UNIVERSIDAD NACIONAL
"PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS

ESCUELA PROFESIONAL DE INGENIERIA ELECTRONICA

TESIS

"REDISEÑO DE LA RED DE COMUNICACIONES Y SEGURIDAD INFORMÁTICA A TRAVÉS DE ENTORNOS CENTRALIZADOS ADMINISTRABLES BASADOS EN SOFTWARE LIBRE"

PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO ELECTRONICO

AUTOR:
Bach. JORGE RAÚL PISCOYA CALDERÓN

LAMBAYEQUE – PERÚ
2015

UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE INGENIERIA ELECTRONICA

Los firmantes, por la presente certifican que han leído y recomiendan a la Facultad de Ciencias Físicas y Matemáticas la aceptación de la tesis titulada "Rediseño de la red de comunicaciones y seguridad informática a través de entornos centralizados administrables basados en software libre", presentada por el Bachiller en Ingeniería Electrónica, Jorge Raúl Piscoya Calderón, en cumplimiento parcial de los requisitos necesarios para la obtención del Título Profesional de Ingeniero Electrónico.

Ing. Manuel Javier Ramirez Castro
Presidente de Jurado de Tesis

Ing. Francisco Segura Altamirano
Secretario de Jurado de Tesis

Ing. Hugo Javier Chiclayo Padilla
Vocal de Jurado de Tesis

UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE INGENIERIA ELECTRONICA

"Rediseño de la red de comunicaciones y seguridad informática a través de entornos centralizados administrables basados en software libre"

Bach. Ing. Jorge Raúl Piscoya Calderón
Autor

Ing. Carlos Oblitas Vera
Asesor

Lambayeque – Peru
Marzo - 2015

AGRADECIMIENTO

EN PRIMER LUGAR A DIOS QUE ME HA DADO TODO.

A MI MADRE CLORINDA CALDERON CARLOS POR SU CONSTANTE EMPUJE Y APOYO MORAL EN LA REALIZACIÓN DE ESTE PROYECTO.

A MI PADRE JORGE PISCOYA FERNANDEZ POR EL INFINITO SACRIFICIO DE BRINDARME EDUCACION.

A MI ESPOSA E HIJO POR MIS HORAS DE AUSENCIA EMPLEADOS EN LA REALIZACIÓN DE ESTE TRABAJO.

DEDICATORIA

CON MUCHO CARIÑO A LA MEMORIA DE MIS ABUELOS JUAN MANUEL PISCOYA SONO Y LUCÍA FERNÁNDEZ CHANAMÉ, POR BRINDARME EN VIDA TANTO AMOR Y APOYO .

RESUMEN

La presente tesis tiene por objeto el Rediseño de la red de comunicaciones y seguridad informática a través de entornos centralizados administrables basados en software libre de la empresa Netkrom SAC. Esta investigación se justifica porque va a permitir a la compañía tener control total sobre los servidores necesarios para su funcionamiento tecnológico. Los servicios de correo, página web y telefonía son administrados por terceras compañías, lo que genera deficiencia en su control. Con el rediseño del cableado estructurado, se pretende mejorar la funcionalidad interna de la red con la finalidad de optimizar tiempos de acceso a información compartida, Los principales servicios como son DHCP, DNS y proxy son manejados por equipos de baja potencia lógica por lo que al cambiarse a servidores dedicados, aumenta el rendimiento de los mismos y permite ser administrado con mucha mayor facilidad. El servicio apache permite tener control total sobre la web corporativa para poder realizar los cambios en caliente de su diseño ya que es una ventana abierta hacia potenciales clientes que necesiten realizar consultas al catálogo de productos y servicios. El servicio de correo permite desligarse de cuotas limitadas de espacio por los operadores externos, así como el número de altas nuevas de usuarios, ya que estos requerimientos tienen costes elevados. Todos los servicios tienen costo cero por licencias operativas, lo que es atractivo para la reducción de costos operativos.

ABSTRACT

This thesis aims to redesign the communication network and computer security through centralized manageable based on free enterprise software Netkrom SAC environments. This research is justified because it will allow the company to take full control over the servers needed for technological operation. Mail services, website and phone are managed by another company, generating deficiency in their control. With the redesign of structured cabling, is to improve internal network functionality in order to optimize time access to shared information, Main services such as DHCP, DNS and proxy are are handled by teams logic low power so to switch to dedicated servers, increases yield and allows the same to be managed far more easily. The apache service allows full control over the corporate website to make changes in design hot as it is a window into potential customers who need to query the catalog of products and services. Mail service allows limited quotas separated from space by the external operators, as well as the high number of new users, since these requirements have high costs. All services have zero cost for operating licenses, which is attractive for reducing operating costs.

INTRODUCCIÓN

En los últimos años la tendencia tecnológica ha conllevado a que el responsable de administrar los servicios informáticos se encuentre en constante capacitación para reforzar lo aprendido durante los años de estudios universitarios. La tecnología ha hecho posible que se pueda administrar grandes redes con la combinación de diversos equipos de diversas marcas tanto así que en este proyecto se ha trabajado con tecnología híbrida, teniendo una estación centralizada con sistemas operativos GNU/Linux; equipos HP Pro Curve encargados de la conectividad de la red de la empresa, equipos de radio Motorola para la interoperatividad inalámbrica de exteriores, dispositivos de comunicaciones propietarios como Cisco Microsystems, etc.

