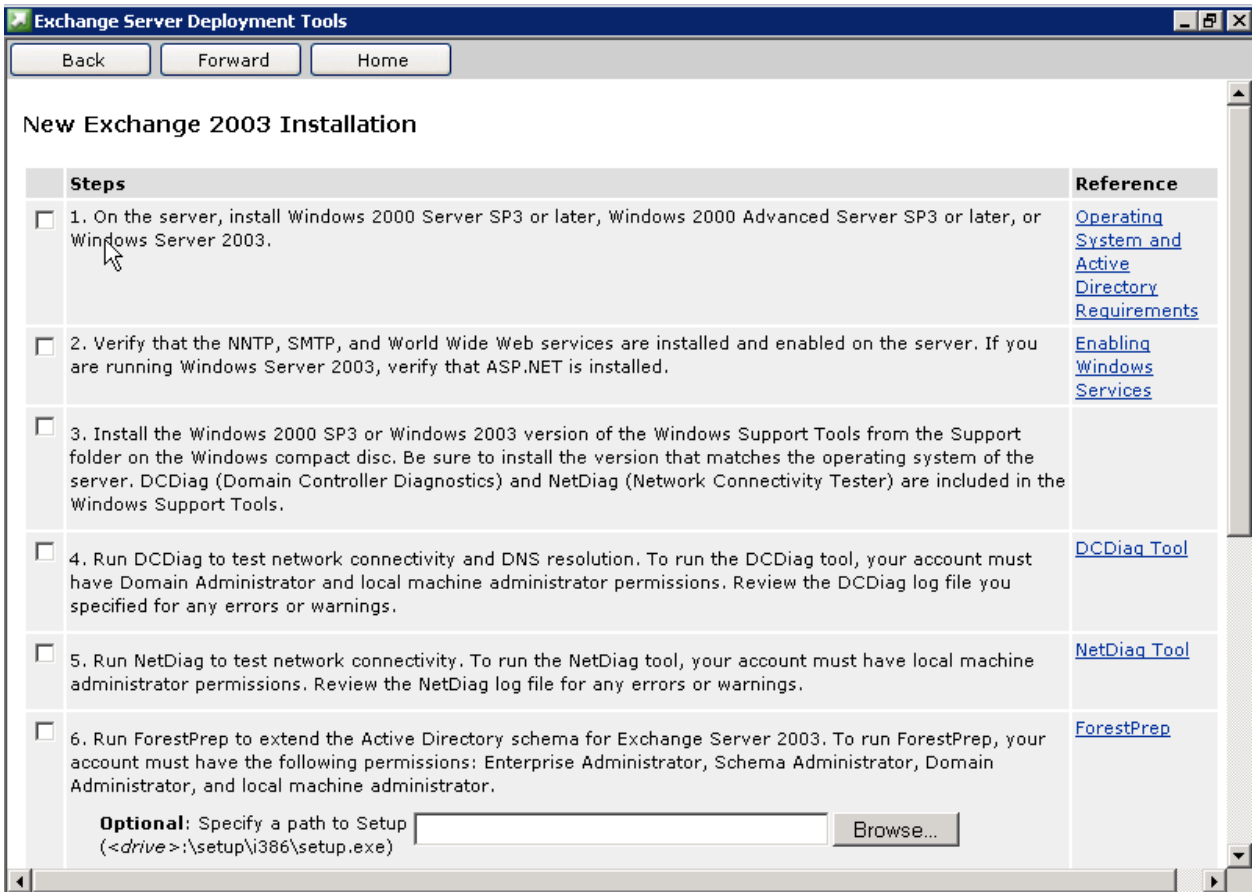
1. Vamos a revisar la configuración de red TCP/IP de la maquina.

   Dirección IP: 172.21.1.10

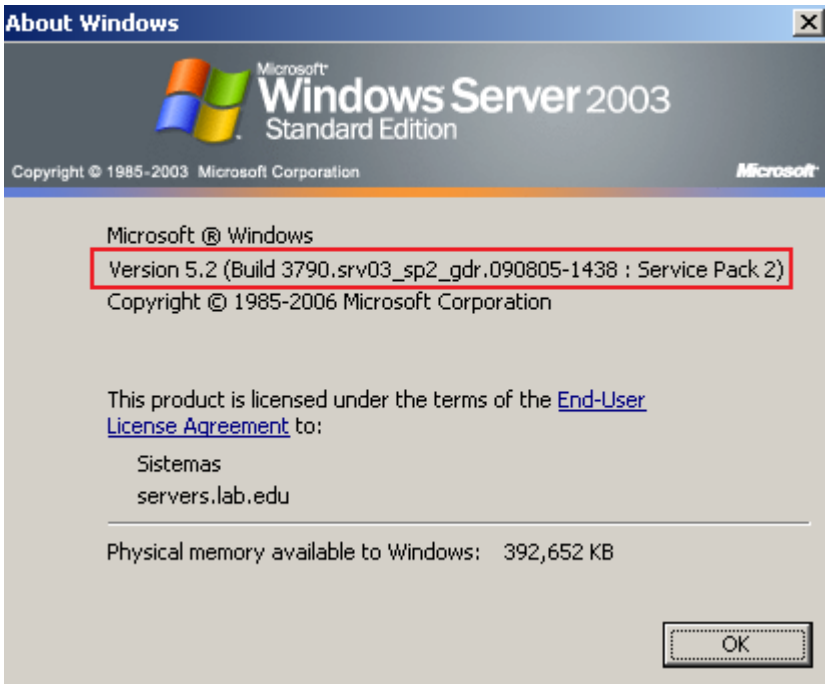
   Mascara de subred: 255.255.255.0

   Gateway: 172.21.1.1

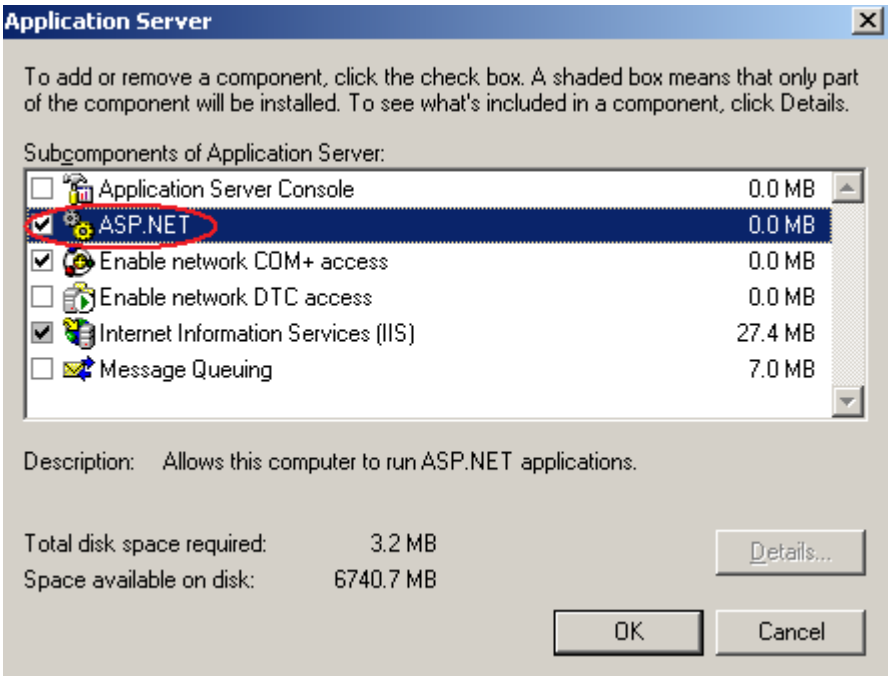
   DNS server: 172.21.1.5
2. El ordenador debe estar autenticado con el Directorio Activo.
3. Para la configuración de Exchange necesitamos tener el CD de Exchange Server 2003. Hacemos click en el setup.exe y nos despliega el asistente, escogemos la opción de herramientas para Exchange server 2003 con sp2, y este nos llevara paso a paso en la instalación.
4. Escogemos la instalación por primera vez.
5. Nos pregunta si vamos a tener coexistencia con otros servidores o si es una instalación nueva, entonces escogemos la instalación nueva.
6. La pantalla a continuación nos ira mostrando paso a paso los requerimientos que necesitamos para la instalación.



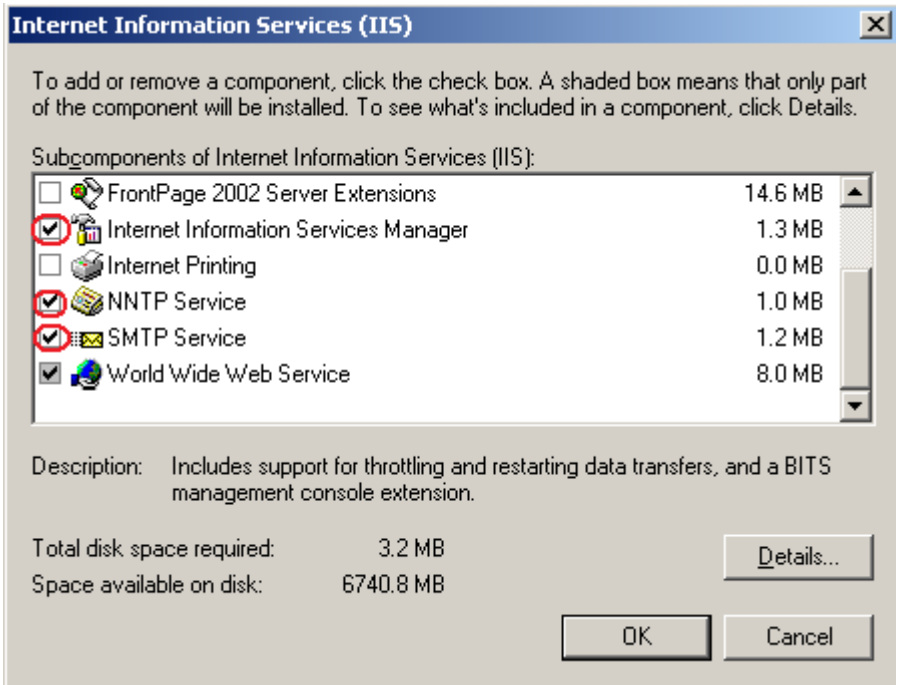
7. En el primer paso nos pregunta si la versión en donde estamos instalando Exchange es la adecuada, entonces verificamos la versión de nuestro ordenador para ver si es compatible.



8. En el segundo paso verificamos si SMTP, NNTP, www y ASP.NET están instalados. Para esto vamos a Panel de Control, click en agregar/quitar programas, click en agregar/quitar componentes de Windows. En aplicaciones de servidores, habilitamos la opción de ASP.NET



9. En los servicios de información de internet IIS habilitamos las opciones de www, NNTP, SMTP.



10. Ponemos aceptar y esperamos a que se instale estas nuevas herramientas, con esto completamos el paso número dos.
11. Para el paso número tres necesitamos instalar unas herramientas adicionales, que nos permitan correr el DCDiag y el NetDiag. Esto verificamos en el cd de Windows server 2003 en la carpeta de support -> tools -> SUPTOOLS.MSI -> hacemos doble click he instalamos. Con esto cumplimos el paso numero tres.
12. En el paso número cuatro debemos correr la herramienta DCDiag para probar la red y las resoluciones del DNS. También verifica los permisos de administrador dentro de la maquina.

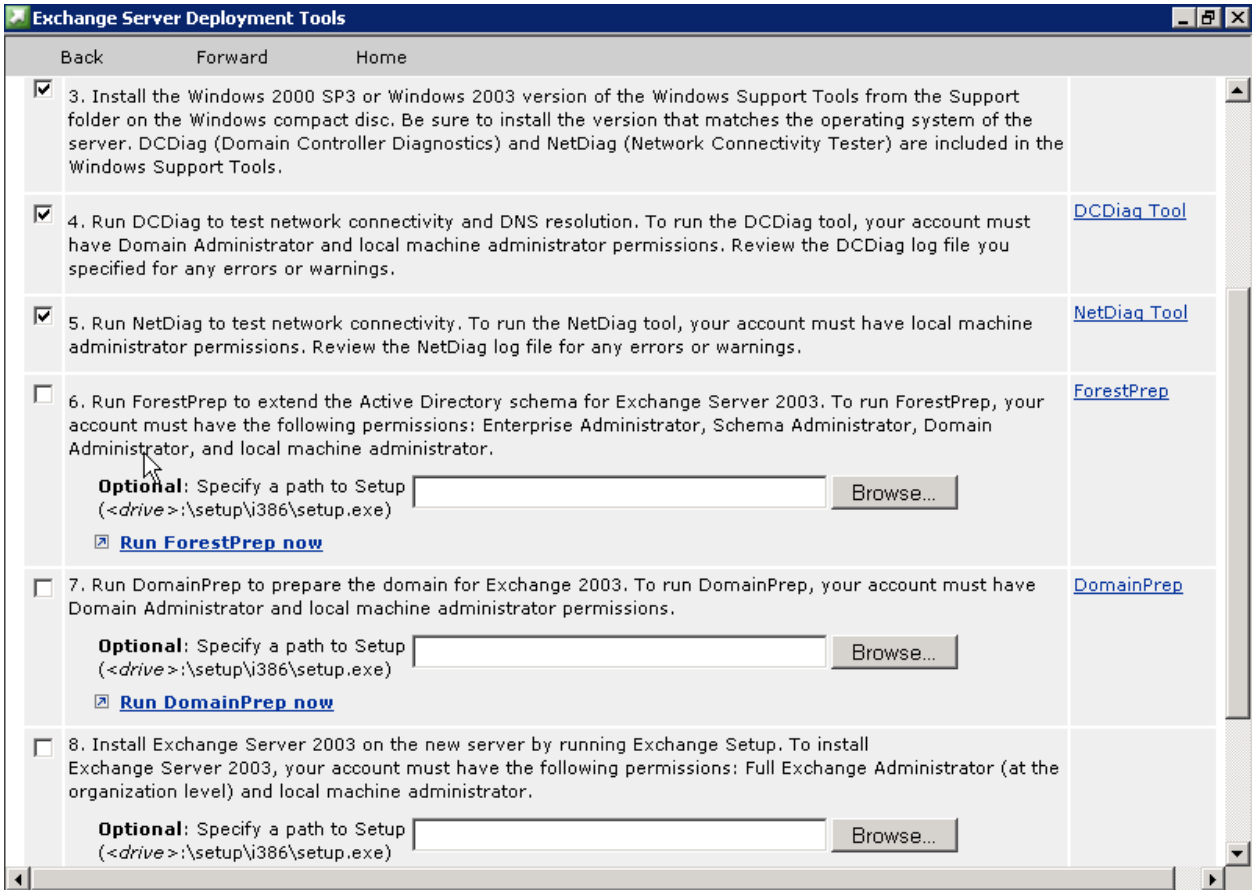
    Sintaxis: cd /Program Files\Support Tools

    s: acldiag.exe

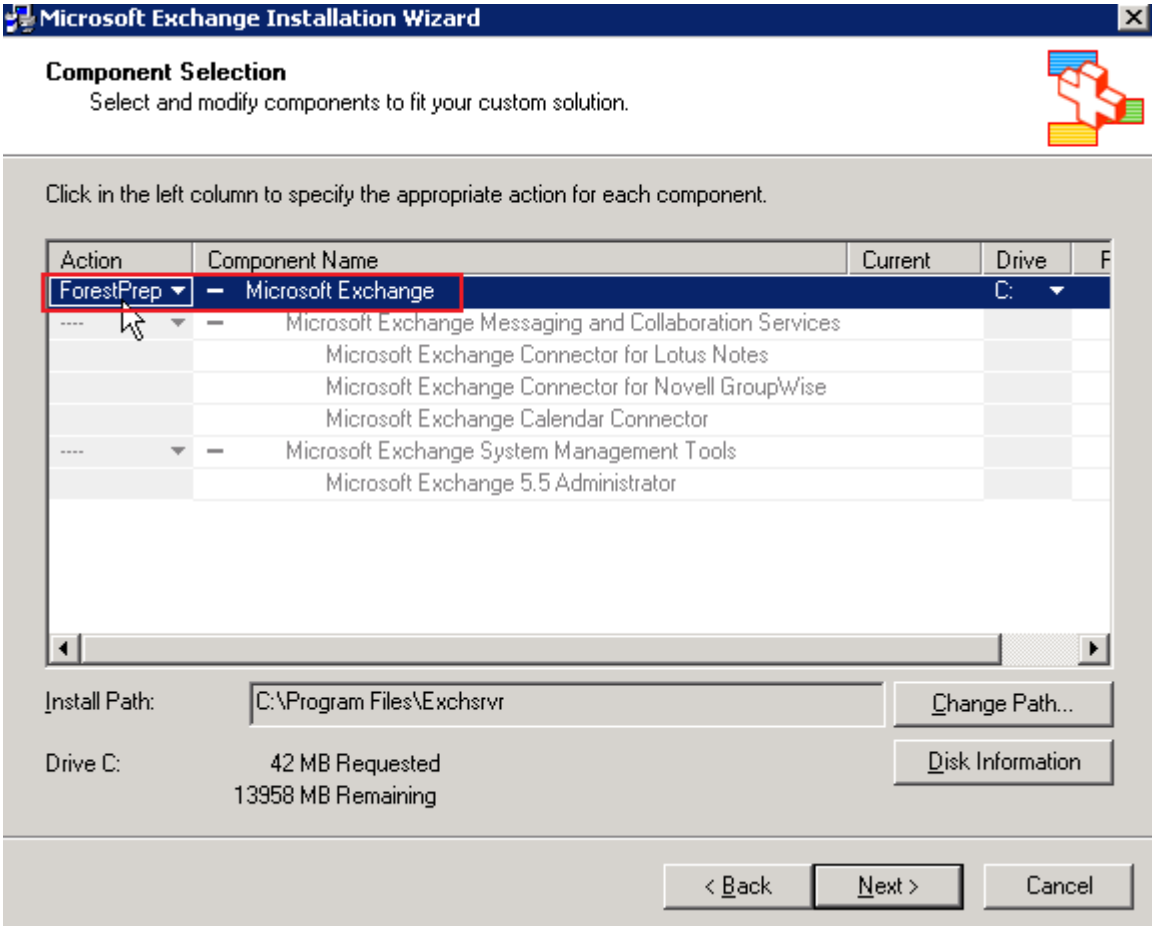
    Cuando termina de correr ha verificado la conexión de red y el resto de requerimientos.
13. En el quinto paso corremos el NETDiag

    Sintaxis: cd /Program Files\Support Tools

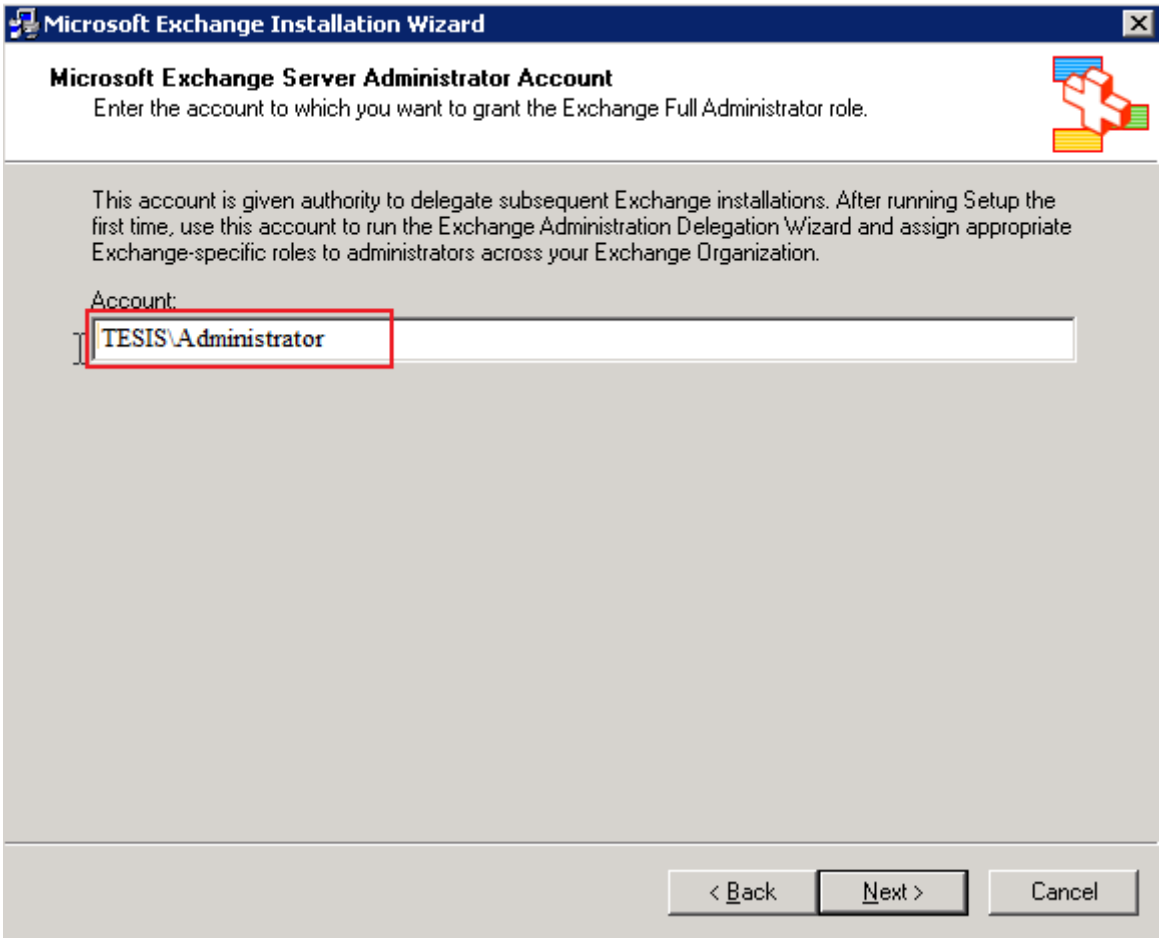
    s: netdiag.log
14. Después de hacer estos pasos de comprobación, podemos instalar el Exchange. Pero necesitamos preparar antes el forest del dominio.