La telefonía IP es una tecnología que ha venido escalando con fuerza en los últimos años, gracias a la empresa Digium que ha puesto al alcance de todos el software que hace posible que se pueda construir una central telefónica usando un servidor. Esto a permitido mejorar el performance de las comunicaciones ya que emplean el mismo canal y equipo físico que es usado para la conectividad de los datos, es decir la infraestructura Internet. Esto genera una reducción de costos al momento de la implementación, lo que conlleva a ahorros significativos en cuanto a economía se trata. Las comunicaciones de audio y video por IP generan a la vez ahorro en el mantenimiento y la puesta en producción.

Hablar de servidores, es hablar de la implementación de tecnologías que cumplan funciones como hosting, correos, fileservers, impresión, antivirus, etc; por lo que la mejor elección en cuanto a costos y aspectos técnicos y de seguridad a llevado a elegir sistemas operativos GNU/Linux para su puesta en producción, ya que éstas no generan costos de licenciamiento y por lo tanto generan un ahorro que es lo que toda empresa al fin y al cabo desea.

En este trabajo se explota profundamente los conocimientos de redes, Networking, y administración de seguridad informática.

Índice

CAPITULO I: Marco Metodológico

1. SITUACION PROBLEMATICA.

1.1. ANTECEDENTES.

Netkrom Technologies SAC es una empresa dedicada al rubro de las Telecomunicaciones, conectividad y Networking, realizando estudios y ejecutando proyectos en el ámbito de la interoperatividad inalámbrica.

Diseñan y ponen en producción sus propios equipos de transmisión y enlace con un mercado no sólo en Perú, también en Colombia y Miami.

Actualmente la tendencia de **Netkrom Technologies SAC** ha sido enfocada a los servicios de Seguridad Ciudadana basados en estándares inalámbricos de ondas de radio y enlaces punto a punto. Esto debido a que la tecnología está basada en cámaras IP de interiores y exteriores monitoreadas en una estación central.

La empresa ha venido presentando un crecimiento acelerado y ha sabido enfocar que el mercado de la seguridad ciudadana es un tema que repercute en la sociedad y por tanto a empezado a obtener diversos contratos a través de Concursos Públicos la Buena Pro para poder ejecutar proyectos con entidades tales como la Municipalidad de San Isidro, Surquillo, Miraflores, San Miguel, San Borja, Breña, y en provincias en Trujillo, Cajamarca, Cuzco y Arequipa.

Este crecimiento no ha ido de la mano con la infraestructura informática con la que cuentan sus instalaciones, ya que el número de personal también a crecido de manera rápida, pasando de 20 personas que inicialmente trabajaban a 100 personas

actualmente, lo que ha originado que la antigua infraestructura prácticamente se vea limitada hasta el punto de convertirse en un cuello de botella y por consecuencia en retraso para la adecuada atención a los potenciales clientes.

Por tanto las comunicaciones digitales es un tema crítico para garantizar la interoperatividad en la empresa, pero actualmente cuenta con servicios muy limitados en cuestión de infraestructura lógica. Se cuenta con una línea Speedy ADSL que brinda Internet a toda la sede central, cuenta con switch's de diferente marca y diferente tecnología de velocidades, cuenta con un servidor de archivos sobre CentOS 64 bits. que se encuentra instalado en un servidor PowerEdge 3200. También cuenta con otro servidor físico IMB X3500 donde tiene instalado un servidor de aplicaciones y sesiones remotas sobre Windows Server 2008 32 bits.

Cada computadora del personal viene con Windows 7 Professional original y con el paquete de Microsoft Office 2007 Professional original.

El servicio de ADSL lo brinda la empresa Telefónica del Perú S.A.

Tiene hosting de correo y web que es el único medio por el que se comunican las diferentes sedes.

Posee una central telefónica que tiene servicio con Americatel cuya marca es Panasonic modelo KX-TDA100 con un número limitado de anexos.

De la exposición anterior se puede sacar el siguiente resumen:

Se cuenta con 01 sistema Operativo CentOS.

Se cuenta con 01 Sistema Operativo Microsoft Windows Server 2008 que no están licenciados porque no son originales.

Se cuenta con un servidor de antivirus Kaspersky 6 que no está licenciado porque no es original.

Se cuenta con 100 licencias originales de Microsoft Windows 7.

Se cuenta con 100 licencias originales de Microsoft Office 2007.

No se cuenta con licencias para las conexiones remotas al servidor de aplicaciones.

Se cuenta con línea de Internet ADSL para las comunicaciones con el mundo exterior.

No se tiene una línea dedicada que pueda facilitar conexiones remotas entre las diferentes sedes.

No se tiene una IP pública fija para poder publicar diferentes servicios como el correo, la pagina web, base de datos.

La línea ADSL resulta muy limitada para el número de equipos y servicios que maneja la empresa.

Los gastos de licencia resultan muy elevados.

INDECOPI ha presentado un documento en el que subraya la utilización de licencias y sistemas operativos originales sino podrían tener problemas legales, por lo que la empresa ha optado por comprar máquinas con licencias de Windows y Office originales con el precio sobre-valorado.

No se tiene soporte técnico de los principales servidores ya que no son originales resultando esto un problema debido a que los sistemas operativos Windows necesitan constante actualización por los numerosos errores y fallas de seguridad presentes. Además de ser muy vulnerable al tema de virus

1.2. BASE TEORICA

En los últimos años la tendencia tecnológica ha conllevado a que el responsable de administrar los servicios informáticos se encuentre en constante capacitación para reforzar lo aprendido durante los años de estudios universitarios. La tecnología ha hecho posible que se pueda administrar grandes redes con la combinación de diversos equipos de diversas marcas tanto así que en este proyecto se ha trabajado con tecnología híbrida, teniendo una estación centralizada con sistemas operativos GNU/Linux; equipos HP Pro Curve encargados de la conectividad de la red de la empresa, equipos de radio Motorola para la interoperatividad inalámbrica de exteriores, dispositivos de comunicaciones propietarios como Cisco Microsystems.

La telefonía IP es una tecnología que ha venido escalando con fuerza en los últimos años, gracias a la empresa Digium que ha puesto al alcance de todos el software que hace posible que se pueda construir una central telefónica usando una computadora personal. Esto a permitido mejorar el performance de las comunicaciones ya que emplean el mismo canal y equipo físico que es usado para la conectividad de los datos, es decir la infraestructura Internet. Esto genera una reducción de costos al momento de la implementación, lo que conlleva a ahorros significativos en cuanto a economía se trata. Las comunicaciones de audio y video por IP generan a la vez ahorro en el mantenimiento y la puesta en producción.

Hablar de servidores, es hablar de la implementación de tecnologías que cumplan funciones como hosting, correos, fileservers, impresión, antivirus, etc; por lo que la mejor elección en cuanto a costos y aspectos técnicos y de seguridad a llevado a elegir sistemas operativos GNU/Linux para su puesta en producción, ya que éstas no generan costos de licenciamiento y por lo tanto generan un ahorro que es lo que toda empresa al fin y al cabo desea.

En este trabajo se explota profundamente los conocimientos de redes, Networking, análisis de presupuestos y administración de seguridad informática.

1.3. PROBLEMA

¿Cómo Re-diseñar la Red de Comunicaciones y Seguridad Informática a través de entornos centralizados administrables basados en software libre en la empresa **Netkrom Technologies SAC.**?

1.4. HIPÓTESIS

El re-diseño de la red de comunicaciones y seguridad informática será a través de entornos centralizados administrables basados en software libre en la empresa Netkrom Technologies SAC..

1.5. OBJETIVOS

1.5.1. OBJETIVOS GENERALES

Re-diseñar la red de comunicaciones y seguridad informática a través de entornos centralizados administrables basados en software libre para la empresa Netkrom Technologies SAC.

1.5.2. OBJETIVOS ESPECÍFICOS

Estudiar las tecnologías y herramientas fundamentales de Networking..

Selección equipos idóneos para realizar el re-diseño de la red de comunicaciones.

Diseñar del sistema centralizado administrable.

Simular con la herramienta Packet Tracer el sistema implementado.

Capacitar al personal del Dpto. de Sistemas en la metodología a emplear en el re-diseño de la red de comunicaciones..

Reducir el impacto en lo más mínimo del cambio en la red de comunicaciones de cara al personal laboral.

1.6. JUSTIFICACION E IMPORTANCIA

La implementación de los diferentes sistemas y servicios está justificada por varias razones: Se cuenta con equipos donde se puedan instalar los diferentes servicios,

se dispone de las herramientas para llevar a cabo la implementación de los servidores como son el sistema operativo, manuales de instalación, código fuente, libertad para modificar el código fuente; hay empresas que si brindan servicios de línea dedicada en las zonas donde se encuentran ubicadas las diferentes sedes.

La importancia de ésta investigación radica en la mejora de la calidad en las comunicaciones de la empresa, permitirá escalabilidad pudiendo agregar más servicios sin que esto demande un replanteo total o genere más inestabilidad de la que ya se presenta. Además es importante recalcar que la implementación de éstos servicios no demandará un coste elevado en cuestión de licencias al ser el Software Open Source y totalmente gratuito y estar disponible para cualquier persona. El departamento de Sistemas presentará ante la gerencia de Operaciones y la gerencia de Administración y Finanzas un plan que involucra la renovación al 90% de la infraestructura Tecnológica así como el presupuesto para la adquisición de equipos tales como router's, switch's, teléfonos y cámaras IP, esto junto a un cronograma de ejecución que se pretende realizarlo en máximo 6 meses, contando como fecha de partida el 28 de enero del 2011.

CAPITULO II: Marco Referencial

2. RADIOENLACE

2.1. DEFINICIÓN DE RADIOENLACE

Se denomina radio enlace a cualquier interconexión entre los terminales de telecomunicaciones efectuados por ondas electromagnéticas. Si los terminales son fijos, el servicio se lo denomina como tal y si algún Terminal es móvil, se lo denomina dentro de los servicios de esas características. Se puede definir al radio enlace del servicio fijo, como sistemas de comunicaciones entre puntos fijos situados sobre la superficie terrestre, que proporcionan una capacidad de información, con características de calidad y disponibilidad determinadas. Típicamente estos enlaces se explotan entre los 800 Mhz y 42 Ghz.