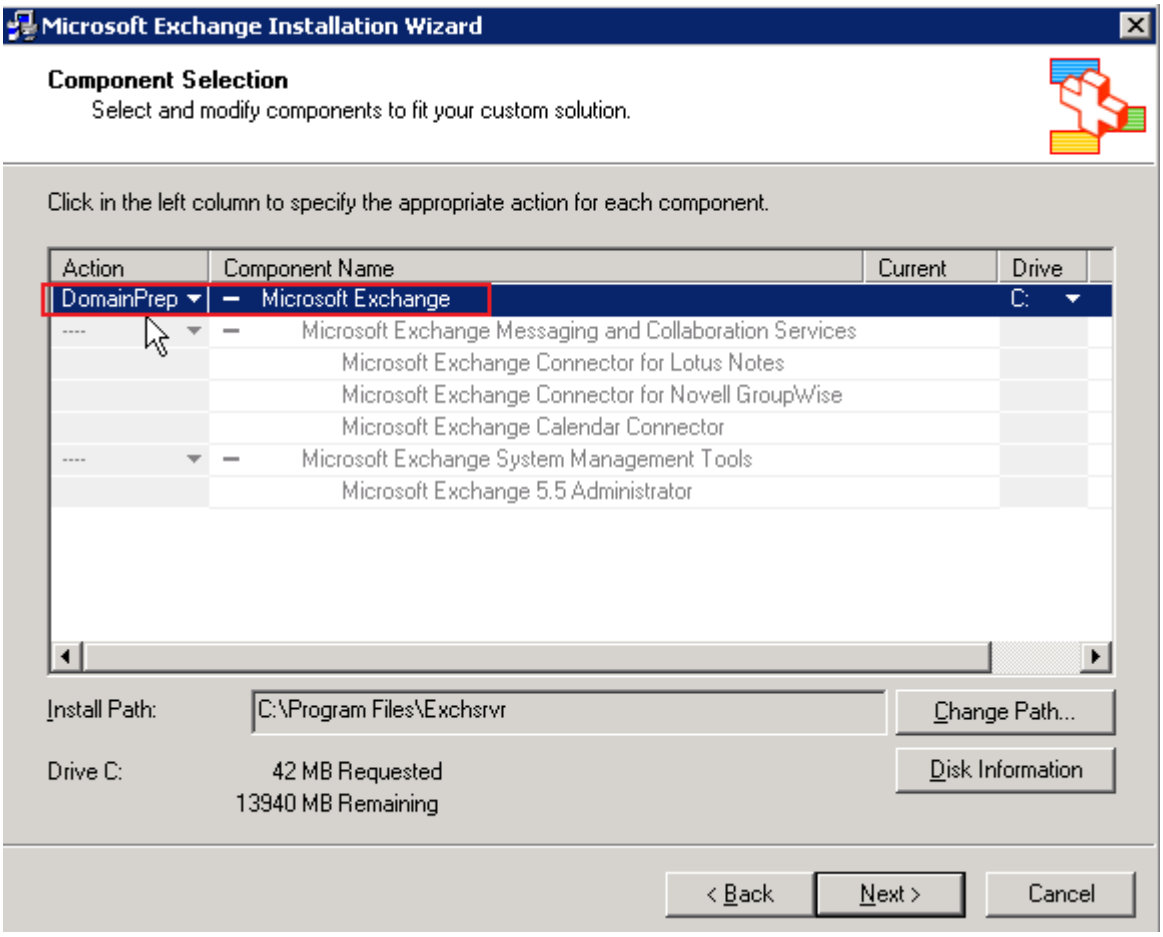
15. En el paso numero 6 nos da el acceso directo para poder correr el ForestPrep que se nos facilita para hacer la preparación.
16. Aceptamos la licencia y escogemos la opción de ForestPrep que nos permite hacer la preparación.



17. Cuando seleccionamos siguiente, verifica la cuenta con la que se va a manejar, en este caso la de administrador con todos los permisos del Dominio Tesis.com



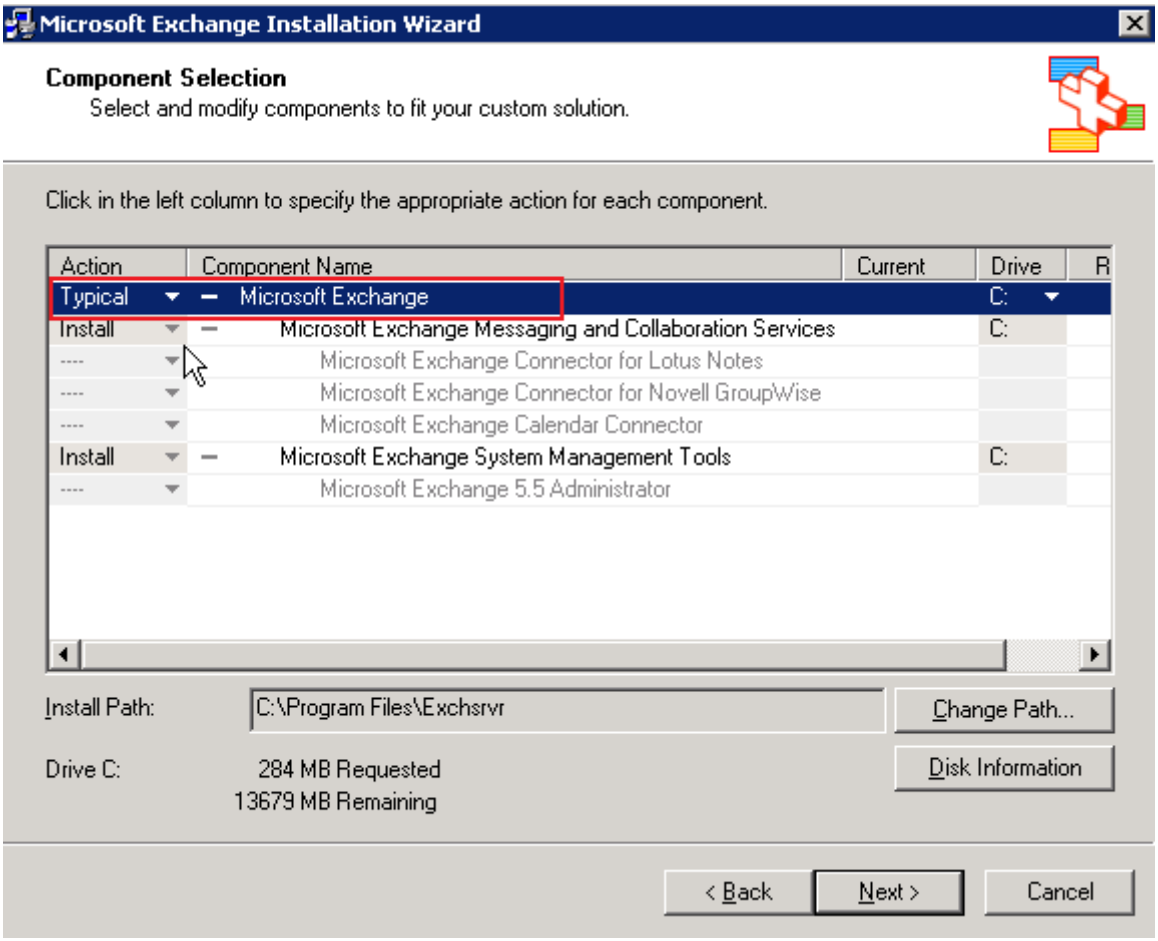
18. Cuando ponemos siguiente, se hace un proceso de chequeo en el Directorio Activo que y las verificación necesarias para la instalación del Exchange. Después de finalizar las actualizaciones, termina la verificación de este proceso.
19. El paso número siete, debemos correr DomainPrep, en el caso de tener varios subdominios debemos correr esta herramienta en cada uno. Aceptamos la licencia. Después sale la herramienta de DomainPrep



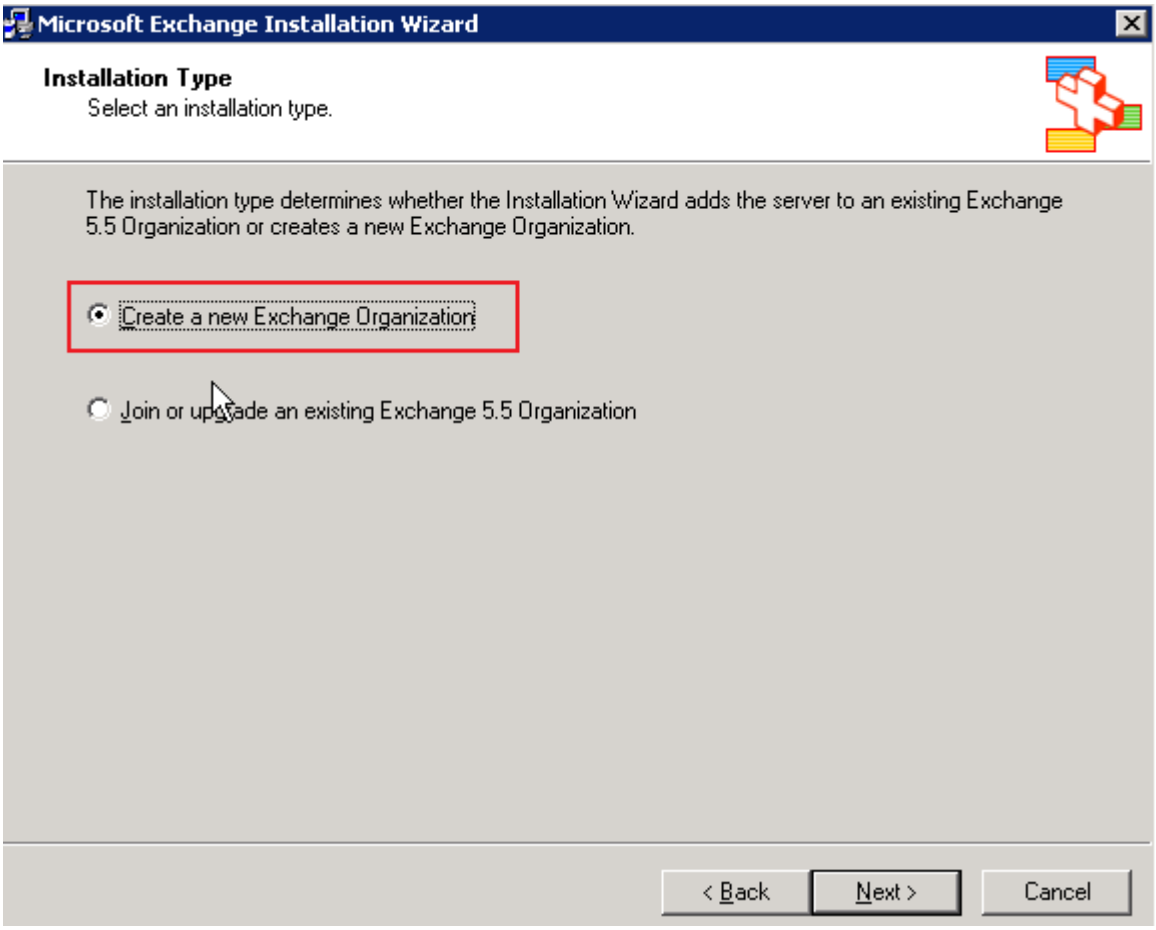
20. Se pone siguiente y se espera a que se realice la instalación. Se finaliza la instalación.

21. El paso número ocho podemos realizar la instalación de Exchange finalmente.

22. Se corre la herramienta, se acepta la licencia y se corre la instalación típica.

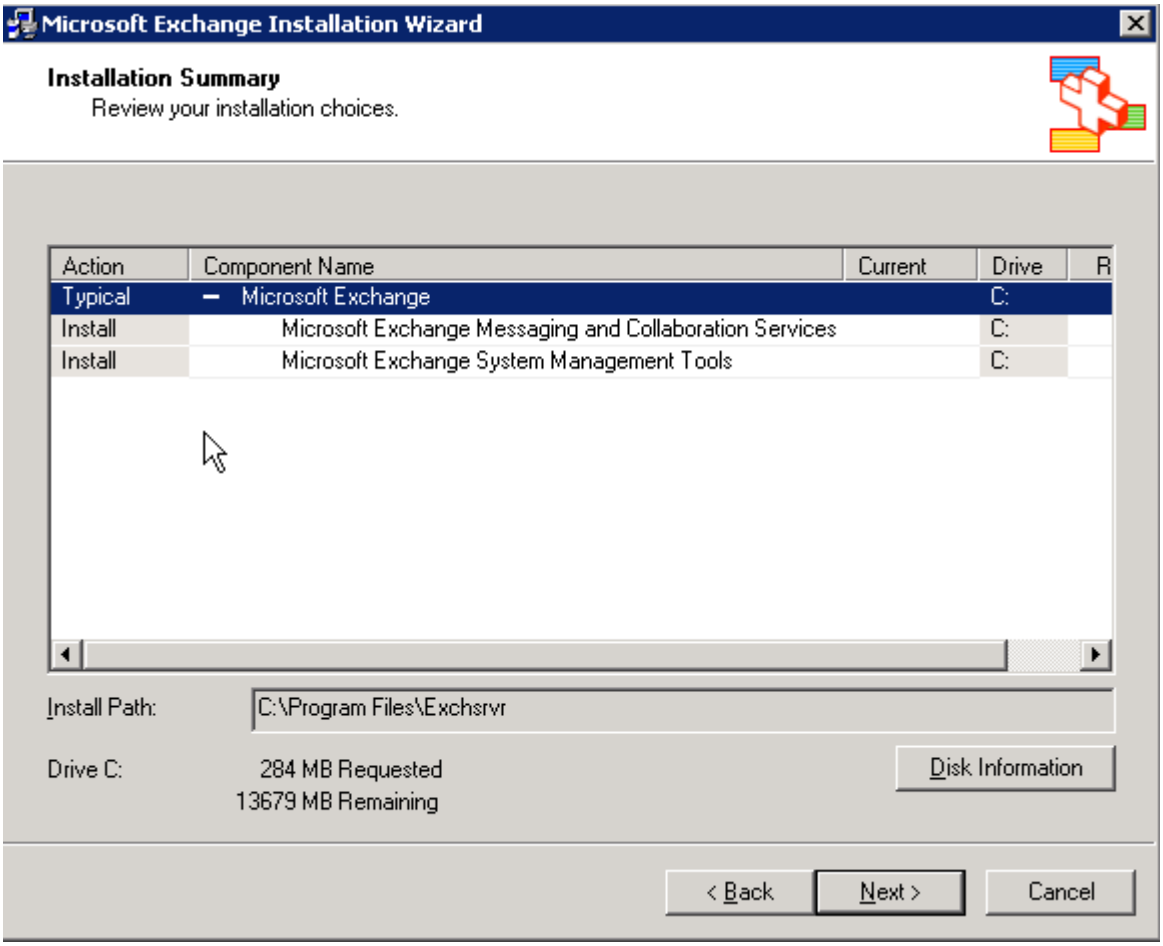


23. Damos siguiente y seleccionamos la creación de una nueva organización de Exchange

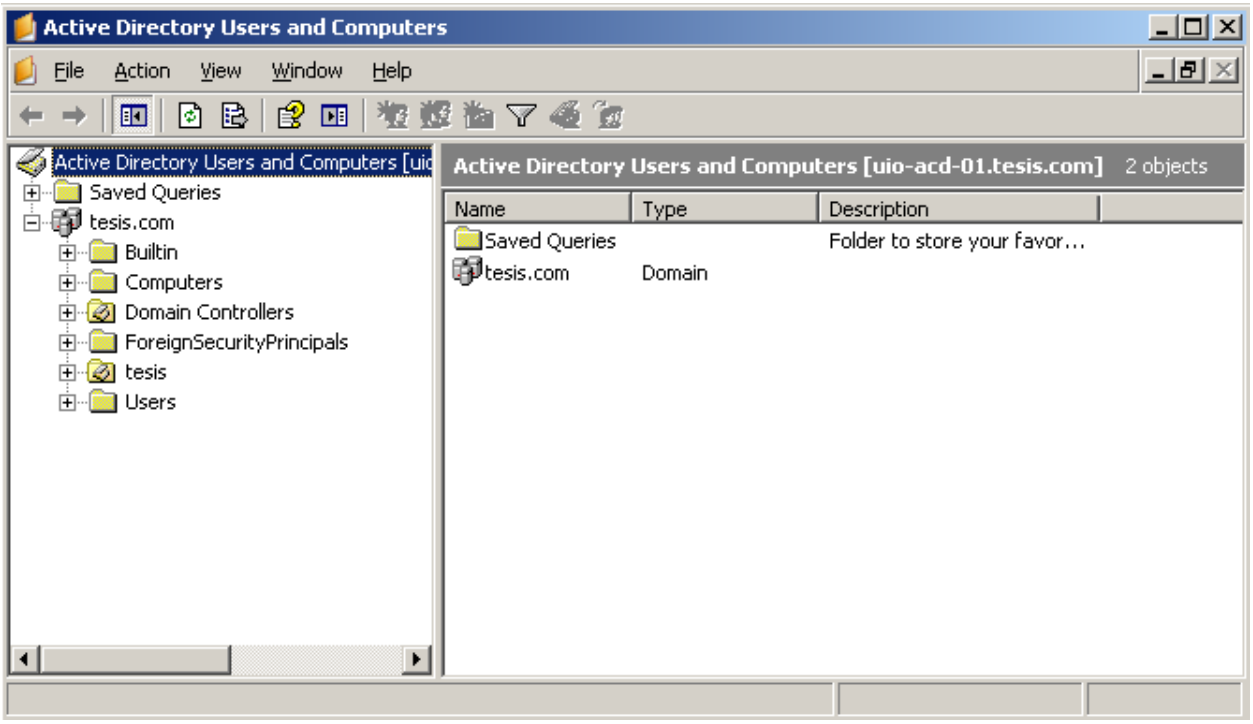


24. Y asignamos el nombre a la organización, y aceptamos la licencia.

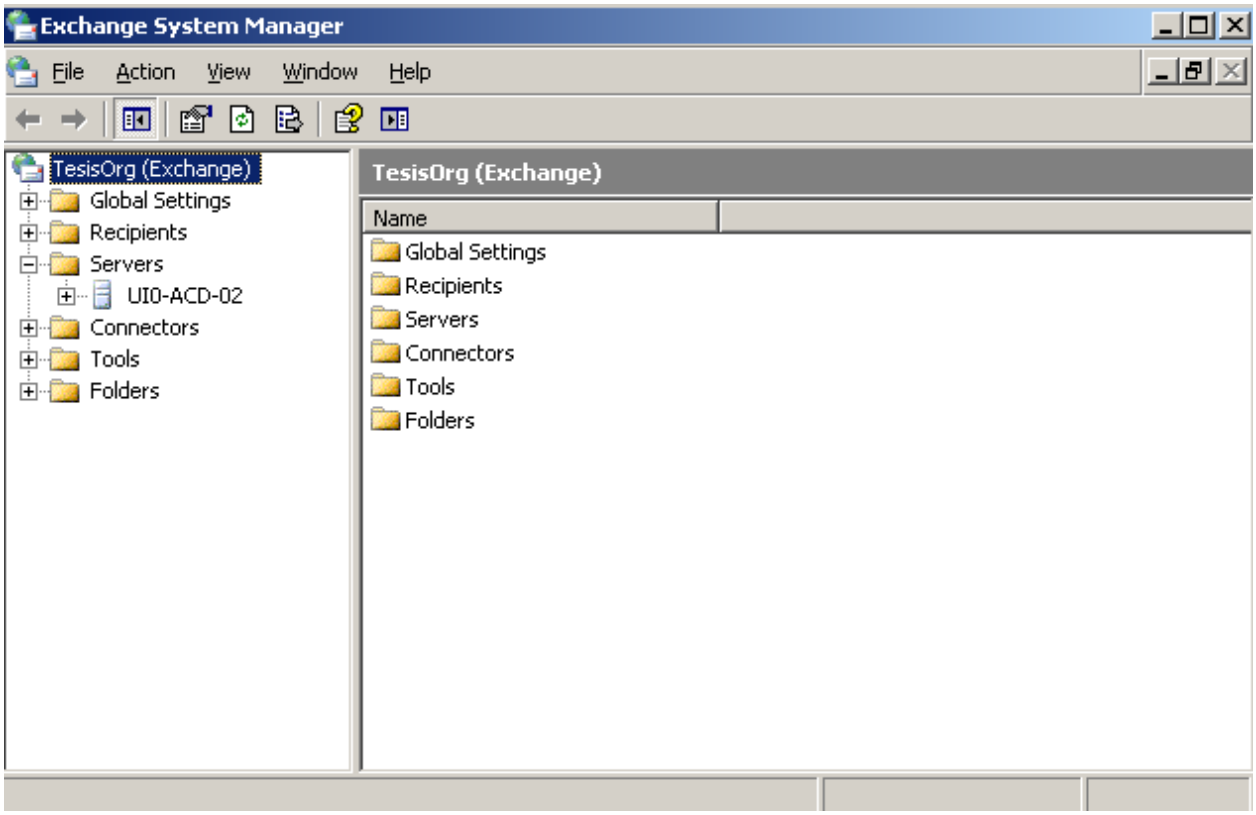
25. Se pone siguiente y se le asigna la instalación típica de Exchange.



26. Se pone siguiente y se realiza la instalación. Después de finalizar la instalación ponemos siguiente y nos pregunta si queremos instalar Exchange en otro servidor, ponemos que no y siguiente.
27. Nos dan sugerencias de lo que se debería hacer después de la instalación de Exchange como la repartición de memoria.
28. Se instala la consola que mostramos a continuación, es muy parecida a la del Directorio Activo y la única diferencia es que al momento de crear los usuarios los hace con un mail box, y si lo hiciéramos desde el Directorio Activo no se crearían las cuentas de mail. Por eso es preferible hacerlo desde esta consola en el ordenador de Exchange.

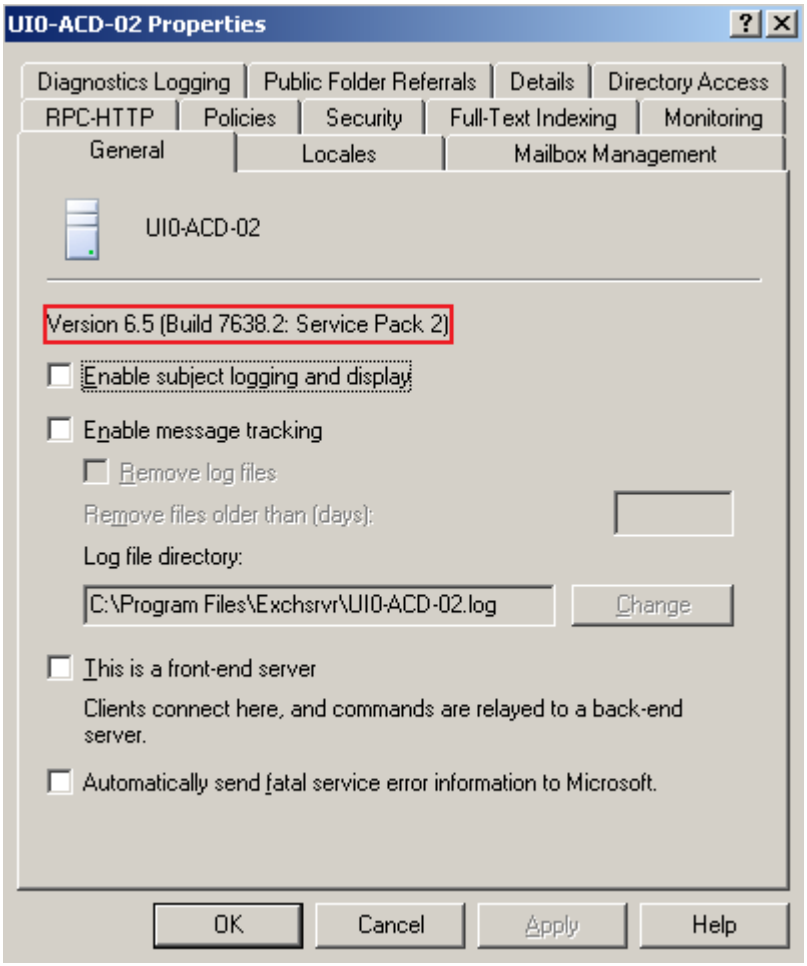


29. Además tenemos una consola de administración de Exchange en donde podemos realizar el control y monitoreo de los servidores conectados, y de herramientas que nos permiten saber el estado y manejo de colas de los correos, etc.