Los radioenlaces, establecen un concepto de comunicación del tipo full -dúplex, de donde se deben transmitir dos portadoras moduladas, una para la transmisión y otra para la recepción. Al par de frecuencias asignadas para la transmisión y recepción de las señales, se lo denomina radio canal. Los enlaces se hacen básicamente entre puntos visibles, es decir, puntos altos de la topografía. Cualquiera que sea la magnitud del sistema de microondas, para un correcto funcionamiento es necesario que los recorridos entre enlaces tengan una altura libre adecuada para la propagación en toda época del año, tomando en cuenta las variaciones de las condiciones atmosféricas de la región. Para poder calcular las alturas libres debe conocerse la topografía del terreno, así como la altura y ubicación de los obstáculos que puedan existir en el trayecto.

2.2. ELEMENTOS DE UN RADIOENALCE

2.2.1. Antenas y sus parámetros

El principio básico de radiación de las antenas se basa en la aceleración o desaceleración de una carga. Se considera a una antena como un elemento transductor, ya que es un elemento de transición entre una onda guiada y una onda de espacio libre y viceversa. Dentro de sus parámetros generales incluyen ganancia, polarización de la antena y ancho del haz.

2.2.2. Ganancia de la antena.

Una antena es un dispositivo pasivo y por lo tanto no puede amplificar la señal, sin embargo esta puede dirigir la señal a que se más fuerte en una dirección respecto de otras. El aumento por el cual la antena dirige su energía en una particular dirección es descrita en términos de su ganancia. Cuando la concentración de la antena en una determinada dirección se compara con una antena isotrópica la medida de la ganancia se expresa en dBi (decibelio isotrópico), y cuando la concentración de la energía en cierta dirección de la antena se compara respecto a un dipolo eléctrico la medida de la ganancia se expresa en dBd (decibelios con respecto a un dipolo ideal). La ganancia de una antena expresada en dB es 2.16 veces menos respecto a una antena isotrópica.

2.2.3. Polarización de la antena.

La polarización de la señal de la antena se refiere al plano sobre el que se desplaza la componente eléctrica del campo electromagnético. Si el plano sobre el que se desplaza el vector de campo eléctrico es vertical se dice que la polarización es vertical, si el plano es horizontal, la polarización es horizontal.

2.2.4. Ancho del haz.

El ancho del haz es una manera de indicar la estrechez del lóbulo principal, el ancho del haz en los puntos de media potencia es el ancho del lóbulo principal e intensidad de media potencia (por ejemplo 3 dB por debajo del punto máximo).

2.2.5. Equipos transceptores de radio

Son el componente fundamental dentro de un radioenlace, estos equipos se encargan de la codificación, encapsulamiento y modulación y demodulación de las señales y datos. En otro apartado de esta investigación trataremos a mayor profundidad los equipos y tecnologías empleadas para este trabajo, así como sus principales características.

2.2.6. Medio de propagación

El medio de propagación juega un rol importante durante una transmisión. Hay distintos medios de propagación de la señal estos medios pueden ser cerrados como en el caso de par de cobre, fibra óptica cable coaxial, etc.; para nuestro caso nos centraremos en el espectro electromagnético, el cuál es el medio de propagación de las señales radioeléctricas. Es en este medio donde la señal sufre alteraciones indeseadas como son:

- Atenuación

Reduce el valor de la señal y puede hacerla tan pequeña como el ruido y hacer que se pierda en este.

- Distorsión

Es el resultado es la deformación que sufre una señal a su paso por un sistema.

- Interferencia

Es un proceso que altera, modifica o destruye la señal durante su trayecto, que es originada por una señal de la misma frecuencia, ajena a la comunicación. La Interferencia puede ser destructiva si la señal interferente se encuentra desfasada 180º respecto a la señal transmitida. La interferencia puede ser constructiva si la señal transmitida e interferente se encuentra en fase (0º), en caso de que las señales se encuentren en una fase distintas la señal original puede sufrir una alteración en sus estructura.

- Ruido

Es un tipo de señal originada por diversos tipos de tipos de perturbación que tienden a enmascarar la información cuando se presenta en la banda de frecuencias del espectro de la señal, es decir dentro de su ancho de banda. Normalmente para medir la influencia del ruido sobre la señal se utiliza la relación señal a ruido que generalmente se maneja en decibelios (dB). En el caso de un radioenlace se tiene en cuenta la relación portadora a ruido (C/N).

2.3. Banda no licenciada

El Ministerio de Transportes y Comunicaciones en el articulo 28 del reglamento general de la ley de telecomunicaciones, establece que aquellos servicios cuyos equipos utilizando las bandas de 902 – 928 MHz, 2400 – 2483.5 MHz y 5725 – 5850

MHz están exceptuados de licencia siempre que operen con una potencia no superior a 100 milivatios (mW) en antena (potencia efectiva irradiada), esto es para espacios cerrados y en el caso de espacios abiertos transmitan con una PIRE (Potencia Isotrópica Radiada Efectiva) menor a 36 dBm.

El Ministerio de Transportes y Comunicaciones a través de la resolución directoral Nº 076-98-MTC/15.19 detalla las características técnicas a las que deben estar sujetas los equipos que operen en banda no licenciada, entre las más importantes tenemos:

Los equipos deben emplear técnicas de transmisión digital que permitan la mutua coexistencia como las modulaciones de espectro ensanchado (secuencia directa (DSSS), salto de frecuencia (FHSS), Multiplexación por División de Frecuencia Ortogonal (OFDM)).