30. A medida que creamos usuarios podemos ir viendo las bandejas que se van creando

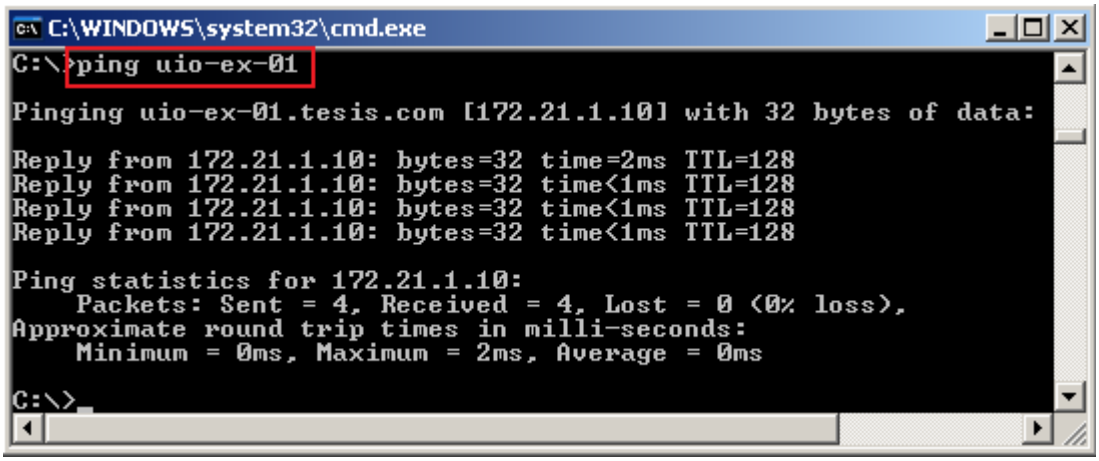
31. No hay que olvidar de instalar el service pack 2 para Exchange



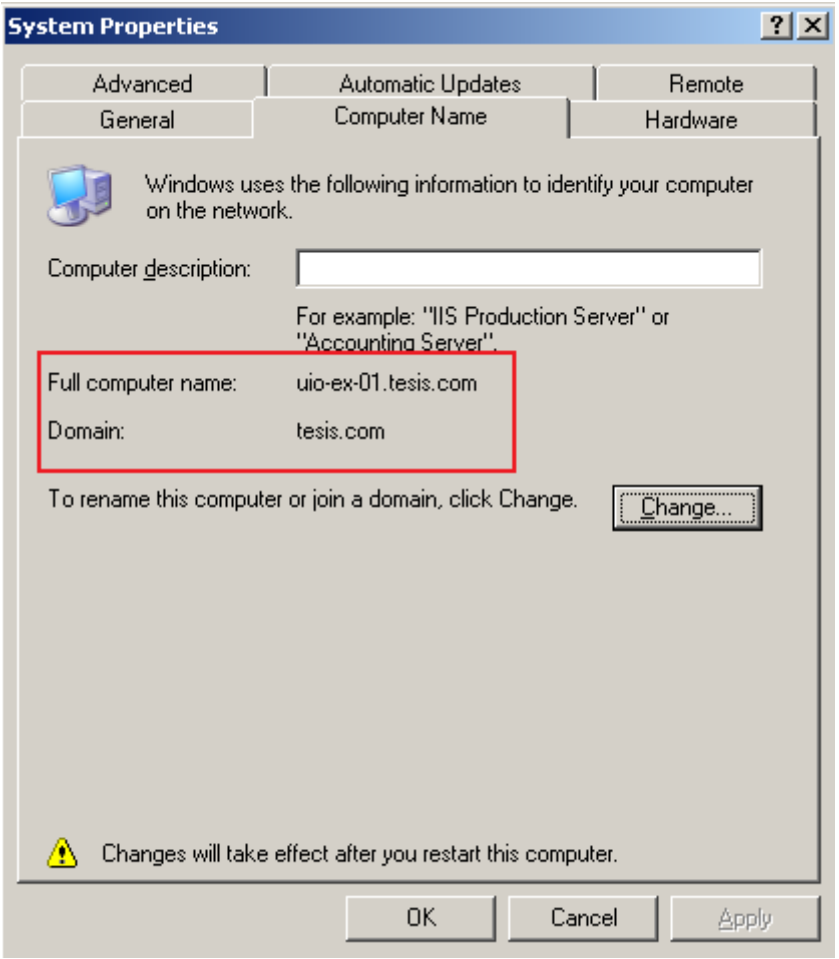
Pruebas

- Comprobar la configuración de red y la integración al dominio.

  Para comprobar la configuración de red hacemos ping desde el isa server a esta máquina.

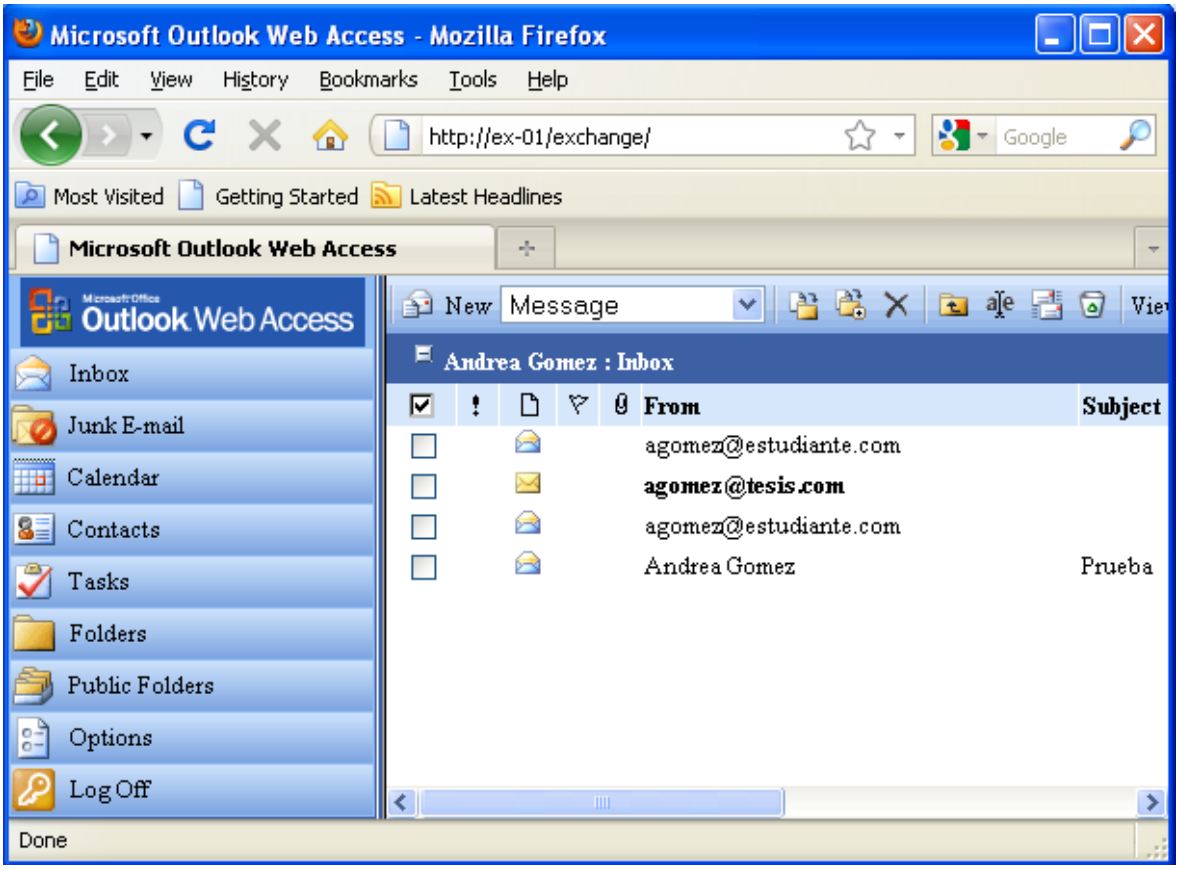


Para autenticarnos al directorio activo es necesario cambiar el nombre de nuestra maquina en este caso va a ser uio-ex-01.tesis.com y el nombre del dominio va a ser tesis.com como se muestra en la figura.



- Probar SMTP para envió y recepción de mensajes, revisar usuarios con mail y la cola de mensajes.

  Para probar el envió y recepción de mensajes se configuro el usuario OWA que es un servicio el cual nos permite utilizar el Outlook vía web para revisar los correos enviados o recibidos. En este caso la figura nos muestra los mensajes de la cuenta agomez@tesis.com y refleja la bandeja de entrada con los mensajes recibidos. De este mismo servidor de correo nos sirvió para hacer el envío y recepción de mensajes de una red a otra.



También se configuró thunderbird para en envío y recepción de correos electrónicos de infraestructura a infraestructura.

ANEXO 4

Proceso de implementación y pruebas de OpenCA

1. Instalación de herramientas para compilación

```
#apt-get install g++ gcc make
```

2. Instalación de perl y modulos necesario

```
#apt-get install libxml-perl libxml-regexp-perl libdbi-perl perl perl-modules libldap2 libldap2-dev libdbd-mysql-perl libauthen-sasl-perl libcgi-session-perl libconvert-asn1-perl lib libcgi-session-perl libconvert-asn1-perl libdigest-md2-perl libdigest-md4-perl libdigest-sha1-perl libio-socket-ssl-perl libio-stringy-perl libmime-lite-perl libmime-perl libmailtools-perl libnet-server-perl liburi-perl libxml-twig-perl libintl-perl libnet-ldap-perl
```

3. Instalación de apache y web server

```
#apt-get install apache2
```

4. Instalación de OpenSSL

```
#apt-get install openssl libssl-dev
```

5. Instalación de Mysql

```
#apt-get install mysql-server
```

6. Instalación de OpenCA

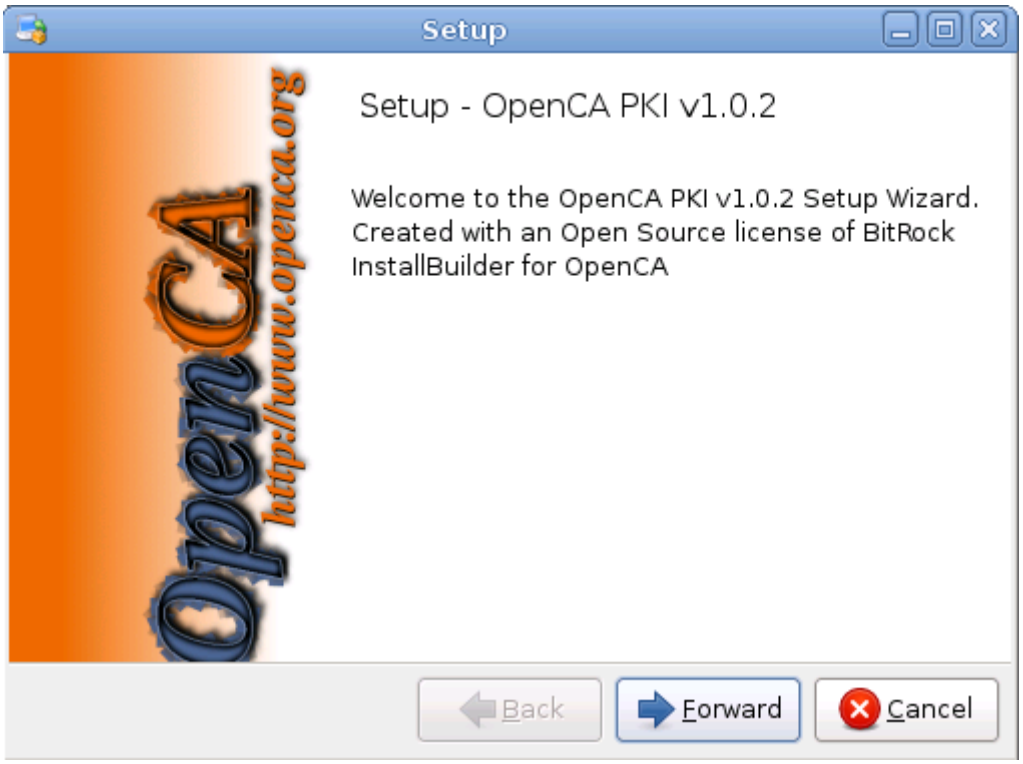
a) Descargar archivo de openca-tools

b) Dar los permisos necesarios y ejecutar

```
#chmod 755 openca-tools

#./openca-tools
```

c) Configuramos con el wizard de instalación

- Aceptamos la licencia
- Ponemos la instalación en el directorio /usr
- Subscribimos nuestra dirección de email



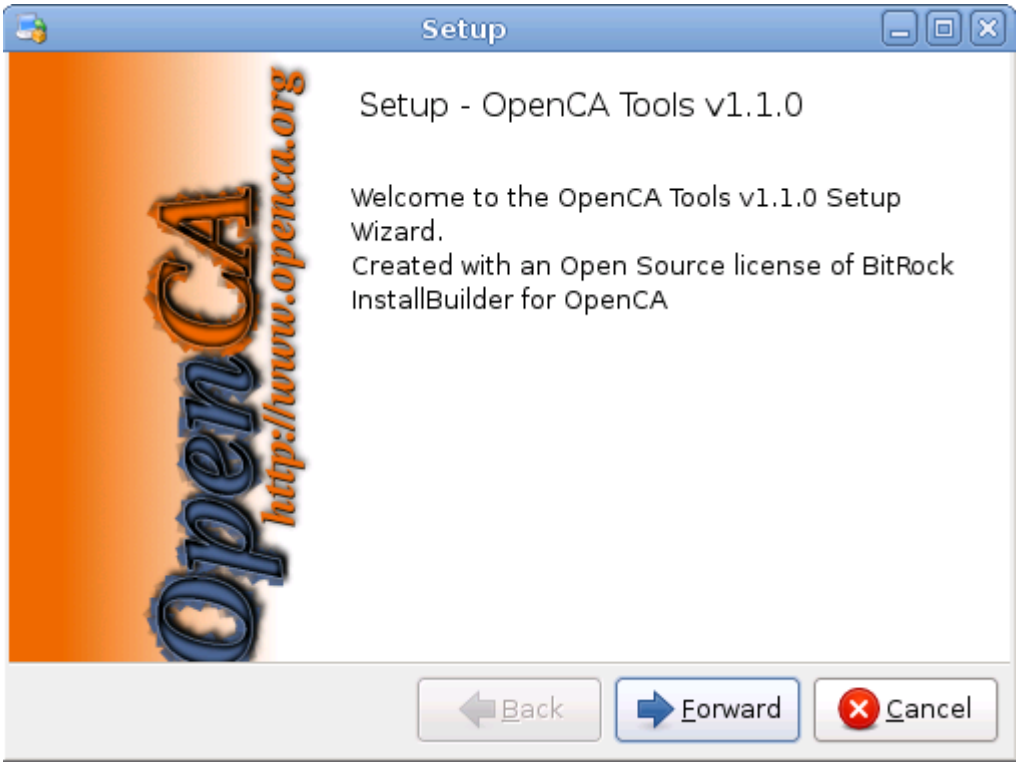
d) Descargar archivo de openca-base

e) Dar los permisos necesarios y ejecutar

```
#chmod 755 openca-tools

#./openca-base
```

f) Configuramos con el wizard de instalación

- Aceptamos la licencia
- Ponemos la instalación en el directorio /usr
- Subscribimos nuestra dirección de email



Configuración de mysql

1. Ingresamos a mysql

```
#mysql –u root –p
```

2. Creamos la base de datos para openca y para openra

```
>create database openca;
>create database openra;
```

3. Creamos los usuarios necesarios

```
>grant all privileges on openca.* to openca@localhost identified by
'openca';
>grant all privileges on openra.* to openra@localhost identified by
'openra';
```

Configuración de apache web server

1. Editamos el archivo `/etc/apache2/sites-available/site-ssl`

2. Generamos certificados de apache SSL

```
#mkdir /etc/apache2/ssl
#cd /etc/apache2/ssl
#openssl req –x509 –newkey rsa:2048 –keyout cakey.pem –days 3650 –
out cacert.pem –nodes
```

3. Editamos el archivo `/etc/apache2/httpd.conf`

```
#serverName localhost
```

4. Reiniciamos apache

```
#/etc/init.d/apache2 restart
```

Configuración de OpenCA

1. Para la configuración de openca es necesario revisar el archivo

```
#vi /opt/openca/etc/openca/config.xml
```

2. Ejecutamos el archivo para correr la configuración de openca

```
#./opt/openca/etc/openca/configure_etc.sh
```

3. Reiniciamos el servicio de openca

```
#./opt/openca/etc/openca/openca_stop
#./opt/openca/etc/openca/openca_start
```

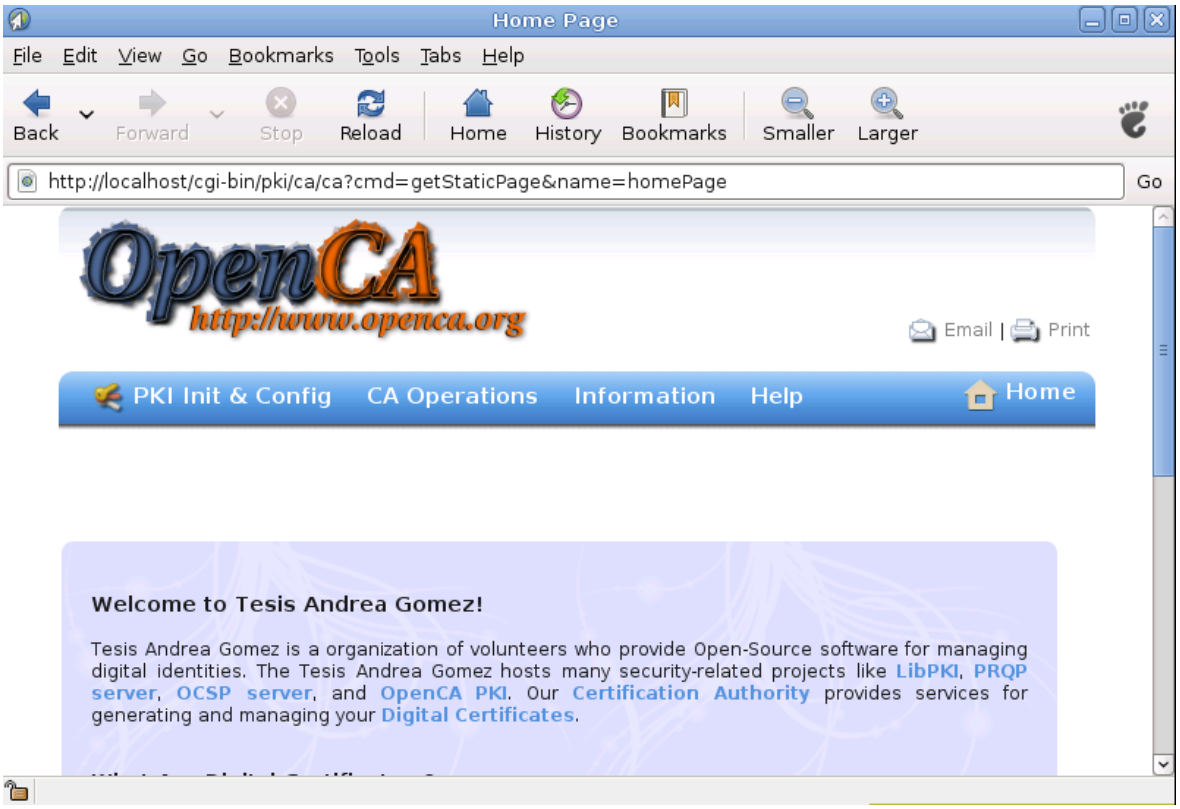
4. Accedemos por web para verificar

   https://localhost

Pruebas

- Probar la emisión de certificados y firmas digitales.

  Para probar la emisión de certificados se debe utilizar la consola de administración de OpenCA y generar los certificados digitales en base a los usuarios que se encuentren configurados en la red y con ello se generan las firmas digitales.



ANEXO 5

Proceso de implementación y pruebas de Firewall Iptables

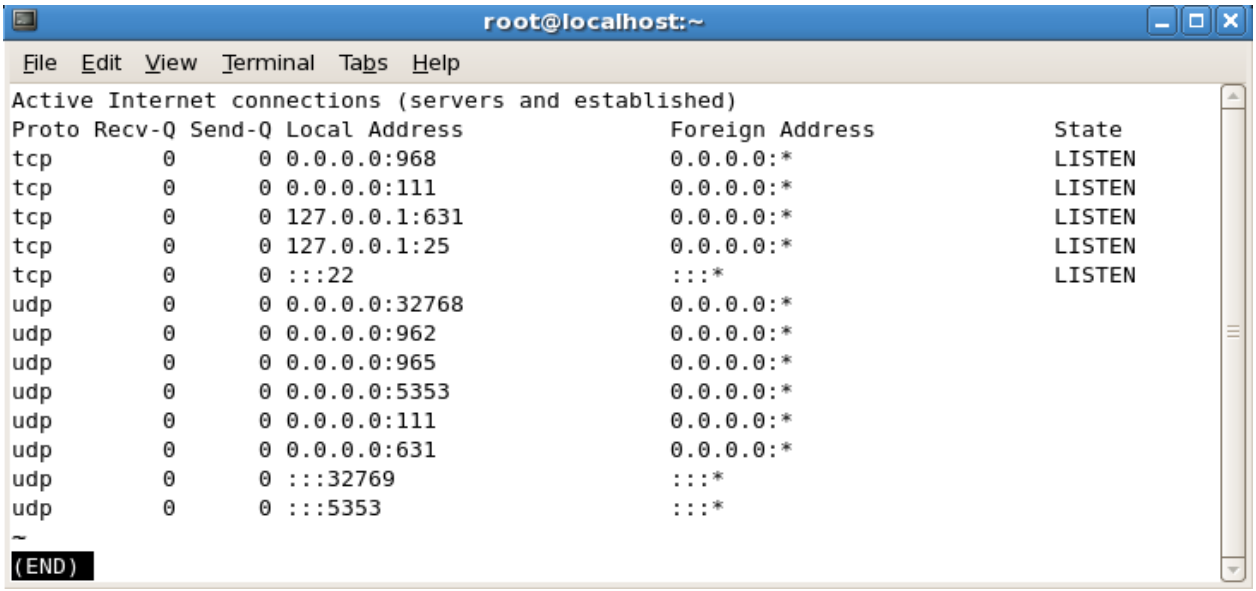
Para implementar un firewall es necesario tomar ciertas medias de seguridad como las que mencionamos a continuación:

1. Crear una clave para ingresar al sistema.
2. Establecemos un timeout para todos los usuarios que ingresen al sistema, este tiempo límite va a ser de una hora máximo.

   ```
   #vi /etc/profile

   #export TMOUT=3600
   ```

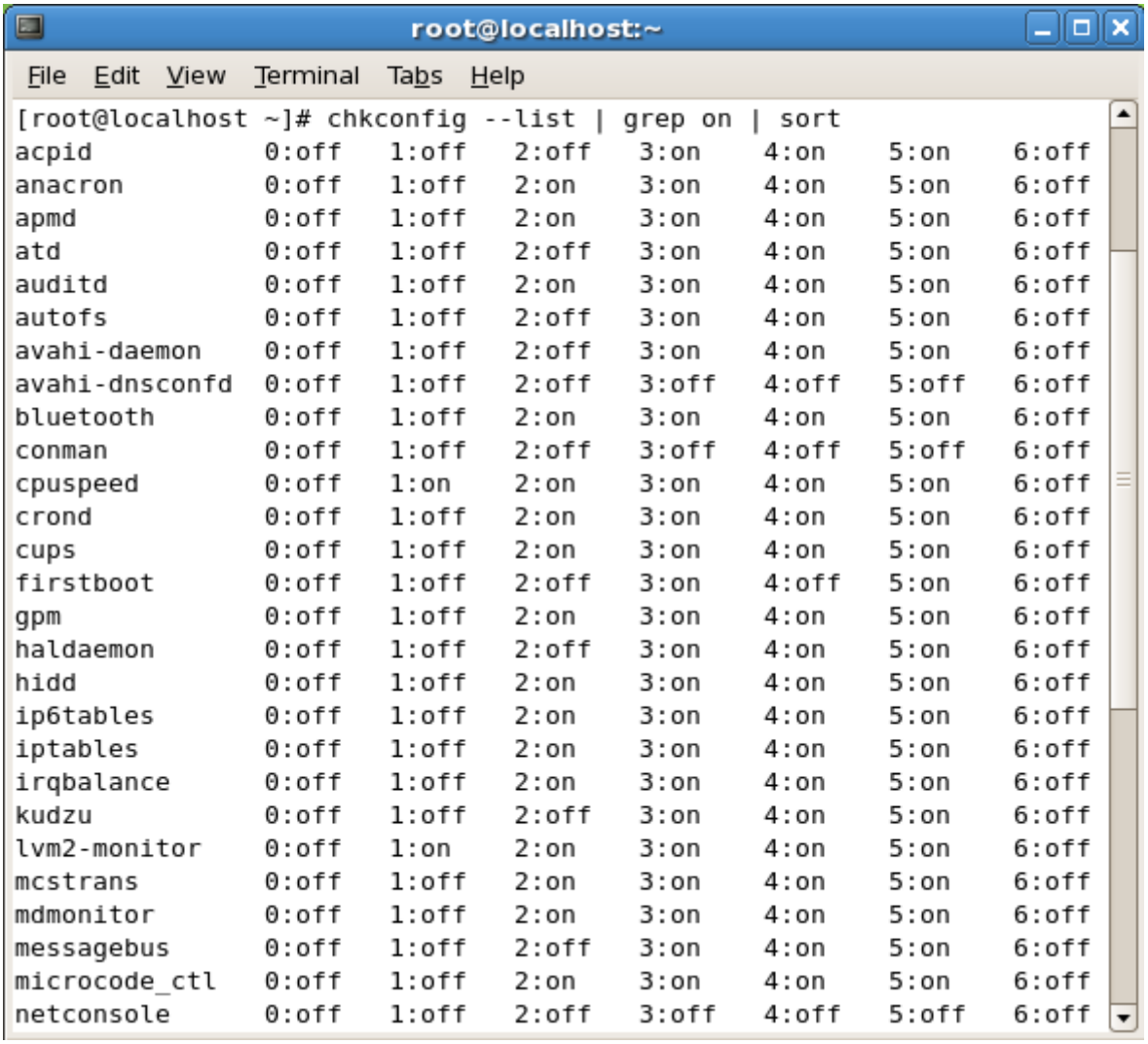
3. Listamos todos los puertos para ver qué servicios de red están activados

   ```
   #netstat -anut    | less
   ```



4. Sacamos una lista de todos los servicios que están inicializados

   ```
   #chkconfig --list | grep on | sort
   ```



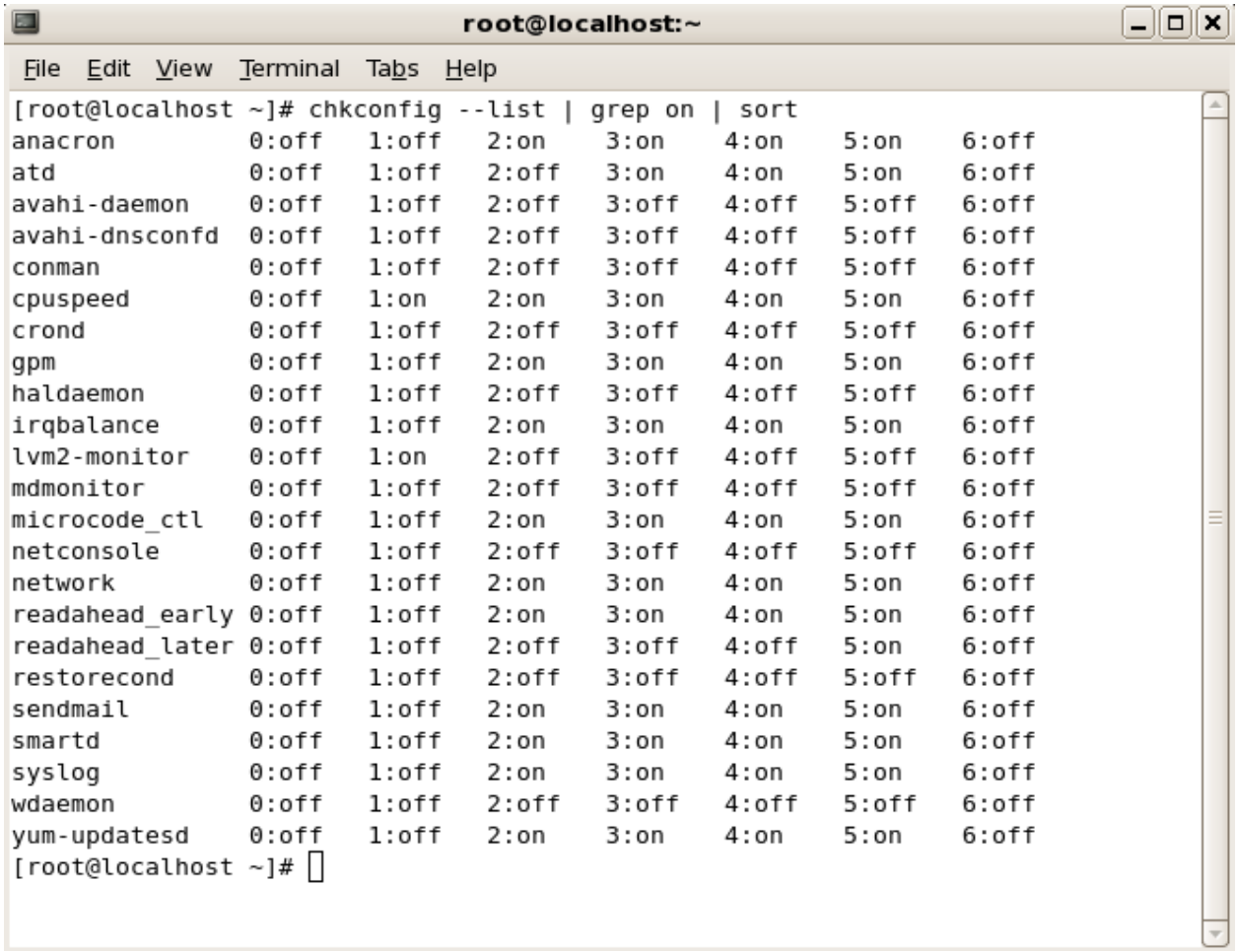
5. Deshabilitamos todos los servicios que no necesitamos

   ```
   #chkconfig acpid off
   ```

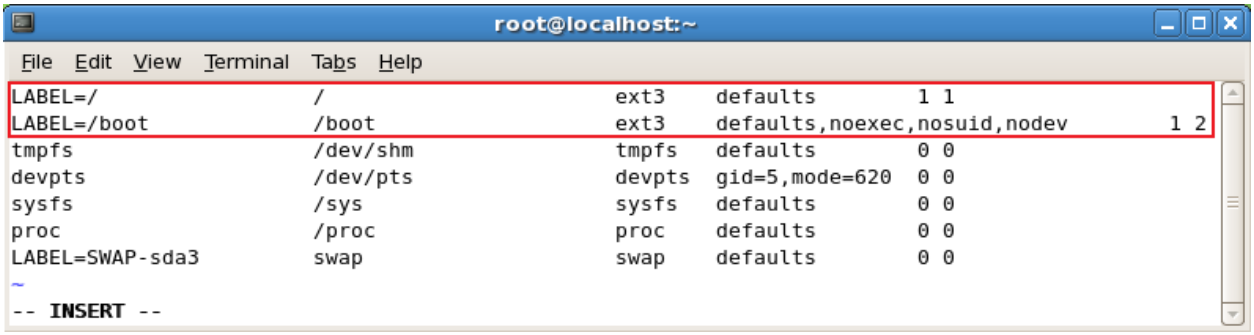
   Solo los servicios listados a continuación deben estar activados:

   - anacron (Fedora)
   - atd
   - crond (Fedora, Red Hat)
   - cpuspeed (Fedora)
   - gpm
   - irqbalance (Fedora)
   - microcode_ctl (Fedora)

- network
- random
- readahead (Fedora)
- readahead_early (Fedora)
- sendmail (Fedora, Red Hat)
- smartd (Fedora)
- syslog



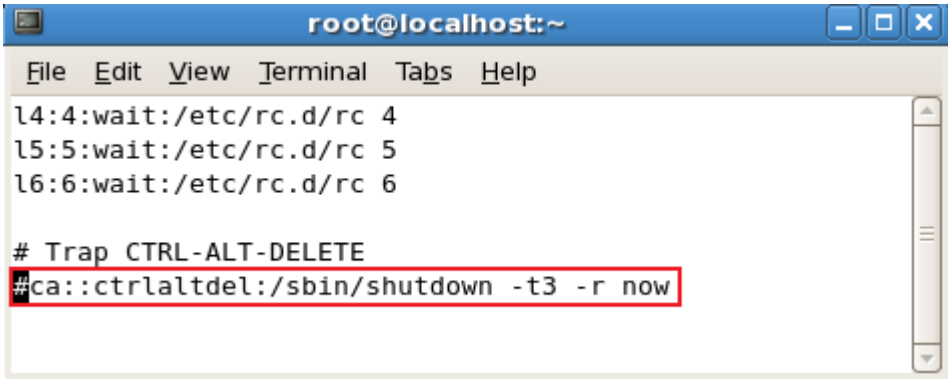
6. Configuramos el archivo de fstab y le damos los siguientes permisos para dar más seguridad al sistema.



7. Deshabilitamos el Ctrl-Alt-Delete

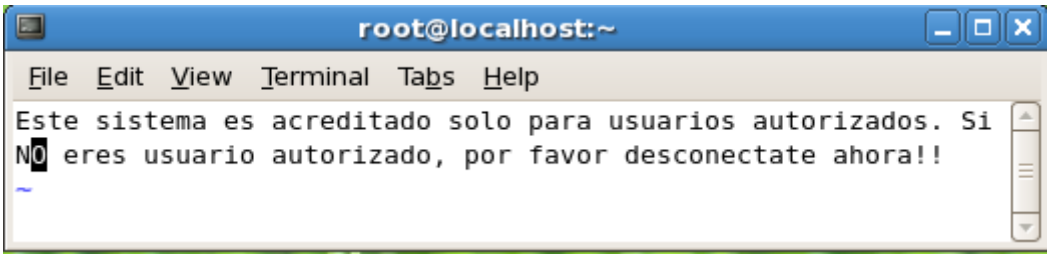
   `#vi /etc/inittab`

   Comentamos la línea ca-line



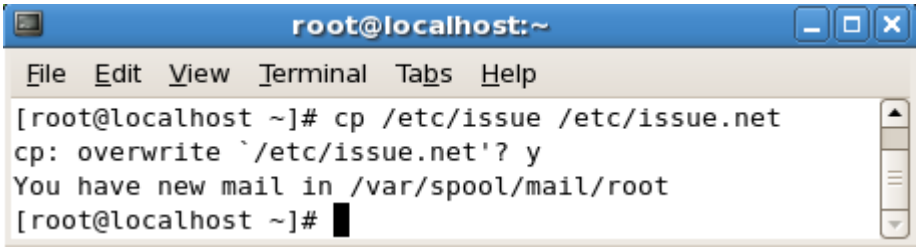
8. Cambiamos los archivos `/etc/issue` y `/etc/issue.net` para que no revele ninguna información sobre el sistema operativo

   Quitamos todas las líneas y ponemos el siguiente comentario

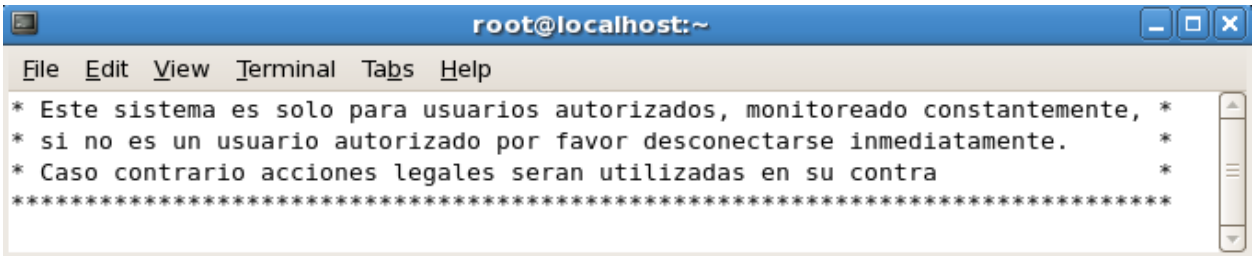


   Y copiamos la misma información en /etc/issue.net

   `#cp /etc/issue /etc/issue.net`



9. Cambiamos el archivo /etc/motd para mostrar los términos de uso del sistema



10. Reiniciamos el sistema

```
#reboot
```

11. Hacemos pruebas de lo que cambiamos

    a. Verificamos que Ctrl-Alt-Delete no funciona.

12. Configuramos las reglas de IPTABLES de acuerdo a nuestras necesidades, listamos las iptables que estan aplicadas por el momento

```
#iptables -n -L
```

13. Creamos un archivo en donde almacenaremos las reglas de IPTABLES

    #vi fw

    Agregamos las reglas explicadas a continuación:

    - Vaciamos las reglas

```
iptables -F INPUT

iptables -F OUTPUT

iptables -F FORWARD
```

```
iptables -X

iptables -t nat -F
```

- Aplicamos las políticas por defecto

```
iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP
```

- Permitimos todas las conexiones en un interfaz local

```
iptables -A INPUT -i lo -j ACCEPT
```

- Negar las conexiones del exterior a la interfaz local

```
iptables -A INPUT -d 127.0.0.0/8 -j REJECT
```

- Permitir el trafico a la interfaz interna

```
iptables -A INPUT -i eth1 -s 172.21.2.1/24 -j ACCEPT

iptables -A OUTPUT -o eth1 -d 172.21.2.1/24 -j ACCEPT
```

- Permitir el tráfico interno

```
iptables -A FORWARD -o eth0 -i eth1 -j ACCEPT
```

- Web externo

```
iptables -A INPUT -i eth0 -p tcp -s any/0 --sport 1024: -d
10.0.0.10/24 --dport 80 -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp -s 10.0.0.10/24 --sport 80
-d any/0 --dport 1024: -j ACCEPT
```

- Enmascaramiento

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

- Permito desde LAN a WAN

Puerto HTTP www

```
iptables -A FORWARD -i eth1 -p tcp -o eth0 --dport 80 -m
state --state RELATED,ESTABLISHED -j ACCEPT
```

Puerto SSH, SCP, SFTP

```
iptables -A FORWARD -i eth1 -p tcp -o eth0 --dport 22 -j AC-
CEPT
```

Puerto HTTPS/SSL para transferencia segura

```
iptables -A FORWARD -i eth1 -p tcp -o eth0 --dport 443 -j AC-
CEPT
```

Puerto POP3 e-mail

```
iptables -A FORWARD -i eth1 -p tcp -o eth0 --dport 110 -j AC-
CEPT
```

Puerto POP3 sobre SSL

```
iptables -A FORWARD -i eth1 -p tcp -o eth0 --dport 995 -j AC-
CEPT
```

Puerto SMTP sobre SSL

```
iptables -A FORWARD -i eth1 -p tcp -o eth0 --dport 465 -j AC-
CEPT

iptables -A FORWARD -i eth1 -p tcp -s ! 172.21.2.1/24 -o eth0
--dport 1863 -j ACCEPT


#iptables -A FORWARD -i eth1 -p icmp -o eth0 --icmp-type 0 -j
ACCEPT

iptables -A FORWARD -i eth1 -p icmp -o eth0 --icmp-type 8 -j
ACCEPT
```

- Salida a la WAN

```
iptables -A OUTPUT -o eth0 -p tcp --dport 80 -m state --state
NEW -j ACCEPT

iptables -A OUTPUT -o eth0 -p udp --dport 53 -m state --state
NEW -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --dport 22 -m state --state
NEW -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --dport 1863 -m state --
state NEW -j ACCEPT

iptables -A OUTPUT -o eth0 -p udp --dport 123 -m state --
state NEW -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp --dport 123 -m state --
state NEW -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --dport 21 -m state --state
NEW -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --dport 20 -m state --state
NEW -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --dport 25 -m state --state
NEW -j ACCEPT
```

- Puertos SNMP protocolo simple de administración de la red

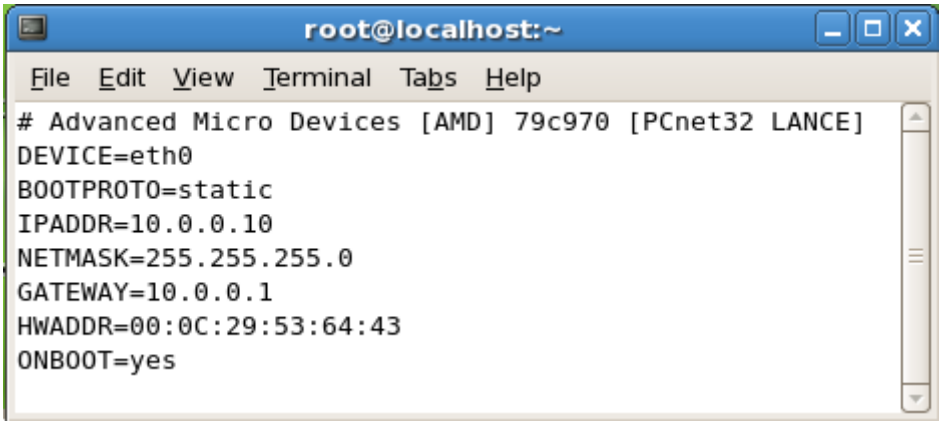
```
iptables -A INPUT -p udp --dport 161 -j ACCEPT

iptables -A FORWARD -p udp --dport 161 -j ACCEPT

iptables -A INPUT -p udp --dport 162 -j ACCEPT

iptables -A FORWARD -p udp --dport 162 -j ACCEPT
```