La Potencia Isotrópica Radiada Equivalente (PIRE) máxima deberá estar sujeta a las siguientes características:

PIRE máxima (espacio cerrado)	PIRE máxima (espacio abierto)
100 mW / 20 dBm	4W / 36 dBm

Tabla 1: PIRE máxima y mínima para espacios abiertos y espacios cerrados, según el MTC

Así mismo en el caso del transmisor la Potencia de salida esta limitado a 1 vatio (W), en el caso de espacios abiertos, con la PIRE indicada anteriormente.

También se prohíbe el uso de amplificadores de transmisión que puedan alterar las condiciones de PIRE anteriormente planteadas.

2.4. Homologación de equipos.

Los equipos que realicen emisiones radioeléctricas con Potencia Isotrópica Radiada Equivalente (PIRE), mayor a 10 milivatios (mW) deben contar con una aprobación del MTC para poder operar en nuestro país. Cuando un equipo cuenta con la aprobación del MTC se dice que ha sido Homologado.

2.5. Estándares Wifi.

Una de los estándares de comunicaciones para larga distancia es la IEEE 802.11 popularmente conocida como WiFi, siendo sus principales ventajas el bajo costo, usos de frecuencias libres de licencia y su ancho de banda, así como su flexibilidad en combinación con desarrollo de software abierto. Con referente a sus frecuencias hacen uso de las bandas de 2.4 GHz y 5.8 GHz.

Existe una gran diferencia entre los estándares WIFI, teniendo así:

El estándar IEEE802.11a trabaja en la banda de frecuencia de los 5GHz utilizando la técnica de transmisión OFDM. Da soporte a velocidades de transmisión de 6Mbps a 54Mbps y ocho canales no interferentes de 20MHz. Esta banda de frecuencia está menos saturada que la de 2.4GHz, lo cual es una ventaja, ya que la banda de 2.4GHz también es utilizada por algunos teléfonos inalámbricos, hornos microondas y equipos Bluetooth. El gran inconveniente de este estándar es el de no ser compatible con el IEEE802.11b, mucho más difundido.

El estándar IEEE802.11b trabaja en la banda de frecuencia de 2.4GHz utilizando el sistema de transmisión HR/DSSS. Mediante el uso de la modulación CCK se da soporte a las velocidades de transmisión de 5.5Mbps y 11Mbps. Se cuenta con catorce canales (que pueden estar limitados a once o trece según el país) de 22MHz, de los cuales se pueden utilizar simultáneamente hasta tres de forma no interferente.

El estándar IEEE802.11g fue desarrollado a raíz del importante problema de incompatibilidad entre los equipos de IEEE802.11a y IEEE802.11b. Además, la creación de este estándar atendía al interés en incrementar la capacidad de los equipos y redes WiFi. IEEE802.11g trabaja en la banda de frecuencia de 2.4GHz, manteniendo además los mismos canales y modulaciones de IEEE802.11b, y añade el sistema OFDM mediante el cual se soportan velocidades de transmisión de hasta 54Mbps.

3. CABLEADO ESTRUCTURADO.

3.1. DEFINICIÓN

El cableado estructurado consiste en el tendido de un cable UTP,STP en el interior de un edificio con el propósito de implantar una red de área local. Suele tratarse de cable de par trenzado de cobre, para redes de tipo IEEE 802.3. No obstante, también puede tratarse de fibra óptica o cable coaxial.

Está destinada a transportar a lo largo del edificio las señales de una fuente origen hacia un receptor y viceversa. Es físicamente una red de cable única y completa con combinaciones de cable de par trenzado, fibra óptica, conectores y adaptadores que cumplen una determinada función de acuerdo a lo normado por los estándares internacionales que establecen categorías con mejoras en la fidelidad de la información transmitida.

3.2. CONSIDERACIONES PARA EL DISEÑO DEL CABLEADO ESTRUCTURADO

La norma EIA/TIA 568 Y EIA/TIA 568B establecen dos tipos de elementos en el diseño de un sistema de cableado estructurado:

3.2.1. Cableado Horizontal

El sistema de cableado horizontal es la porción del sistema de cableado de telecomunicaciones que se extiende del área de trabajo al cuarto de telecomunicaciones o viceversa. El cableado horizontal consiste de dos elementos básicos:

Rutas y Espacios Horizontales (también llamado "sistemas de distribución horizontal"). Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Estas rutas y espacios son los "contenedores" del cableado Horizontal.

- Si existiera cielo raso suspendido se recomienda la utilización de canaletas para transportar los cables horizontales.
- Una tubería de ¾ in por cada dos cables UTP.
- Una tubería de 1in por cada cable de dos fibras ópticas.
- Los radios mínimos de curvatura deben ser bien implementados.

El cableado horizontal incluye:

Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo. En inglés: Work Area Outlets (WAO).

Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.

Paneles de empalme (patch panels) y cables de empalme utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

Se deben hacer ciertas consideraciones a la hora de seleccionar el cableado horizontal: contiene la mayor cantidad de cables individuales en el edificio.

Consideraciones de diseño: los costes en materiales, mano de obra e interrupción de labores al hacer cambios en el cableado horizontal pueden ser muy altos. Para evitar estos costes, el cableado horizontal debe ser capaz de manejar una amplia gama de aplicaciones de usuario. La distribución horizontal debe ser diseñada para facilitar el mantenimiento y la re-localización de áreas de trabajo. El diseñador también debe considerar incorporar otros sistemas de información del edificio (por ej. televisión por cable, control ambiental, seguridad, audio, alarmas y sonido) al seleccionar y diseñar el cableado horizontal.