14. Configuración de eth0 (ip publica)

    Dirección IP = 10.0.0.10

    Mascara de red = 255.255.255.0

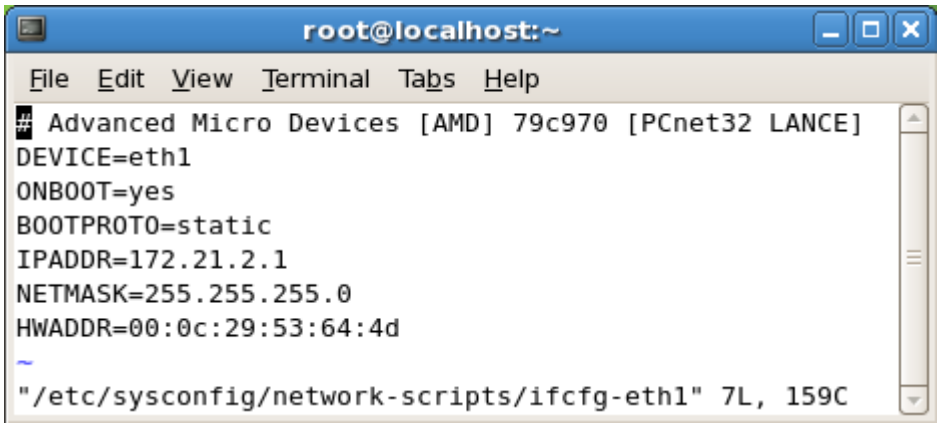
    Gateway = 10.0.0.1



15. Configuración de eth1 (ip privada)

    Dirección IP = 172.21.2.1

    Mascara de red = 255.255.255.0

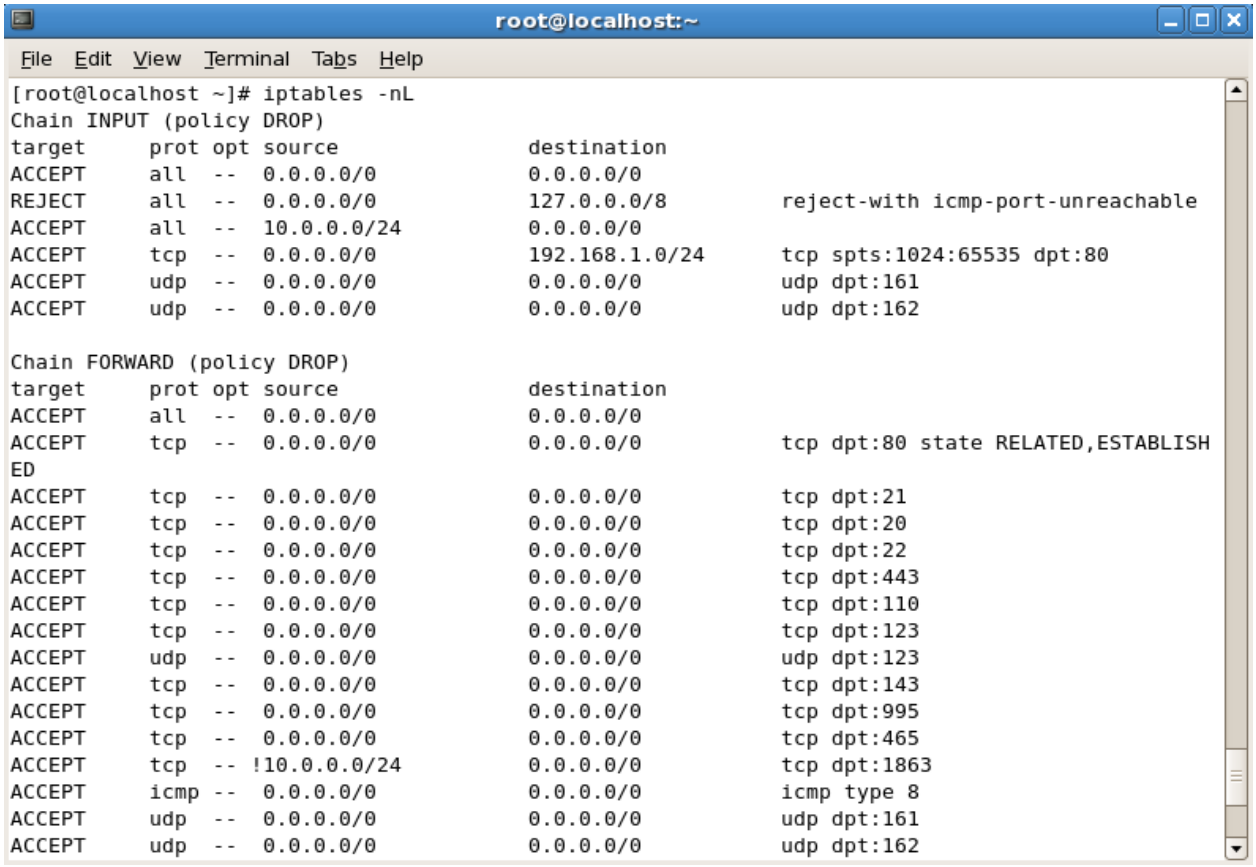


16. Corremos el archivo

```
#./fw
```

17. Observamos las reglas aplicadas

```
#iptables -nL
```



18. Guardamos las reglas iptables

```
#iptables-save > /etc/sysconfig/iptables
```

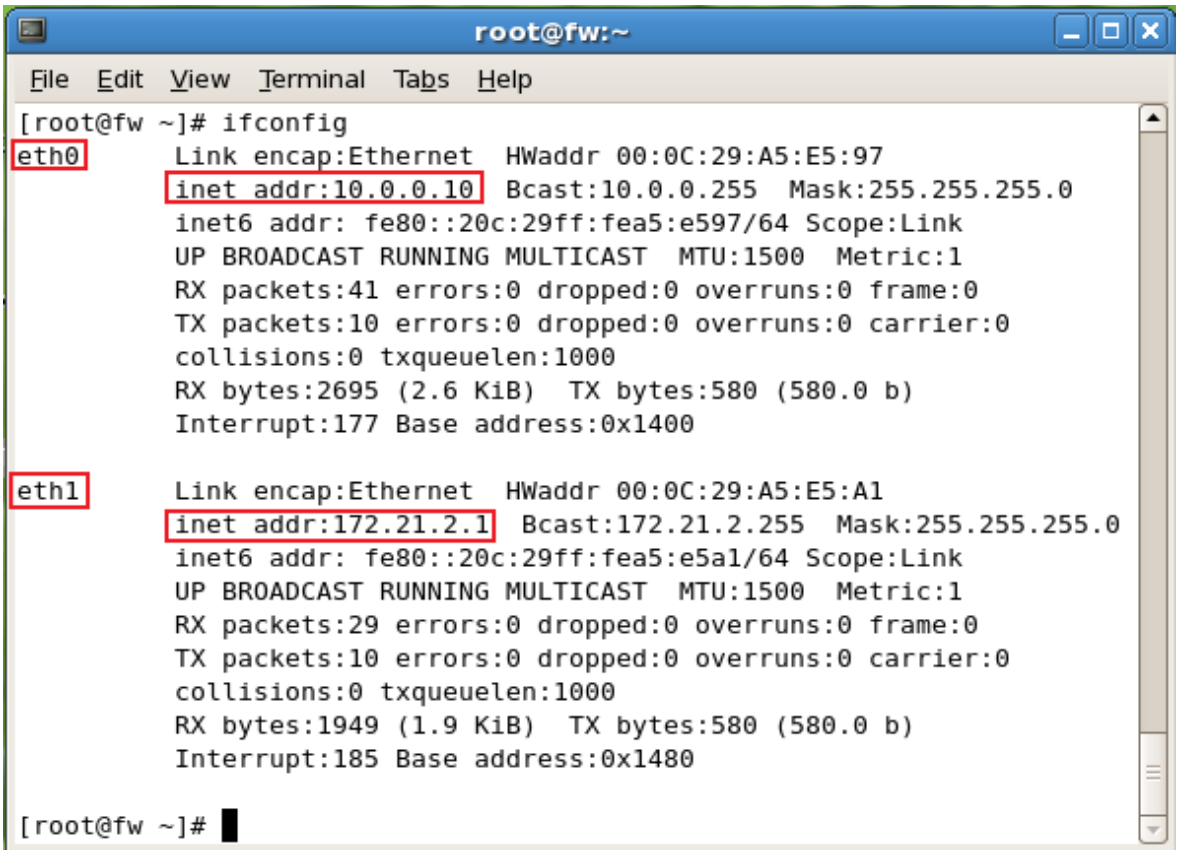
19. Levantamos el servicio

```
#chkconfig iptables on

#service iptables start
```

Pruebas

- Configuración de tarjetas de red.

Realizamos ifconfig para ver las tarjetas de red que estan configuradas



- Funcionamiento del filtrado de paquetes por la aplicación de las reglas.

Para comprobar esta prueba se realizó una serie de intentos que probaron el funcionamiento de la red, es decir la comunicación y el intercambio de mensajes entre las infraestructuras fueron el resultado del funcionamiento de las reglas aplicadas en el firewall.

ANEXO 6

Proceso de implementación y pruebas de OpenLDAP

La configuración de este ordenador va a ser en el Sistema Operativo de GNU/Linux Fedora 11.

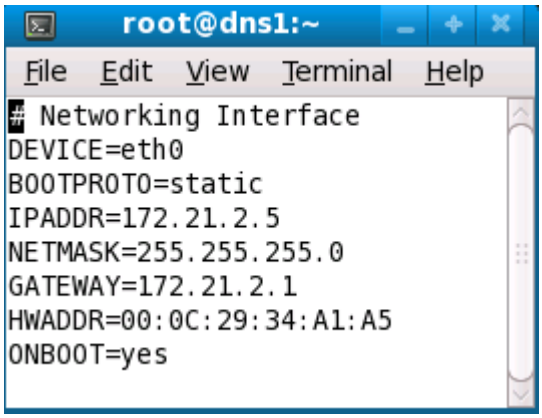
Verificamos la configuración de la red.

Direccion IP = 172.21.2.5

Mascara de red = 255.255.255.0

Gateway = 172.21.2.1

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```



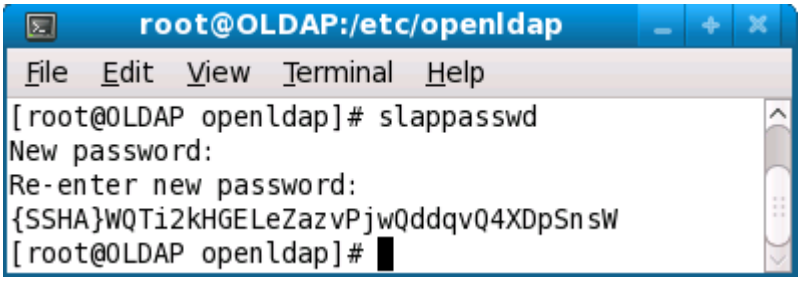
Configuración OpenLDAP servidor

1. Instalamos los paquetes necesarios para la implementación de este servicio.

   ```
   #yum -y install openldap openldap-servers openldap-clients
   ```

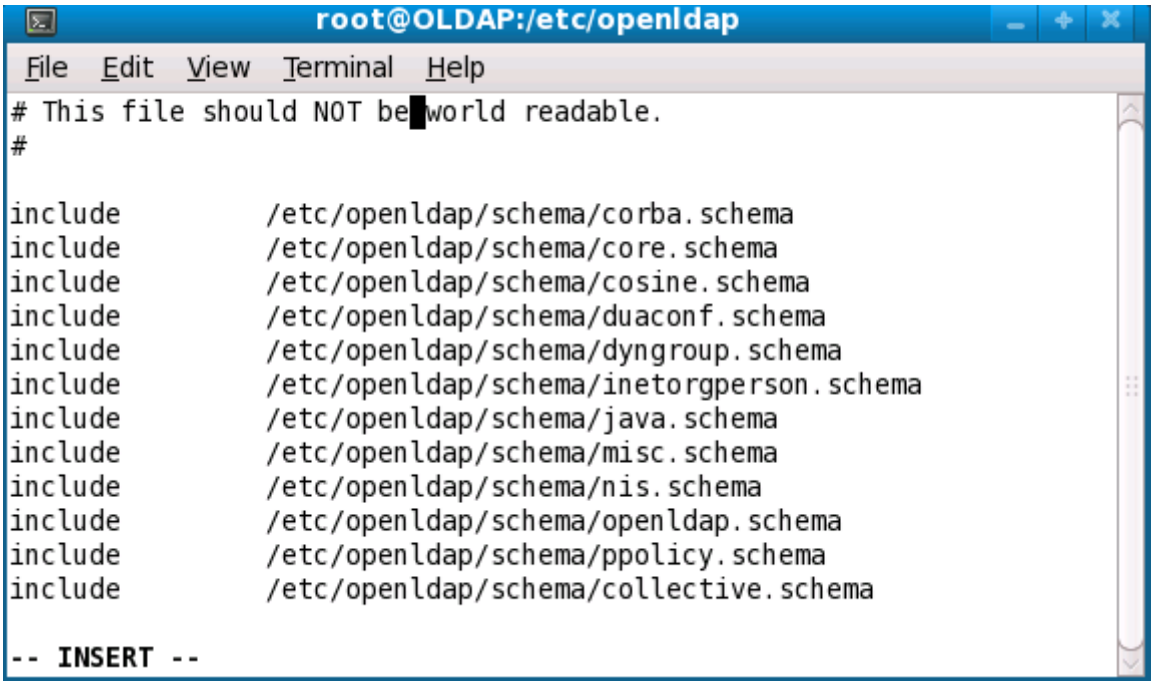
2. Generamos las claves para el acceso a LDAP, esta le servirá para el usuario administrador del sitio.

   ```
   #slappasswd
   ```



3. Configuramos el fichero de esquema, Base DN, Root DN y Root DN password

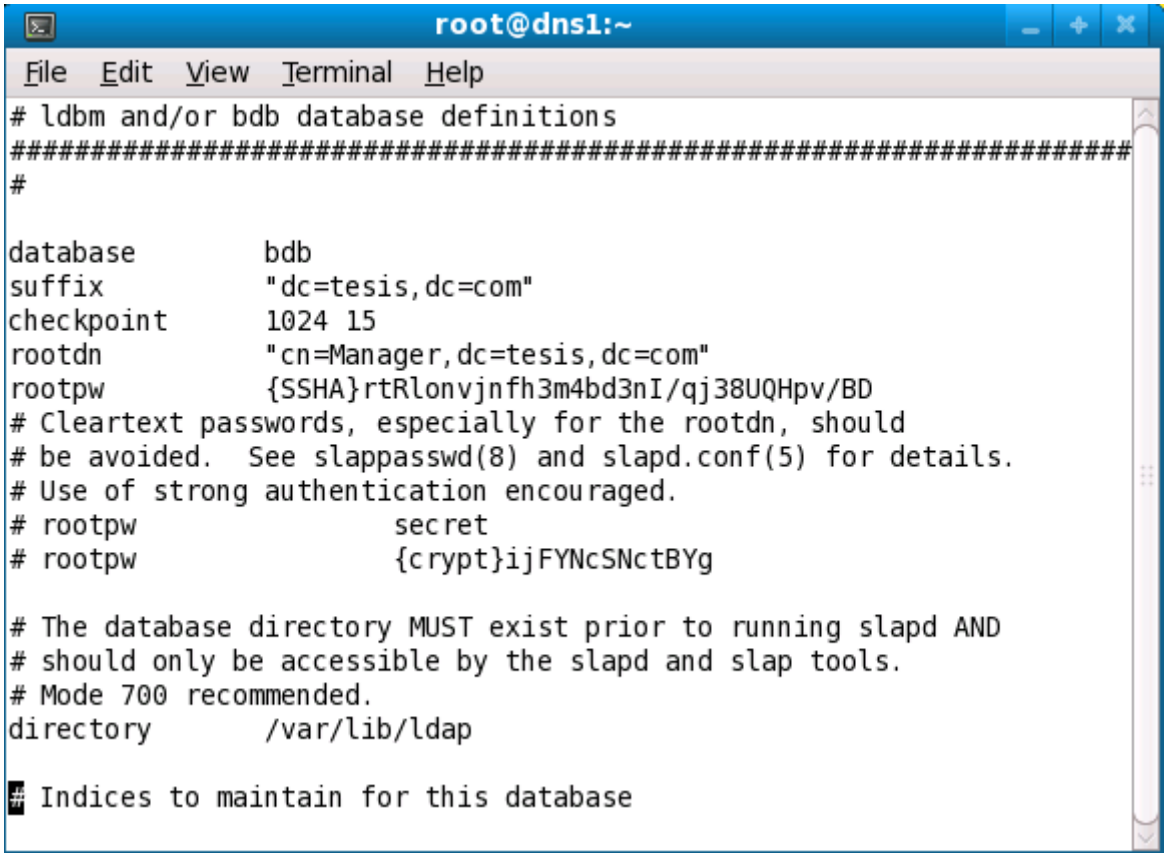
```
#vi /etc/openldap/slapd.conf
      include /etc/openldap/schema/core.schema
      include /etc/openldap/schema/cosine.schema
      include /etc/openldap/schema/inetorgperson.schema
      include /etc/openldap/schema/nis.schema
      include /etc/openldap/schema/misc.schema
```



Cambiar los sufijos de rootdn y rootpw. Además se definirá el nuevo directorio que se utilizara como libreta de direcciones, donde el dc=tesis, dc=com corresponde al nombre único y exclusivo para el nuevo directorio.

```
# vi /etc/openldap/slapd.conf
      suffix "dc=tesis, dc=com"
```

```
rootdn "cn=Manager, dc=tesis, dc=com"

rootpw secret
```

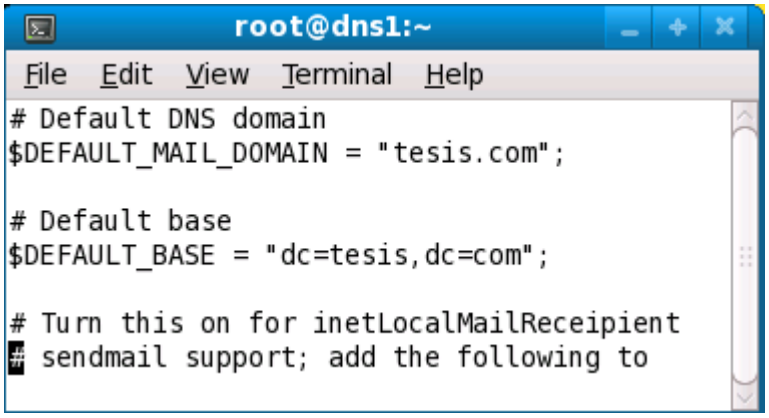


4. Copiamos los archivos que deseamos migrar al ldap como usuarios y grupos.

```
#cp /etc/passwd /etc/passwd.old

#cp /etc/group /etc/group.old
```

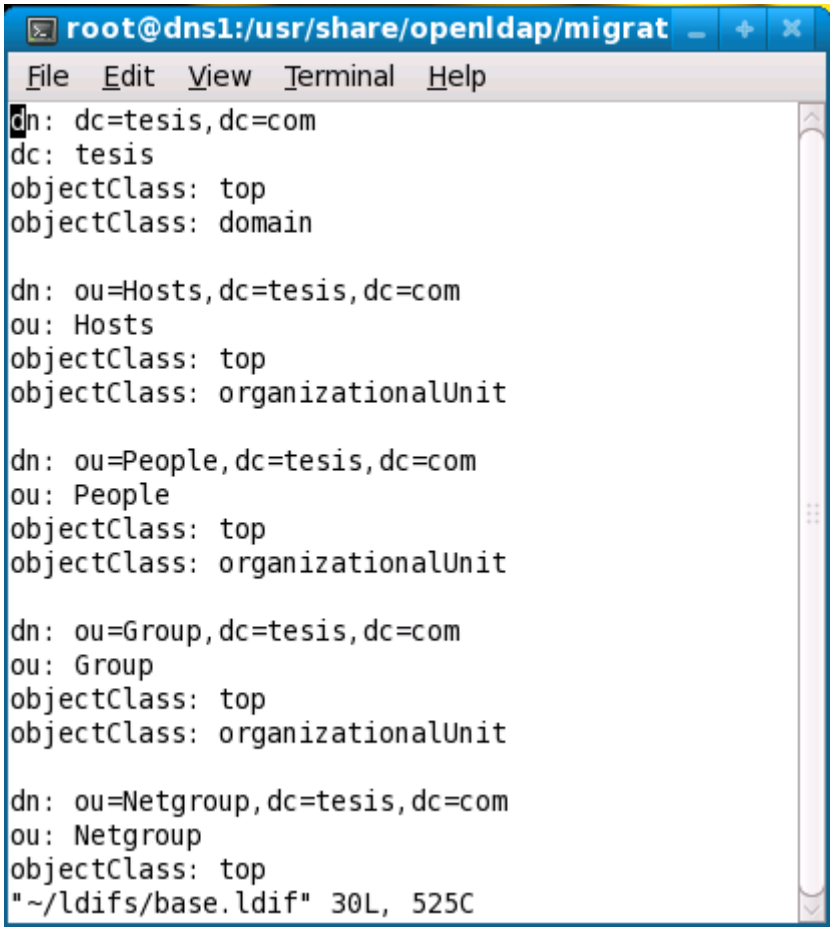
5. Cambiar el directorio de herramientas de migración y migrar todos los datos de autenticación de LDAP.

```
#cd /usr/share/openldap/migration

# vi migrate_common.ph

$DEFAULT_MAIL_DOMAIN = "tesis.com";

$DEFAULT_BASE = "dc=tesis, dc=com"
```



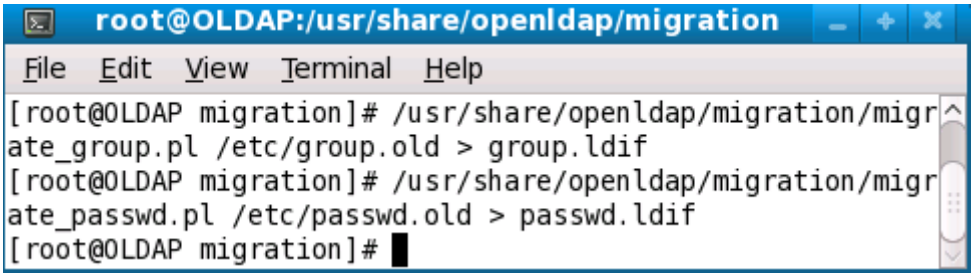
6. Definimos las bases (/etc/passwd) (/etc/group) hacia los archivos ldif

```
#/usr/share/openldap/migration/migrate_base.pl > base.ldif

#vi base.ldif
```

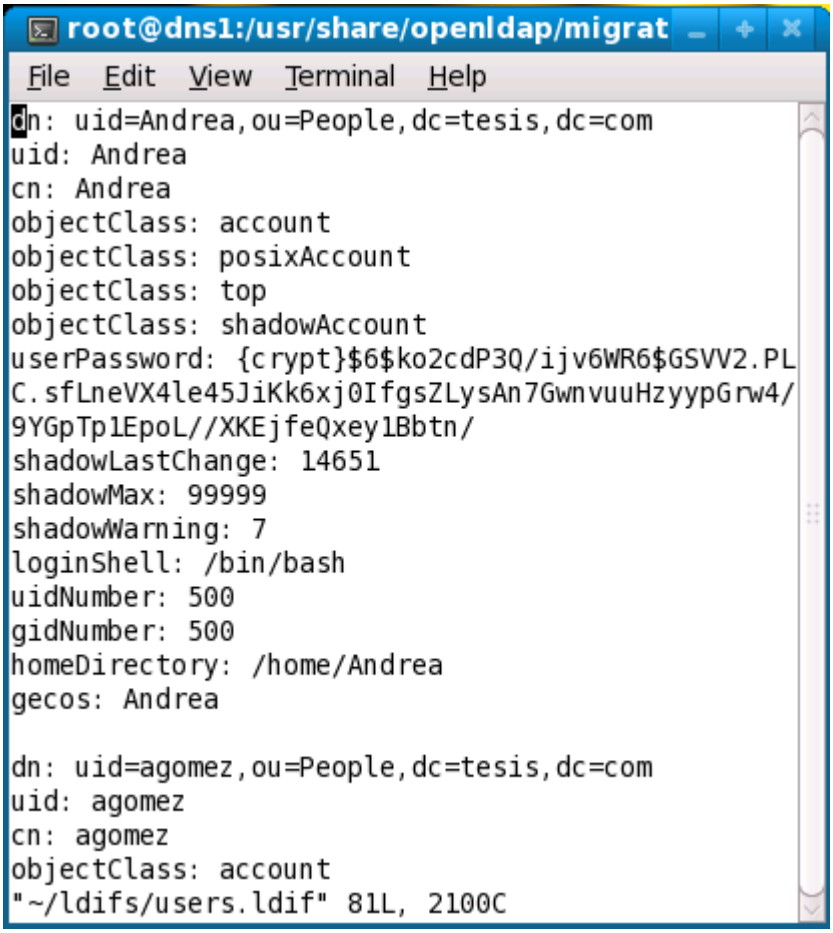



```
#/usr/share/openldap/migration/migrate_passwd.pl    /etc/passwd    >
passwd.ldif
```

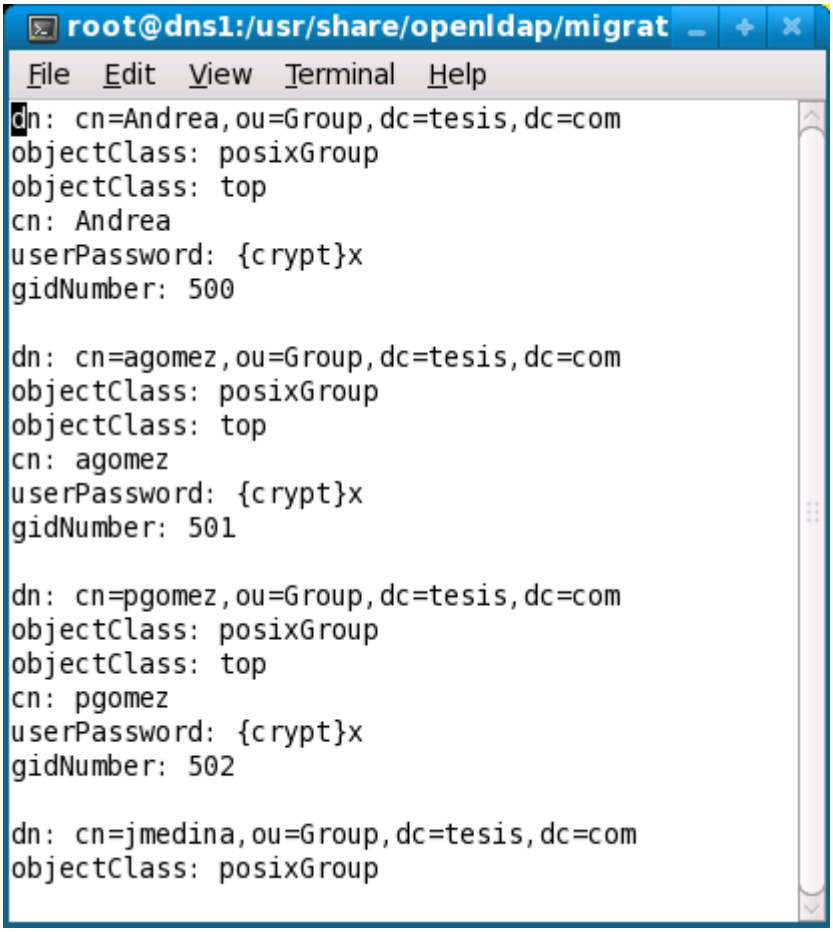
```
#/usr/share/openldap/migration/migrate_group.pl     /etc/group     >
group.ldif
```




```
#vi users.ldif
```