Topología: la norma EIA/TIA 568A hace las siguientes recomendaciones en cuanto a la topología del cableado horizontal: El cableado horizontal debe seguir una topología estrella. Cada toma/conector de telecomunicaciones del área de trabajo debe conectarse a una interconexión en el cuarto de telecomunicaciones.

Distancias: sin importar el medio físico, la distancia horizontal máxima no debe exceder 90 m. La distancia se mide desde la terminación mecánica del medio en la interconexión horizontal en el cuarto de telecomunicaciones hasta la toma/conector de telecomunicaciones en el área de trabajo. Además se recomiendan las siguientes distancias: se separan 10 m. para los cables del área de trabajo y los cables del cuarto de telecomunicaciones (cordones de parcheo, jumpers y cables de equipo).

Medios reconocidos: se reconocen tres tipos de cables para el sistema de cableado horizontal:

Cables de par trenzado sin blindar (UTP) de 100 ohm y cuatro pares.
Cables de par trenzado blindados (STP) de 150 ohm y cuatro pares .
Cables de fibra óptica multimodo de 62.5/125 um y dos fibras.

3.2.2. Cableado Vertical

El propósito del cableado del backbone es proporcionar interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos. El cableado del backbone incluye medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas. El cableado vertical realiza la interconexión entre los diferentes gabinetes de telecomunicaciones y entre estos y la sala de equipamiento. En este componente del sistema de cableado ya no resulta económico mantener la estructura general utilizada en el cableado horizontal, sino que es conveniente realizar instalaciones independientes para la telefonía y datos. Esto se ve reforzado por el hecho de que, si fuera necesario sustituir el backbone, ello se realiza con un coste relativamente bajo, y causando muy pocas molestias a los ocupantes del edificio. El backbone telefónico se realiza habitualmente con cable telefónico multipar. Para definir el backbone de datos es necesario tener en cuenta cuál será la disposición física del equipamiento. Normalmente, el tendido físico del backbone se realiza en forma de estrella, es decir, se interconectan los gabinetes con uno que se define como centro de la estrella, en donde se ubica el equipamiento electrónico más complejo.

El backbone de datos se puede implementar con cables UTP y/o con fibra óptica. En el caso de decidir utilizar UTP, el mismo será de categoría 5e, 6 o 6A y se dispondrá un número de cables desde cada gabinete al gabinete seleccionado como centro de estrella.

Actualmente, la diferencia de coste provocada por la utilización de fibra óptica se ve compensada por la mayor flexibilidad y posibilidad de crecimiento que brinda esta tecnología. Se construye el backbone llevando un cable de fibra desde cada gabinete al gabinete centro de la estrella. Si bien para una configuración mínima Ethernet basta con utilizar cable de 2 fibras, resulta conveniente utilizar cable con

mayor cantidad de fibra (6 a 12) ya que la diferencia de coste no es importante y se posibilita por una parte disponer de conductores de reserva para el caso de falla de algunos, y por otra parte, la utilización en el futuro de otras topologías que requieren más conductores, como FDDI o sistemas resistentes a fallas. La norma EIA/TIA 568 prevé la ubicación de la transmisión de cableado vertical a horizontal, y la ubicación de los dispositivos necesarios para lograrla, en habitaciones independientes con puerta destinada a tal fin, ubicadas por lo menos una por piso, denominadas armarios de telecomunicaciones. Se utilizan habitualmente gabinetes estándar de 19 pulgadas de ancho, con puertas, de aproximadamente 50 cm de profundidad y de una altura entre 1.5 y 2 metros. En dichos gabinetes se dispone generalmente de las siguientes secciones:

- Acometida de los puestos de trabajo: 2 cables UTP llegan desde cada puesto de trabajo.
- Acometida del backbone telefónico: cable multipar que puede determinar en regletas de conexión o en “patch panels”.
- Acometida del backbone de datos: cables de fibra óptica que se llevan a una bandeja de conexión adecuada.
- Electrónica de la red de datos: Hubs, switch's, Bridges y otros dispositivos necesarios.
- Alimentación eléctrica para dichos dispositivos.
- Iluminación interna para facilitar la realización de trabajos en el gabinete.
- Ventilación a fin de mantener la temperatura interna dentro de límites aceptables.

3.2.3. Sistema de puesta a tierra

El sistema de puesta a tierra y puenteo establecido en estándar ANSI/TIA/EIA-607 es un componente importante de cualquier sistema de cableado estructurado moderno. El gabinete deberá disponer de una toma de tierra, conectada a la tierra general de la instalación eléctrica, para efectuar las conexiones de todo equipamiento. El conducto de tierra no siempre se halla indicado en planos y puede ser único para ramales o circuitos que pasen por las mismas cajas de pase, conductos ó bandejas. Los cables de tierra de seguridad serán puestos a tierra en el subsuelo.

3.2.4. Cuarto de entrada de servicios

Consiste en cables, accesorios de conexión, dispositivos de protección, y demás equipo necesario para conectar el edificio a servicios externos. Puede contener el punto de demarcación. Ofrecen protección eléctrica establecida por códigos eléctricos aplicables. Deben ser diseñadas de acuerdo a la norma EIA/TIA-569-A.