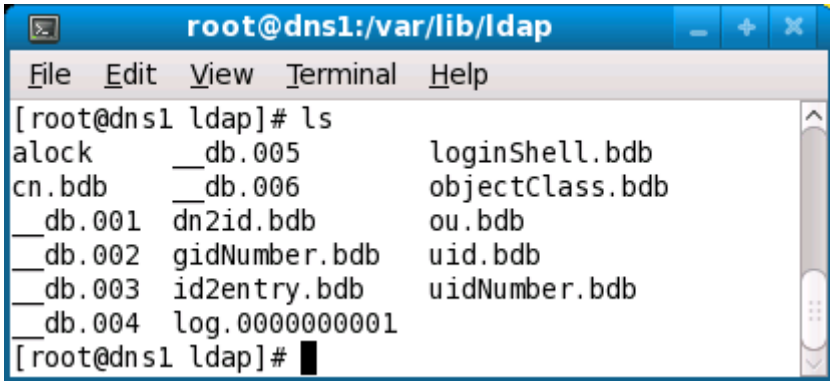



```
#vi grupos.ldif
```



7. Inicializamos el servicio y chequeamos los logs que se crearon

```
#service ldap restart

#chkconfig ldap on

#ls /var/lib/ldap
```



8. Insertar la información generada en los directorios que se creó anteriormente

Se utilizará **ldapadd** para insertar los datos necesarios. Las opciones utilizadas con este comando son las siguientes:

-x	autenticación simple
-W	solicitar clave de acceso
-D binddn	Nombre Distinguido (dn) a utilizar
-h	Servidor LDAP a acceder
-f	Fichero a utilizar

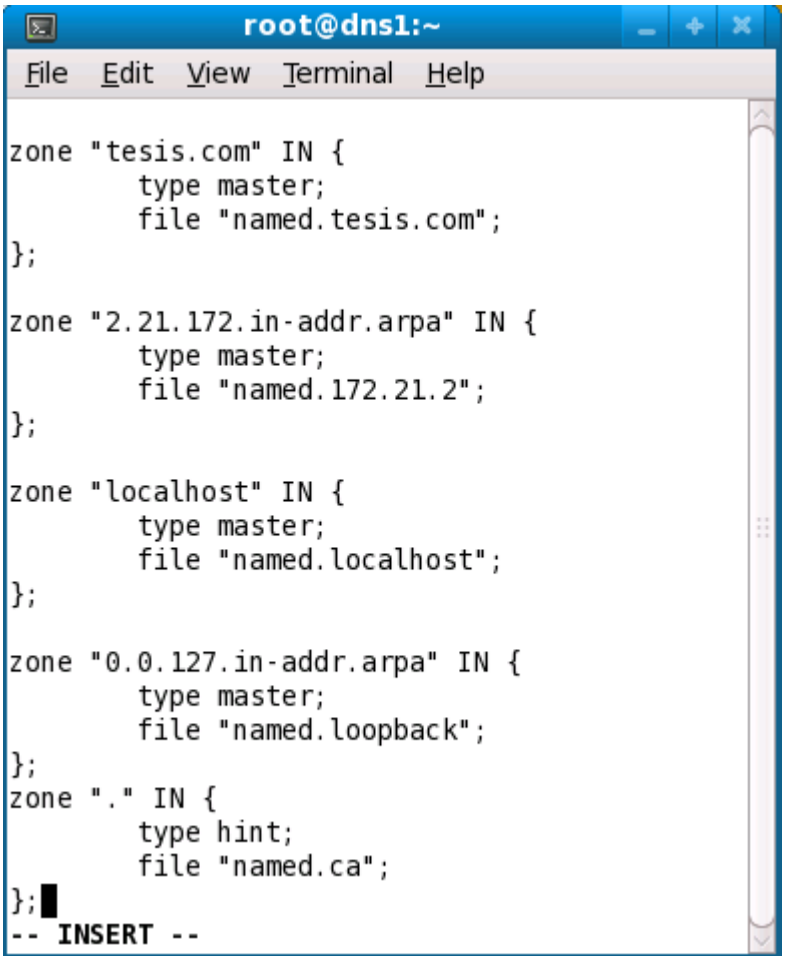
Una vez comprendido el comando aplicamos

```
#cd /usr/share/openldap/migration
#ldapadd -x -W -D 'cn=Manager, dc=tesis, dc=com' -h 127.0.0.1 -f base.ldif
#ldapadd -x -W -D 'cn=Manager, dc=tesis, dc=com' -h 127.0.0.1 -f users.ldif
#ldapadd -x -W -D 'cn=Manager, dc=tesis, dc=com' -h 127.0.0.1 -f grupos.ldif
```

Configuración del DNS server

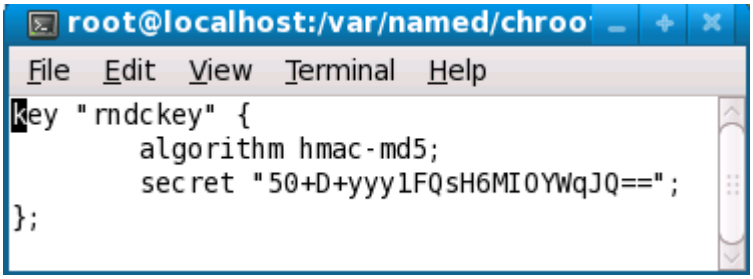
1. Crear la configuración del nombre del servidor

```
#vi /etc/named.conf
```

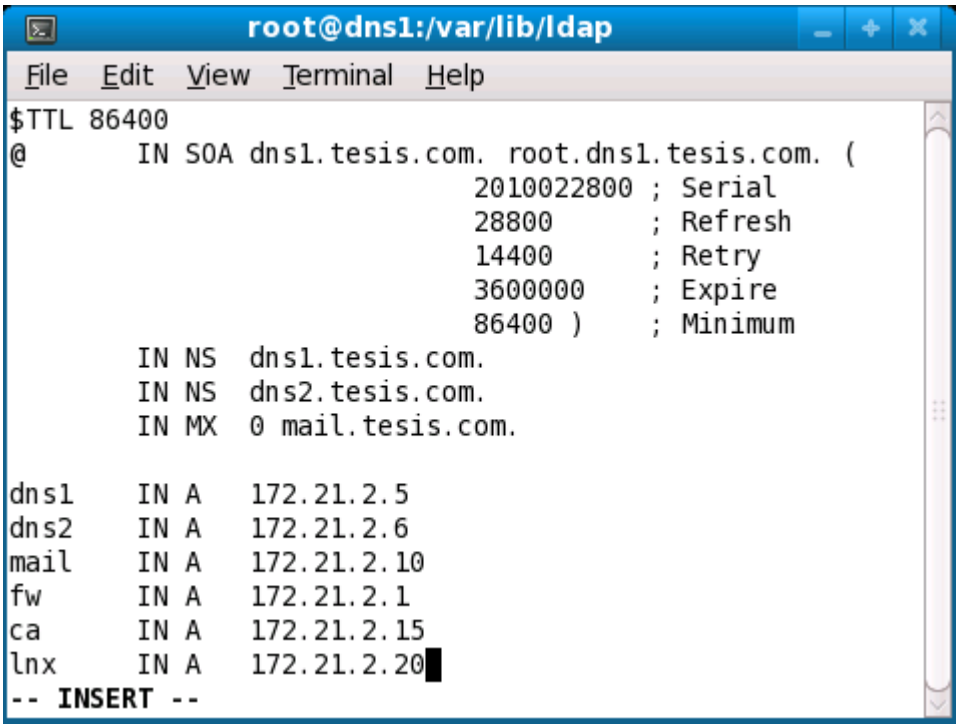


2. Observamos el archivo rndc.key, para comprobar la existencia de la clave, sino hay que crear una.

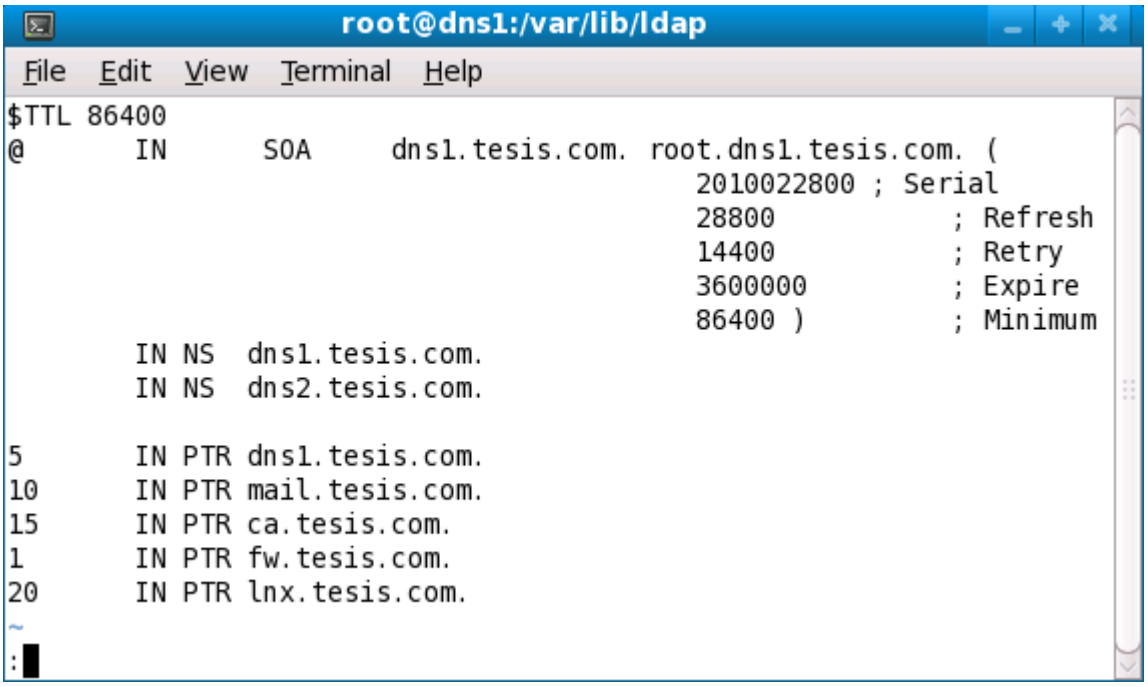
```
#view nrdc.key
```



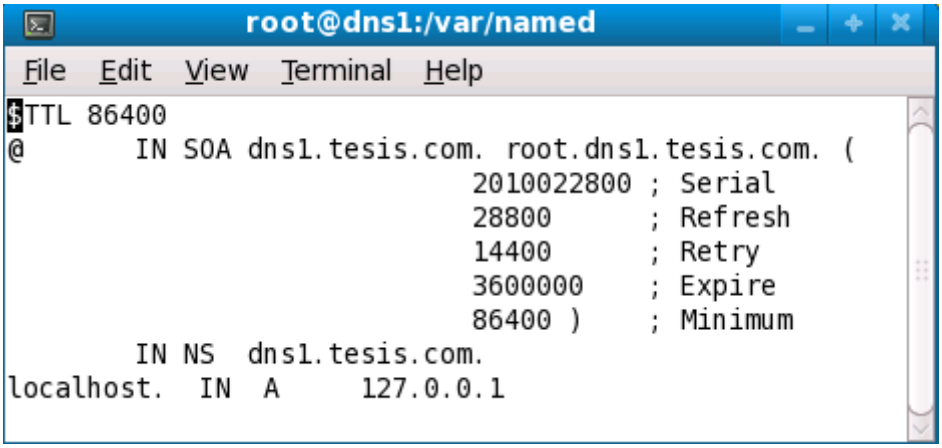
3. Creamos el archivo de zonas `#vi /var/named/named.tesis.com`



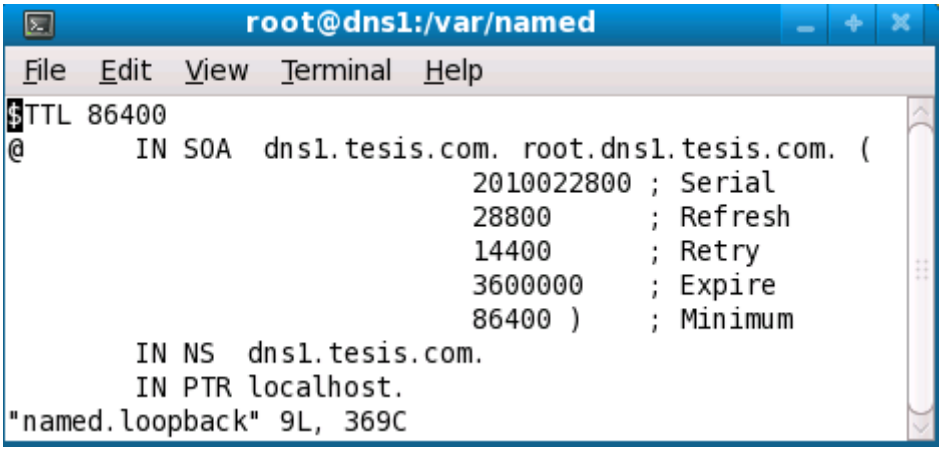
4. Creamos el archivo de zonas reversas `#vi /var/named/named.172.21.2`



5. Creamos el archivo de zonas locales `#vi /var/named/named.localhost`

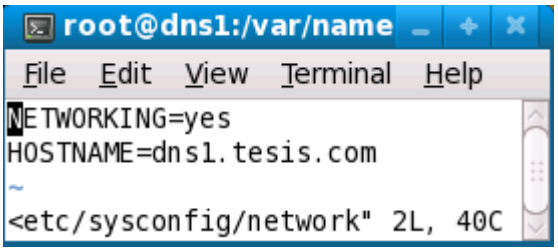


6. Creamos el archivo de zona reversa local `#vi /var/named/named.loopback`

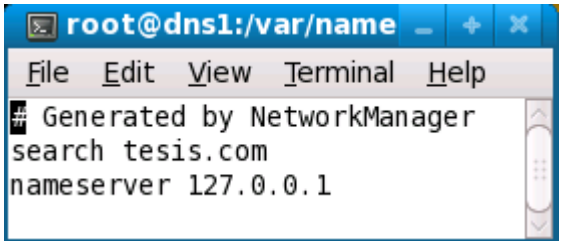


7. Asegurarnos que el dominio sea calificado, configurando el hostname

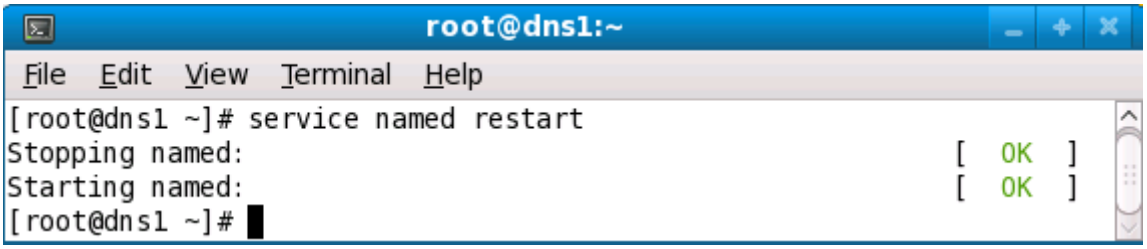
`#vi /etc/sysconfig/network`



8. Modificar el archivo `#vi /etc/resolv.conf` con `domain tesis.com`



9. Inicializar el servicio de DNS (named)



Pruebas

- Probar el funcionamiento del DNS y resolución de nombres internos como externos a la red.

  Para esto se utilizó el comando host y el nombre o la ip del servidor para verificar la resolución de los nombres tanto directo como reverso de la red.

- Autenticación al openldap y el dominio con el usuario creado.

  Para esto se utilizó la consola de gráfica de openldap en donde refleja el dominio creado y las unidades organizativas que pertenecen a esta infraestructura, se puede observar en la siguiente figura la consola de gráfica de openldap y las unidades organizativas creadas.

ANEXO 7

Proceso de implementación y pruebas de EXIM

Es necesario implementar el sistema de correo electrónico EXIM en una maquina que tenga debían ya que las características de este sistema operativo nos permite llevar a cabo una implementación más segura y completa según nuestras necesidades.

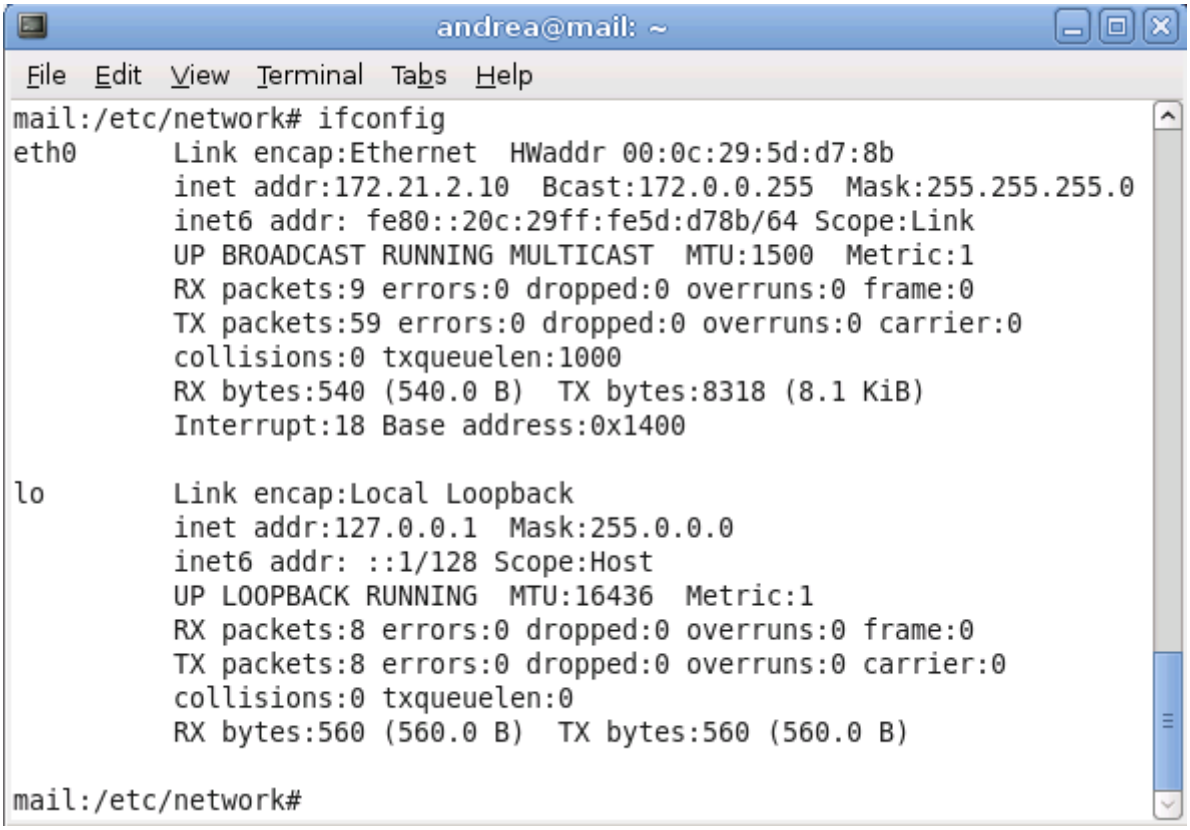
Configuración de EXIM

Revisamos la configuración de interface de red de nuestra maquina.

Dirección IP = 172.21.2.10

Mascara de red = 255.255.255.0

Gateway = 172.21.2.1



1. Instalación del paquete de exim4

```
#apt-get install exim4
```

2. Como ya está instalado hacemos la reconfiguración

```
#dpkg-reconfigure –plow exim4-config
```

- Configuramos el sitio de internet
- La configuración, es enviada y recibida usando SMTP
- Da el nombre completo del servidor inclusive el domini**o**
- Dejamos en blanco las direcciones IP que escuchan conexiones SMTP entrantes.
- Destino del dominio que recibe los mails.
- Verificación del DNS
- Mantenemos el número mínimo de queries del DNS
- Método de entrega para el correo local, escogemos el mbox.
- Y escogemos si, para que separe la configuración de archivos pequeños.

Podemos hacer la configuración manual en el archivo directamente.

#vi /etc/exim4/exim4.conf

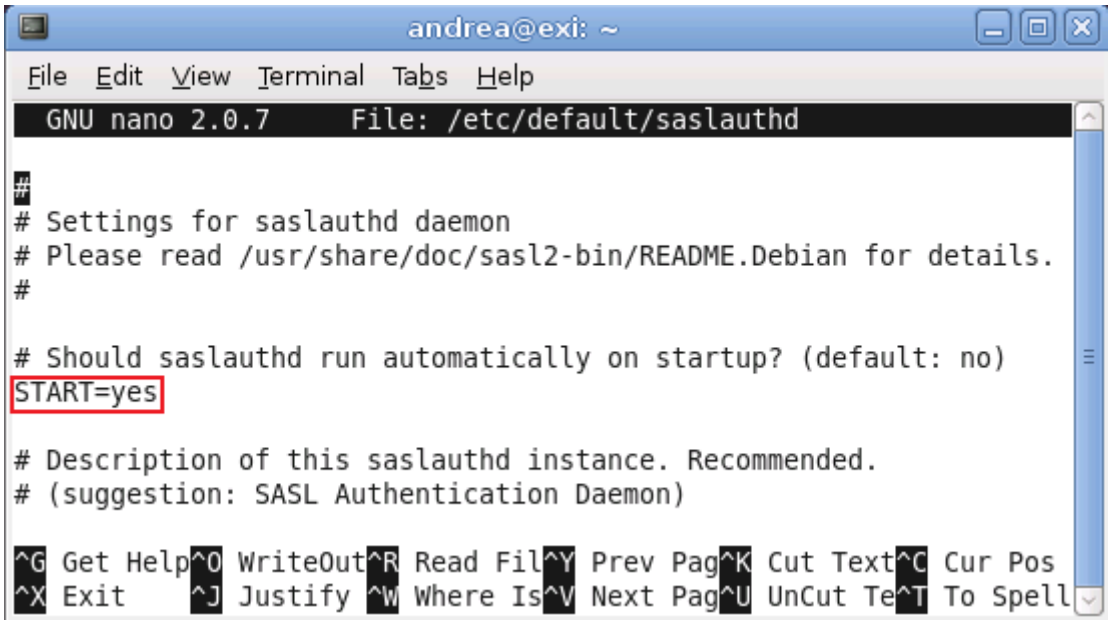
Autenticación SMTP con SASL

1. Instalamos los paquetes sasl2-bin y libsasl2-modules

```
#apt-get install sasl2-bin libsasl2-modules
```

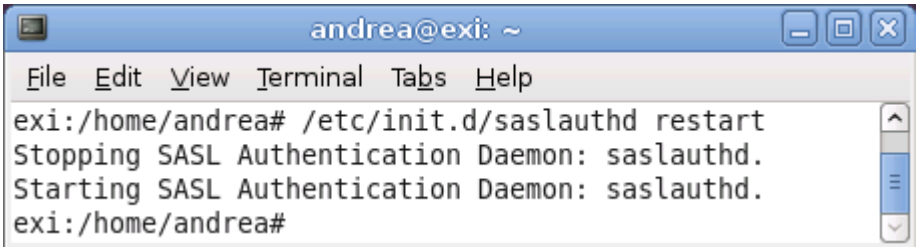
2. Editamos el archivo /etc/defaults/saslauthd y modificamos la variable a START

```
#nano /etc/defautls/saslauthd
START=yes
```



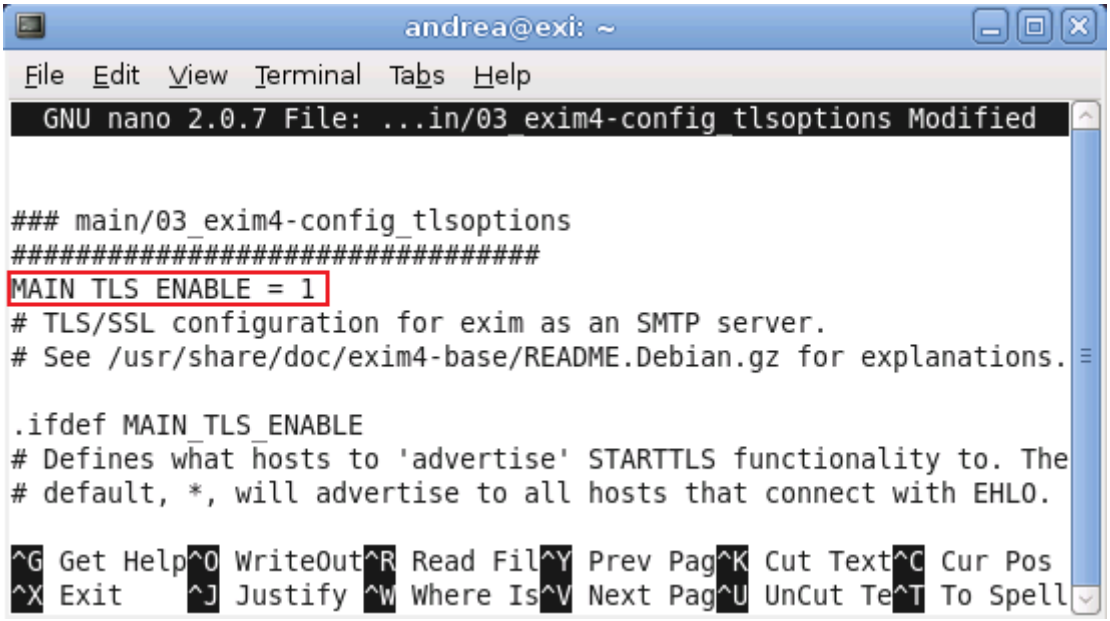
3. Reiniciamos el servidor SASL

```
#service saslauthd restart
```



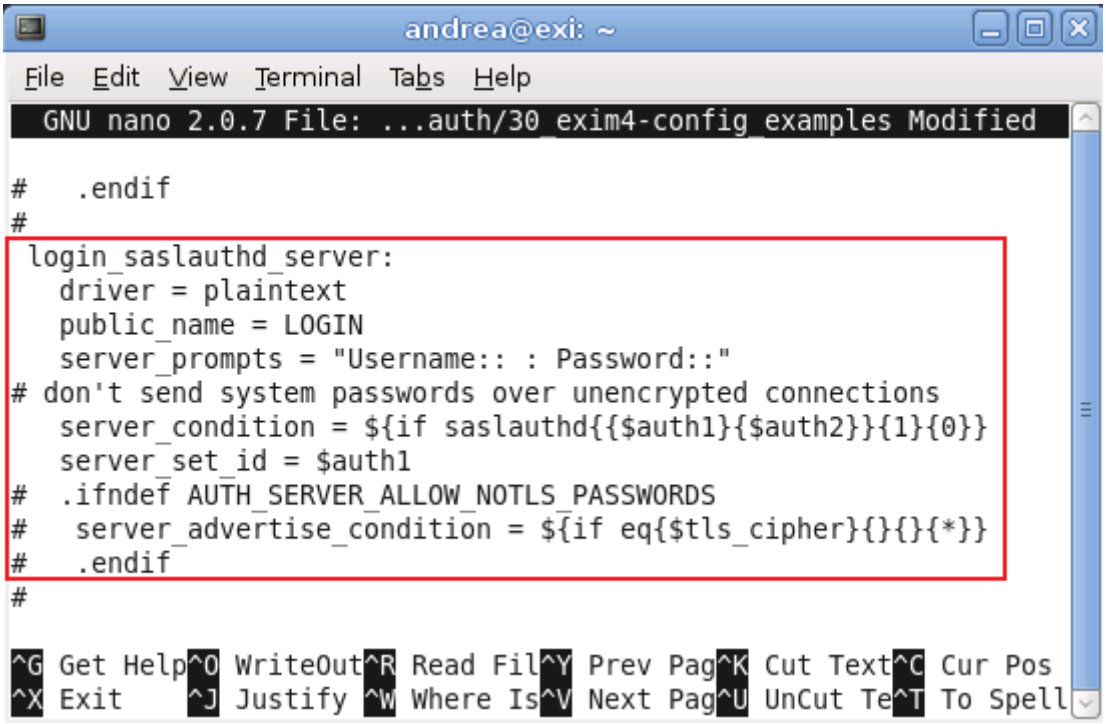
4. Editamos el archivo /etc/exim4/conf.d/main/03_exim4-config _tlsoptions agregamos al inicio del archivo.

```
MAIN_TLS_ENABLE = 1
```



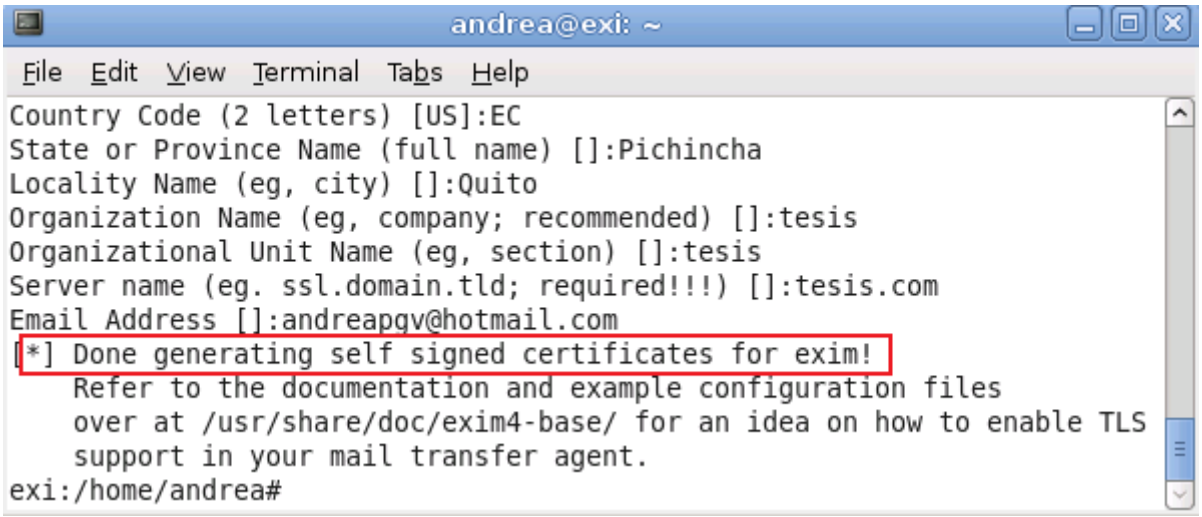
5. Editamos el archivo /etc/exim4/conf.d/auth/30_exim4-config_examples y des co-mentamos

```
Login_saslauthd_server:
```



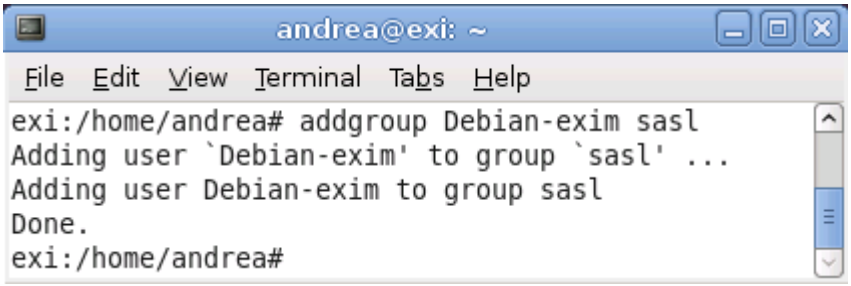
6. Generamos un certificado de seguridad

```
#/usr/share/doc/exim4-base/examples/exim-gencert
```



Los archivos exim.crt y exim.key son almacenados en /etc/exim4, validos por tres anos.

7. Agregamos exim al grupo de sasl



8. Actualizamos la configuración de exim

```
#update-exim4.conf
```

9. Reiniciamos el demonio de exim4

```
#/etc/init.d/exim4 restart
```

10. Probamos una conexión SMTP

- `telnet localhost 25`
- `EHLO exi.tesis.com.ec`

Configuración de CLAMAV

1. Instalamos el clamav, esto instalara también los paquetes adicionales que necesitaremos más adelante como, clamav-base, clamav-freshclam y libclamav1

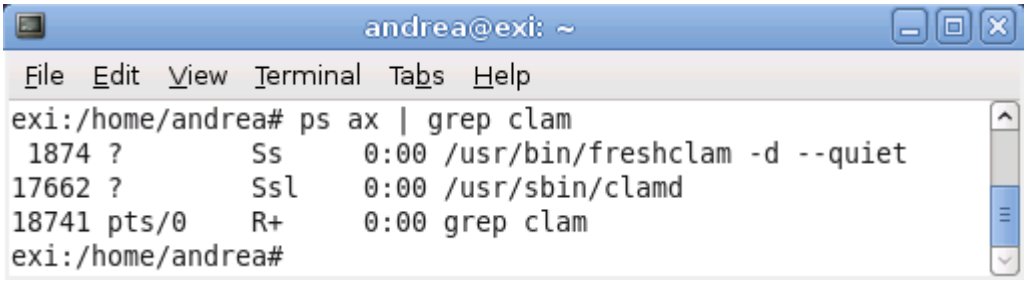
   ```
   #apt-get install clamav clamav-daemon freshclam
   ```

2. Instalamos también otros descompresores que suelen ser usados por algunos virus, si estos paquetes estan instalados, permitirá la detección inmediata por el antivirus clamav.

   ```
   #apt-get install arj zoo lzop
   ```

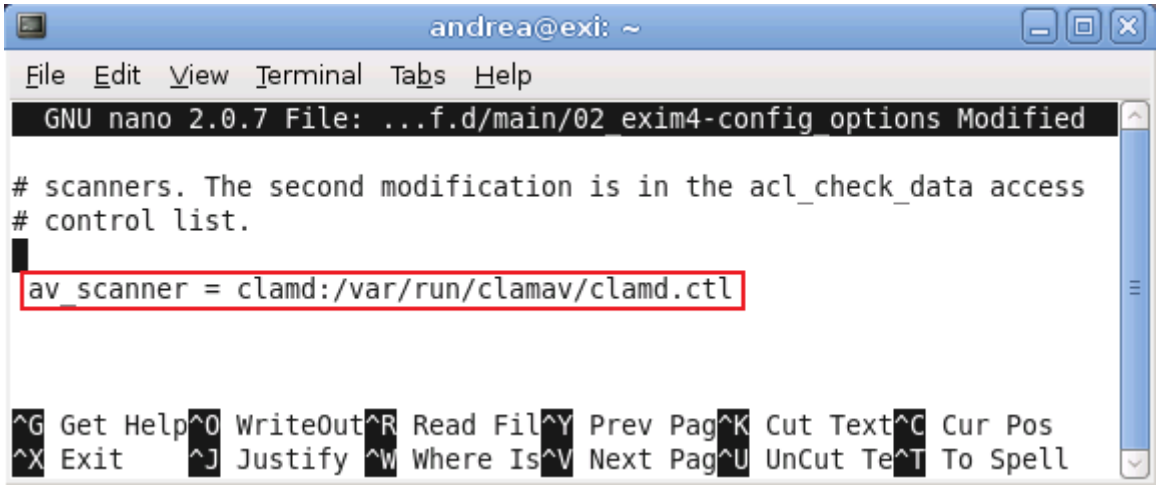
3. Nos aseguramos que los dos demonios más importantes de este antivirus estén funcionando, ya que clamav-daemon es el scanner y clamav-freshclam descarga la base de datos de los virus de Internet y la actualiza regularmente.