Los requerimientos de instalación son:

Precauciones en el manejo del cable.

Evitar tensiones en el cable.

Los cables no deben enrutarse en grupos muy apretados.

Utilizar rutas de cable y accesorios apropiados 100 ohms UTP y STP.

No giros con un angulo menor de 90 grados ni mayor de 270.

3.2.5. Atenuación y capacitancia.

Las señales de transmisión a través de largas distancias están sujetas a distorsión que es una pérdida de fuerza o amplitud de la señal. La atenuación es la razón principal de que el largo de las redes tenga varias restricciones. Si la señal se hace muy débil, el equipo receptor no interceptará bien o no reconocerá esta información. Esto causa errores, bajo desempeño al tener que retransmitir la señal. Se usan repetidores o amplificadores para extender las distancias de la red más allá de las limitaciones del cable. La atenuación se mide con aparatos que inyectan una señal de prueba en un extremo del cable y la miden en el otro extremo.

La capacitancia puede distorsionar la señal en el cable, entre más largo sea el cable, y más delgado el espesor del aislante, mayor es la capacitancia, lo que resulta en distorsión. La capacitancia es la unidad de medida de la energía almacenada en un cable. Los probadores de cable pueden medir la capacitancia de este par para determinar si el cable ha sido roscado o estirado. La capacitancia del cable par trenzado en las redes está entre 17 y 20 pF.

La atenuación y capacitancia están ligadas estrechamente al tipo de conductor, el cobre es usado comúnmente para estos fines.

3.2.6. Par trenzado.

Consiste de 02 alambres de cobre aislados que se trenzan de forma helicoidal constituyendo un circuito de transmisión de datos.

El trenzado consigue eliminar la interferencia eléctrica tanto exterior como de elementos cercanos.

Un cable de par trenzado está formado por un grupo de pares trenzados, normalmente cuatro, recubiertos por un material aislante.

Cada uno de estos pares se identifica mediante un color, siendo los colores asignados y las agrupaciones de los pares de la siguiente forma:

- Par 1: Blanco-Azul/Azul
- Par 2: Blanco-Naranja/Naranja
- Par 3: Blanco-Verde/Verde
- Par 4: Blanco-Marrón/Marrón

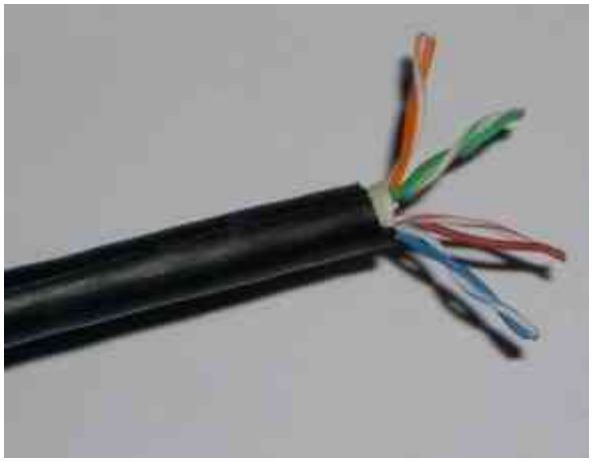


Ilustración 1: Cable de Par Trenzado

3.2.7. Categoría

Dependiendo del número de pares que tenga el cable, del número de vueltas por metro que posea su trenzado y de los materiales utilizados, los estándares de cableado estructurado clasifican a los cables de pares trenzados por categorías: 1, 2, 3, 4, 5, 5e, 6 y 7. Las dos últimas están todavía en proceso de definición.

- Categoría 3: soporta velocidades de transmisión hasta 10 Mbits/seg. Utilizado para telefonía de voz, 10Base-T Ethernet y Token ring a 4 Mbits/seg.
- Categoría 4: soporta velocidades hasta 16 Mbits/seg. Es aceptado para Token Ring a 16 Mbits/seg.
- Categoría 5: hasta 100 Mbits/seg. Utilizado para Ethernet 100Base-TX.

- Categoría 5e: hasta 622 Mbits/seg. Utilizado para Gigabit Ethernet.
- Categoría 6: soporta velocidades hasta 1000 Mbits/seg.

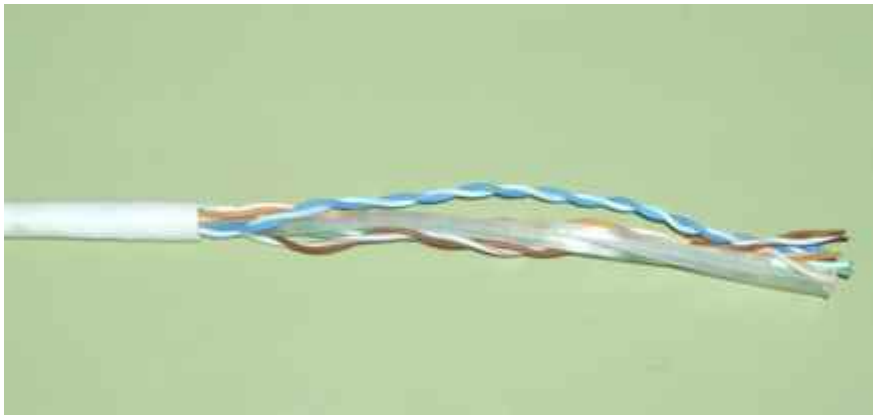


Ilustración 2: Cable UTP Categoría 6

3.2.8. Consideraciones finales

El cable de Par Trenzado debe emplear conectores RJ45 para unirse a los distintos elementos de hardware que componen la red. Actualmente de los ocho cables sólo cuatro se emplean para la transmisión de los datos. Éstos se conectan a los pines del conector RJ45 de la siguiente forma: 1, 2 (para transmitir), 3 y 6 (para recibir).