   ```
   #ps ax | grep clam
   ```

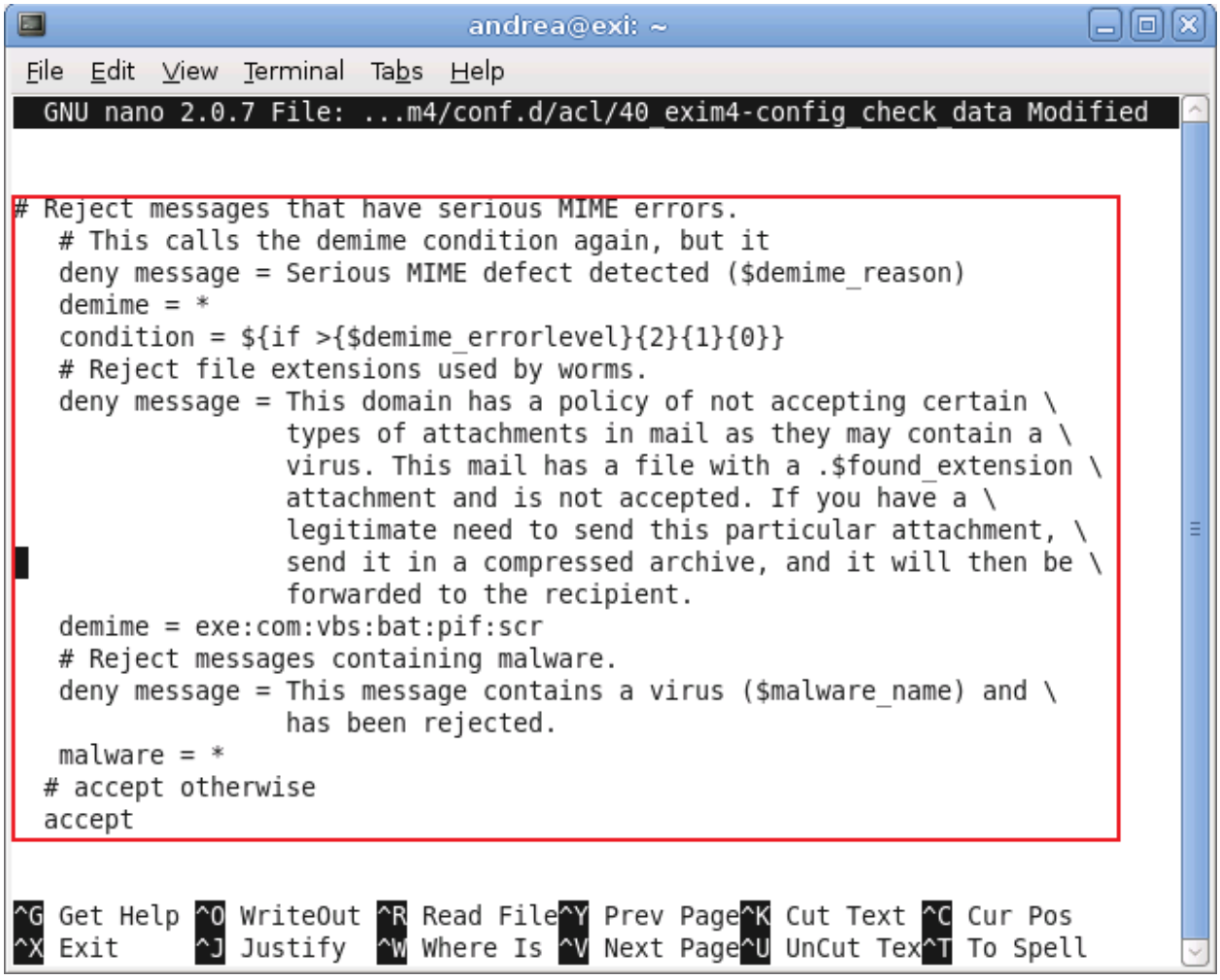


4. Editamos /etc/exim4/conf.d/main/02_exim4-config_options y modifica El instructivo av_scanner

   ```
   #av_scanner = clamd:/var/run/clamav/clamd.ctl
   ```



5. Editamos /etc/exim4/conf.d/acl/40_exim4-confg_check_data y agregamos al final antes de accept



6. Crear el directorio con atributos de escritura, lectura y ejecución.

```
#mkdir -p -m 777 /var/spool/exim4/scan
```

7. Agrega el usuario clamav al grupo de Debian-exim

```
#addgroup clamav Debian-exim
```

8. Actualizamos la configuración de exim

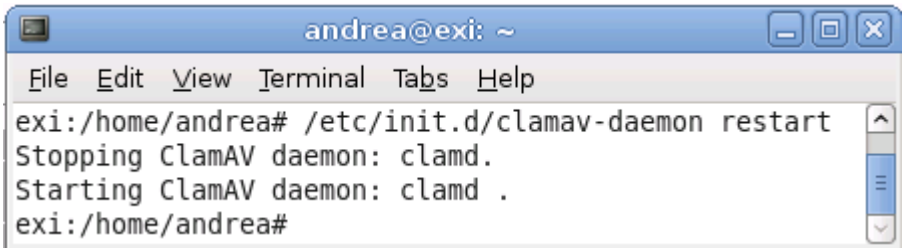
```
#update-exim4.conf
```

9. Reiniciamos exim

```
#/ect/init.d/exim4 restart
```

10. Reiniciamos Clamav-daemon

```
#/etc/init.d/clamav-daemon restart
```



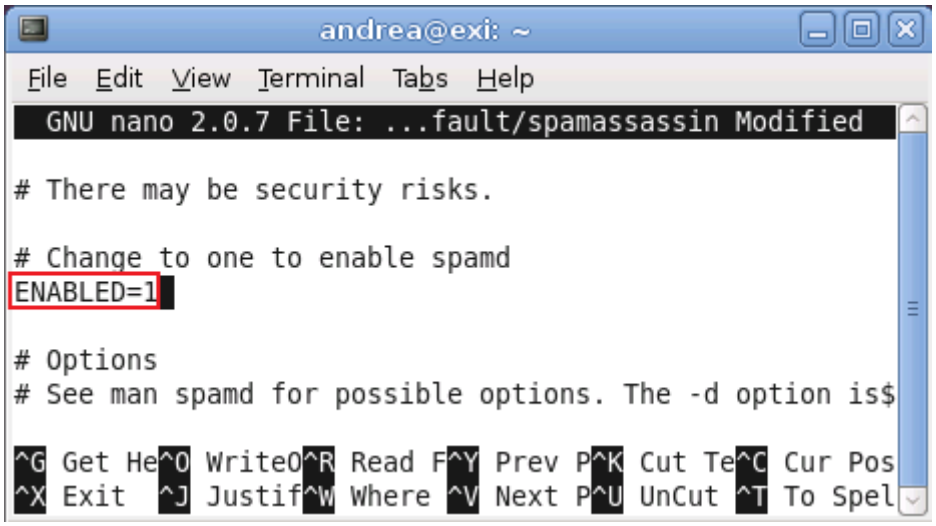
Configuración de Spamassassin

1. Instalamos spamassassin y spamc

```
#apt-get install spamassasin spamc
```

2. Editamos /etc/defaults/spamassassin modificamos enabled

```
ENABLED = 1
```



3. Inicializamos spamd

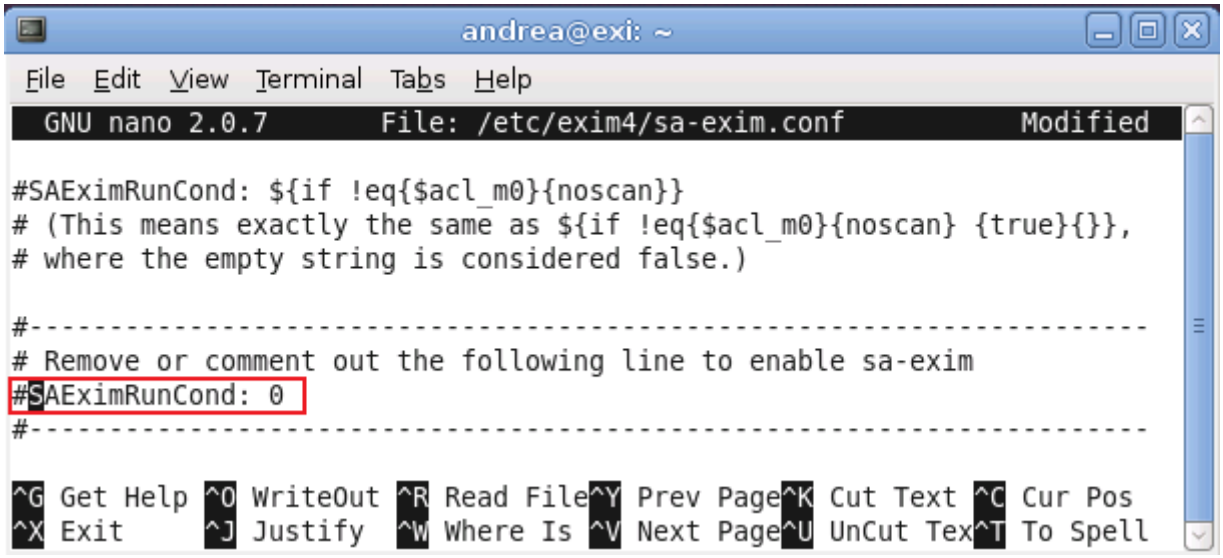
```
#/etc/init.d/spamassasin start
```

4. Instalamos el paquete sa-exim

```
#apt-get install sa-exim
```

5. Editamos /etc/exim4/sa-exim.conf y comentamos

```
#nano /etc/exim4/sa-exim.conf

#SAEximRunCond: 0
```



6. Actualizamos la configuracion de exim

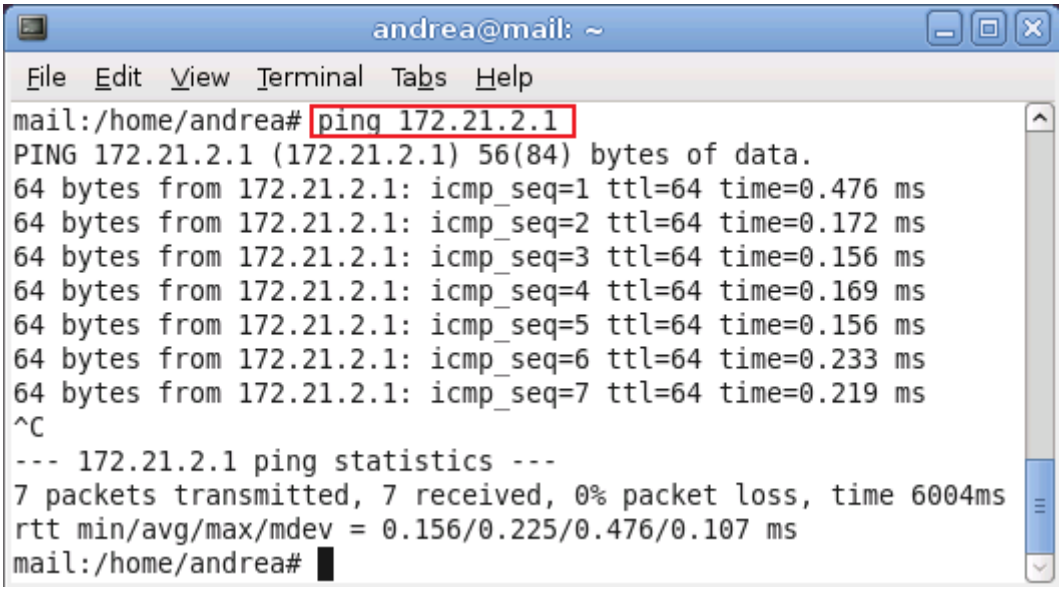
```
#update-exim4.conf
```

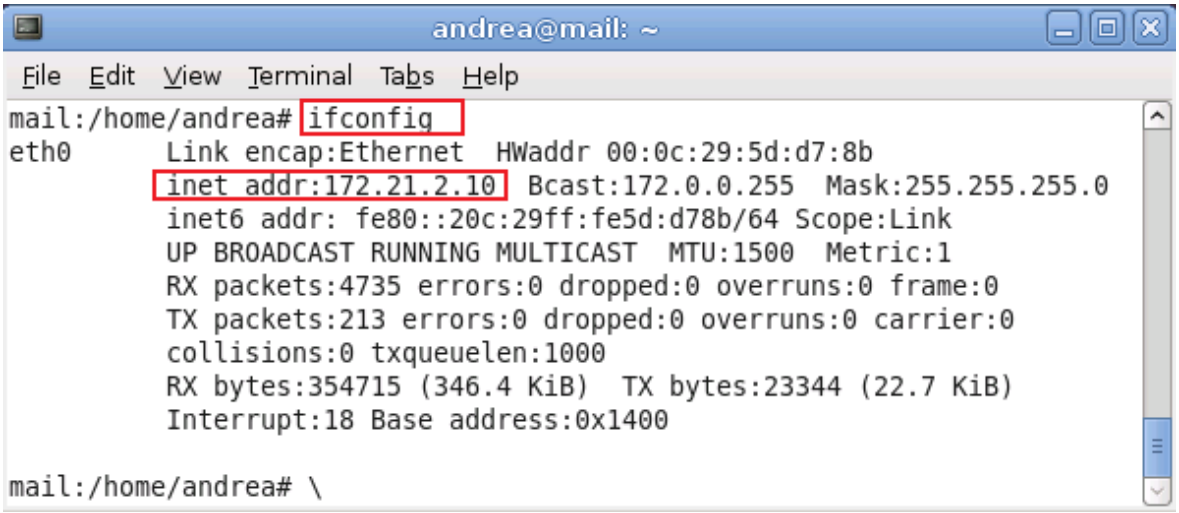
7. Reiniciamos exim

```
#/etc/init.d/exim4 restart
```

Pruebas

- Comprobar la configuración de red





- Probar SMTP para envió y recepción de mensajes.

  Para revisar el envío, recepción de mensajes y la cola que tiene el exim se puede revisar los log de exim4 y comprobar los envíos, usuarios y el estado de los correos. El comando que se utilizo fue tail –f /var/log/exim4/main.log

- Comprobar la aplicación de firmas digitales y certificados.

  Para esta prueba se puede verificar en cada uno de los usuarios de cada una de las infraestructuras las firmas y certificados que se envían cuando se realiza el envio o recepción de mensajes.

ANEXO 8

Proceso de implementación y pruebas de clientes Windows y Linux

Cliente Windows

Para poder hacer el registro de las computadoras dentro del dominio, debemos hacer que la maquina que quiere ingresar al Directorio sea parte del dominio de la siguiente manera.

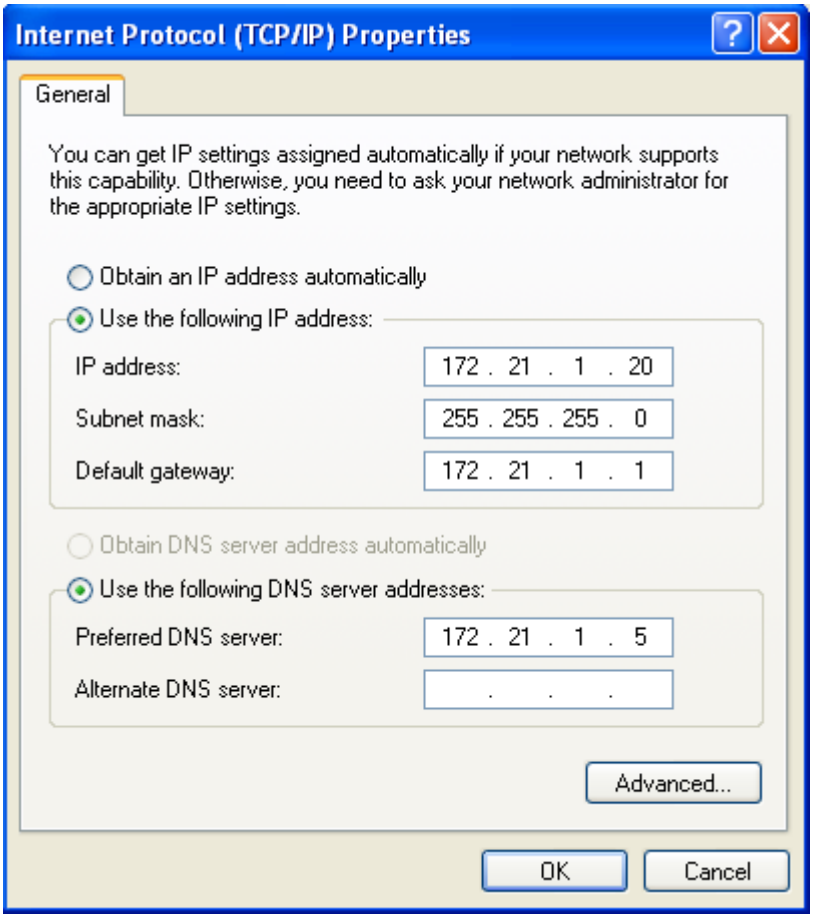
1. Configuración de TCP/IP para la maquina.

   Dirección IP: 172.21.1.20

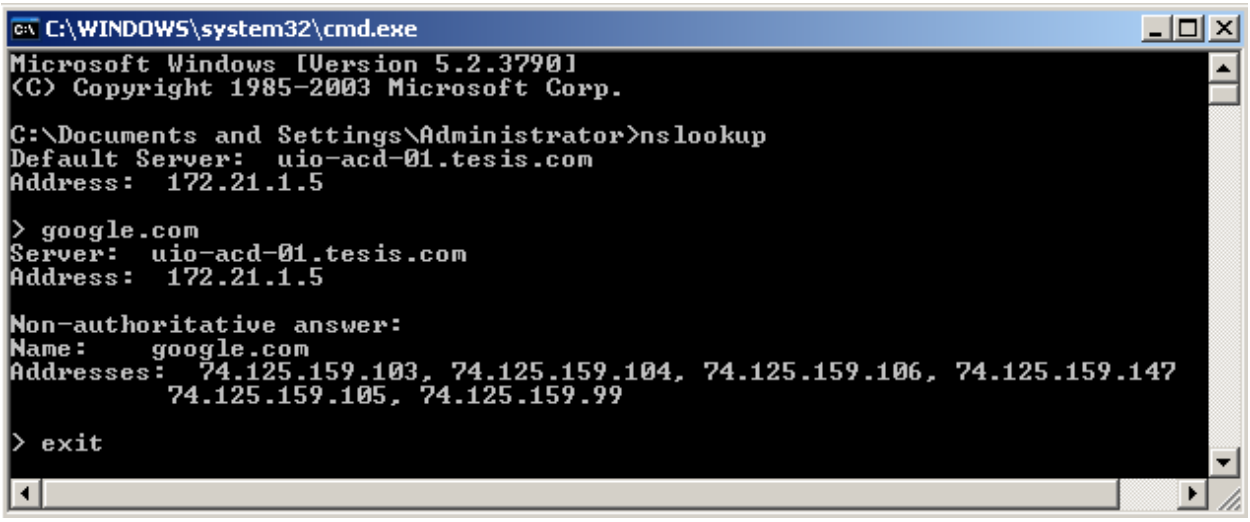
   Mascara de subred: 255.255.255.0

   Gateway: 172.21.1.1

   DNS server: 172.21.1.5

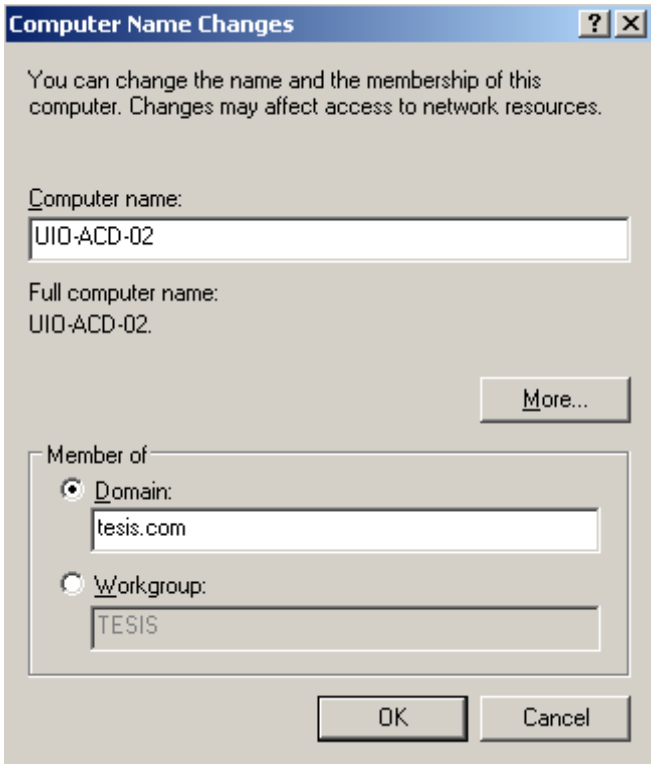


2. Comprobamos si está resolviendo con *nslookup* podemos observar que está resolviendo cuando devuelve el nombre del ordenador del Directorio Activo.



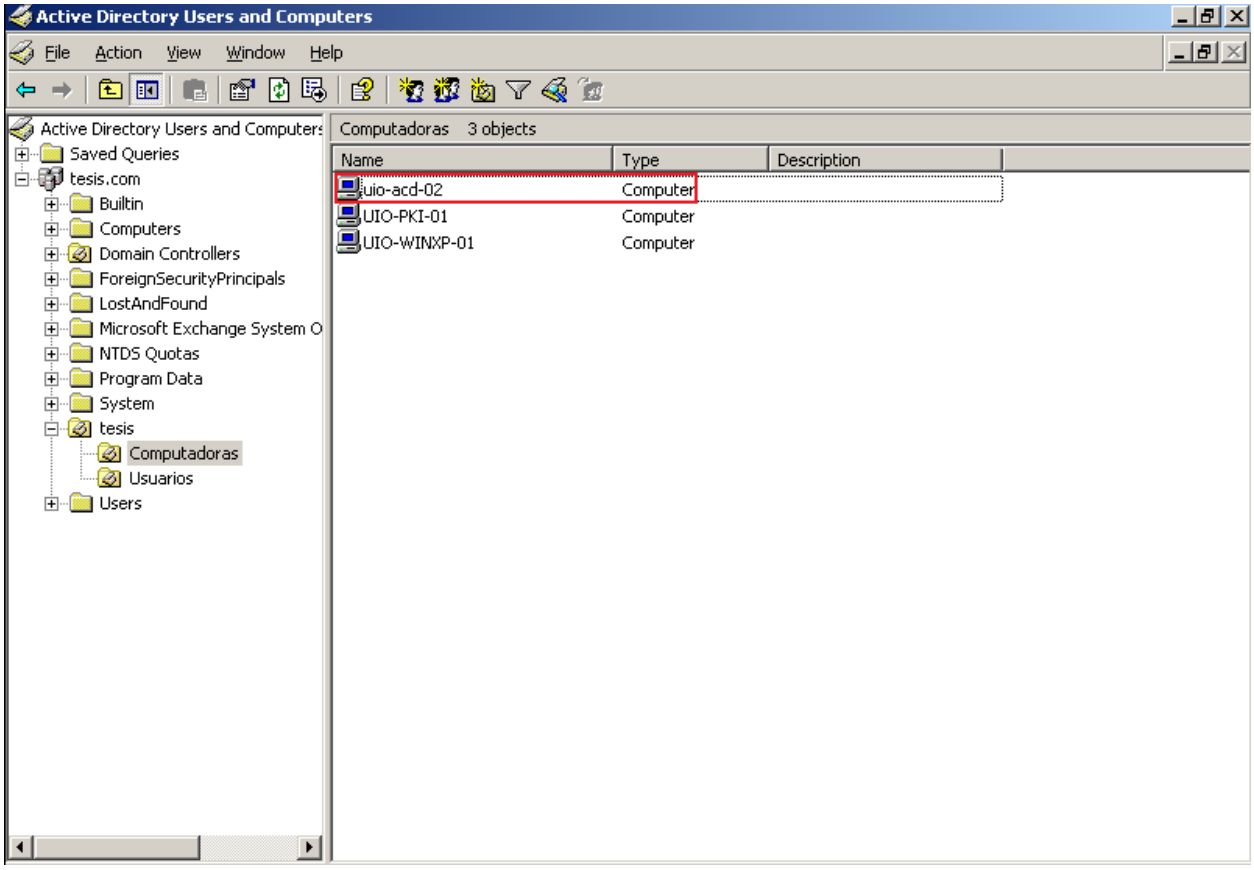
3. Para que la maquina sea parte del dominio, vamos a My Computer, hacemos click derecho en properties y en la pestaña de Computer Name

   Vemos el nombre de la maquina y hacemos click en Domain, colocamos el nombre de nuestro dominio.



4. Si no sale esta pantalla de autenticación, puede ser que tengamos problemas con la resolución de DNS o no este hecha bien la configuración.

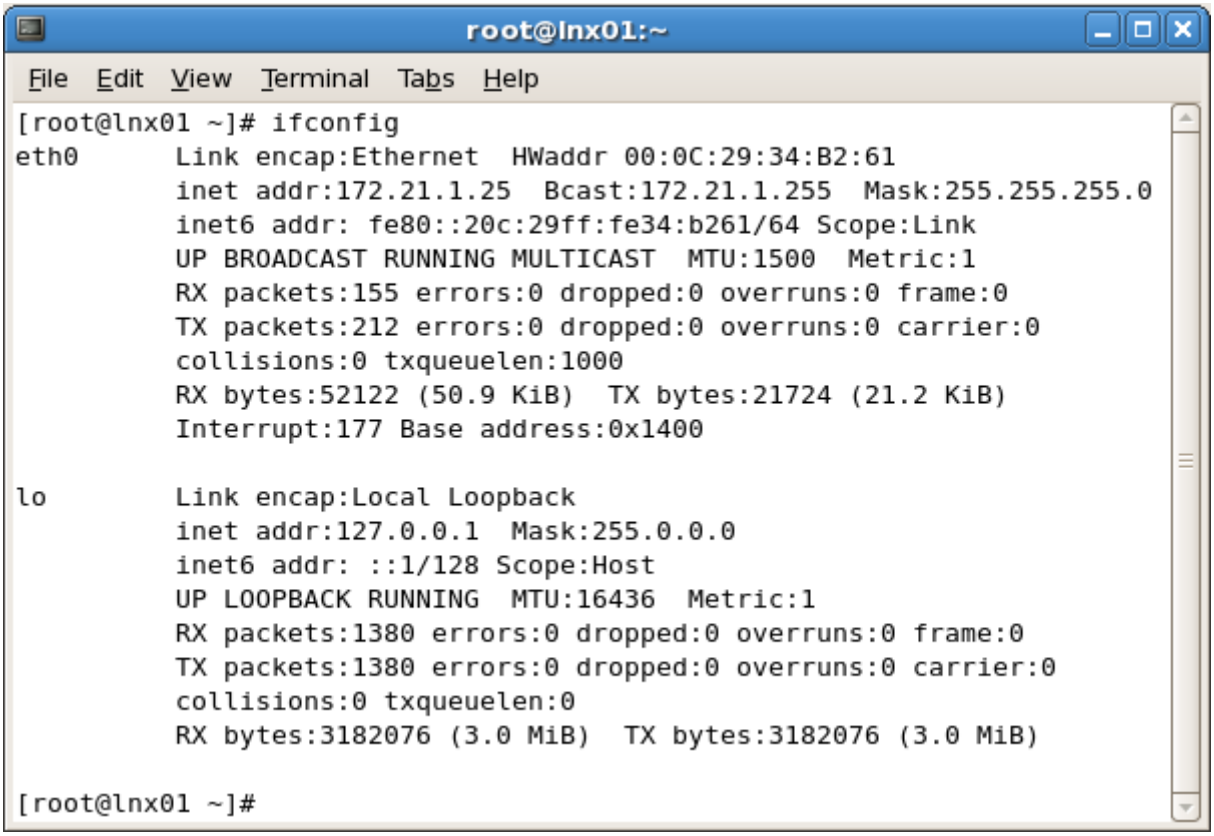
5. Después se autentica al directorio Activo y podemos ver en el directorio como fue agregada esta computadora



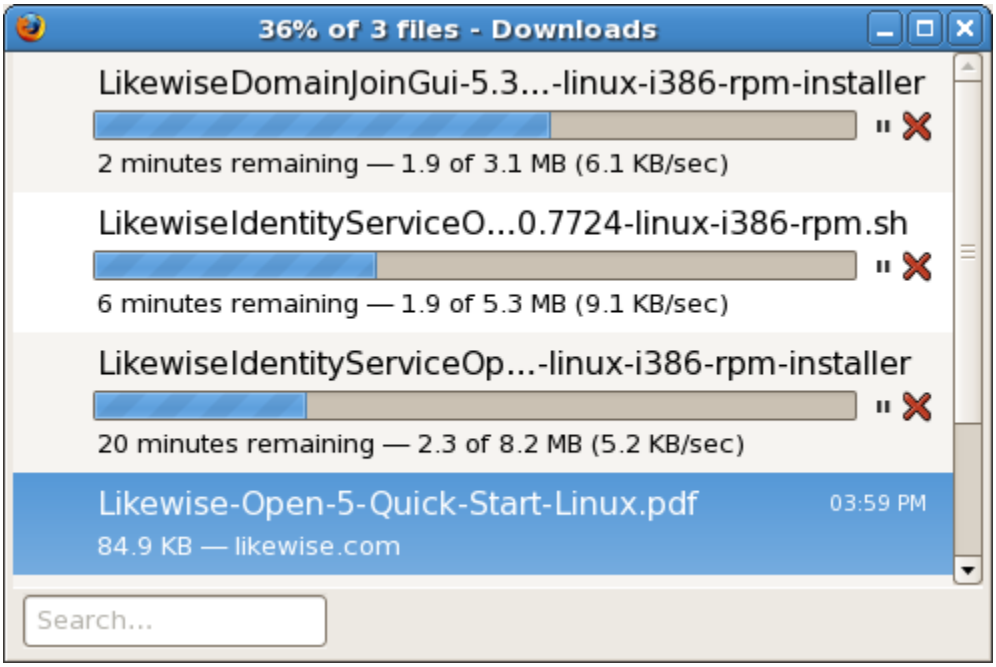
6. El usuario y la maquina que hemos creado nos sirve para autenticarnos al directorio Activo y poder tener acceso a los recursos de la red.

Cliente Linux

1. Configuracion de red

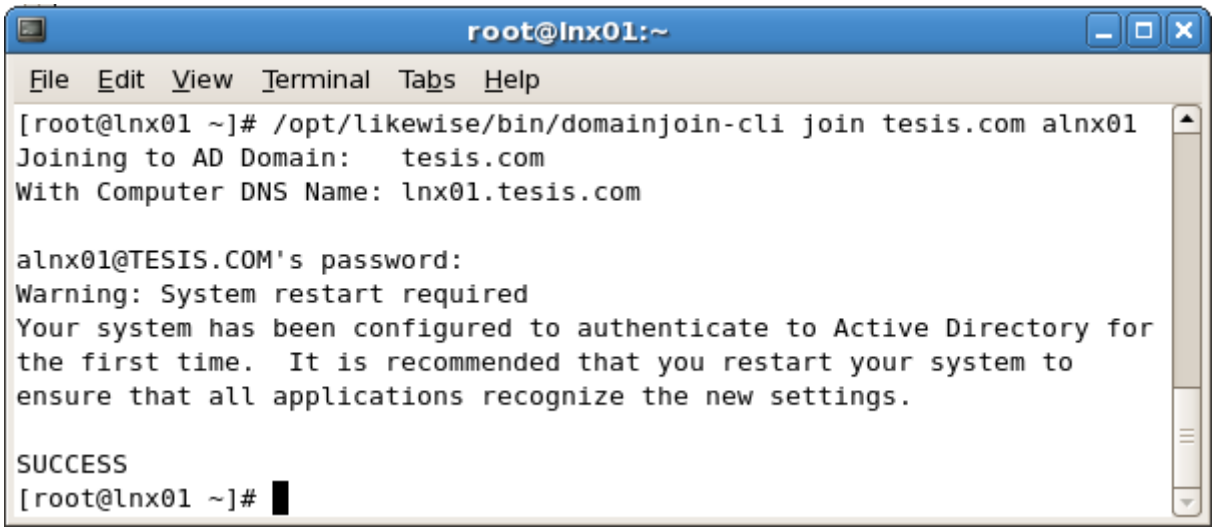


2. Integracion de usuario linux con el directorio activo, descarga de los archivos necesarios para la integracion de usuarios linux



3. Despues de instalar los paquetes, nos integramos al directorio activo con el siguiente comando.

```
#/opt/likewise/bin/domainjoin-cli join tesis.com alnx01
```



4. Reiniciamos el ordenador e ingresamos con el nombre del usuario que creamos


alnx 01
TESIS\alnx01 on lnx01
Password:
Cancel
Unlock