La Galga o AWG, es un organismo de normalización sobre el cableado. Es importante conocer el significado de estas siglas porque en muchos catálogos aparecen clasificando los tipos de cable. Por ejemplo se puede encontrar que determinado cable consta de un par de hilos de 22 AWG.

AWG hace referencia al grosor de los hilos. Cuando el grosor de los hilos aumenta el AWG disminuye. El hilo telefónico se utiliza como punto de referencia; tiene un grosor de 22 AWG. Un hilo de grosor 14 AWG es más grueso, y uno de 26 AWG es más delgado.

4. SERVICIO DE DIRECTORIO Y PROTOCOLO LDAP

4.1. DEFINICIÓN Y ASPECTOS GENERALES

El servicio de directorio activo o simplemente “El Directorio” es un término ambiguo que se utiliza para referirse a la información contenida, el conjunto hardware / software que gestiona dicha información, las aplicaciones cliente / servidor que utilizan esta información, etc; por lo que se puede decir que el Servicio de Directorio es un conjunto complejo de componentes que trabajaban de forma cooperativa para prestar un servicio.

Partiendo de lo descrito, podemos concluir que “El directorio” es una gran base de datos donde se almacena y organiza la información sobre los usuarios de una red de ordenadores y centraliza la gestión de los mismos, como dar de alta a un usuario, administrar las contraseñas de acceso, ingresar un ordenador al sistema, etc.

En 1988, la CCITT creó el estándar X.500, sobre servicios de directorio. En 1990 este estándar fue adoptado por la ISO como “ISO 9594, Data Communications Network Directory Recommendations X.500-X.521”.

Este estándar organiza las entradas en el directorio de forma jerárquica, capaz de almacenar gran cantidad de datos con grandes capacidades de búsqueda y fácilmente escalable. X.500 especifica que la comunicación entre el cliente y el servidor de directorio debe emplear el Directory Access Protocol (DAP), pero DAP es un protocolo de la capa de aplicación, por lo que tanto el cliente como el servidor debían implementar toda la pila de protocolo OSI.

LDAP (Ligthweight Directory Access Protocol) surge como alternativa a DAP, cuyas ventajas pronto hicieron que alcanzara gran uso y desarrollo por parte de desarrolladores. Estas ventajas son:

- LDAP utiliza TCP/IP (que requiere mucho menos recursos y está disponible para la mayoría de ordenadores) en lugar de OSI.
- El modelo funcional de LDAP es más simple y a eliminado características raramente usadas en X.500. LDAP es mucho más fácil de implementar.
- LDAP representa la información mediante cadena de caracteres en lugar de complicadas estructuras ASN.1.

4.2. CARACTERÍSTICAS DE UN DIRECTORIO

- ✔ El directorio es dinámico; se puede actualizar la información frecuentemente y que pueda ser consultada por el lado del cliente.
- ✔ Es flexible; ya que se puede almacenar cualquier tipo de información y ampliarla y su organización permite localizarla de diferente manera pudiendo realizar búsquedas aproximadas con un resultado rápido y satisfactorio.

- ✔ Es seguro; ya que se puede controlar su acceso a través de ACL, passwords, de tal manera que no cualquiera pueda modificar su contenido, e incluso poder visualizar su contenido.
- ✔ Es configurable; la información puede ser personalizada antes de mostrarse a los diferentes usuarios.

Un directorio puede verse como una base de datos especializada, la diferencia entre una base de datos de propósito general y un directorio son las siguientes:

- ➔ Relación entre lectura / escritura; esto se debe a que la información contenida raramente se modifica, por el contrario siempre responden a consultas de parte de los usuarios, como por ejemplo el correo de un usuario, su número SIP, etc.
- ➔ Extensibilidad; ya que se puede extender sus funciones con schemas que cumplan un determinado formato establecido.
- ➔ Replicación de la información; esto es muy común en sistemas informáticos debido a la necesidad de balancear la carga y tener backup's cuando el servidor principal o “maestro” se vea colapsado.
- ➔ Rendimiento; a diferencia de una base de datos relacional, el directorio deberá responder a miles de consultas por segundo en vez de permitir miles de transacciones por segundo.
- ➔ Estándares; ya que al tratarse de un estándar no se verá restringido a un solo fabricante, pudiendo cambiar de proveedor en el momento que lo considere conveniente, sin tener que cambiar el software que usen los clientes.

4.3. ARQUITETURA CLIENTE SERVIDOR

Los servicios de directorio suelen implementarse siguiendo el modelo cliente-servidor, de modo que una aplicación que desea acceder al directorio no accede directamente a la base de datos, sino que llama a una función de la API (Application Programming Interface), que envía un mensaje a un proceso en el servidor. Dicho proceso accede al directorio y devuelve el resultado de la operación.

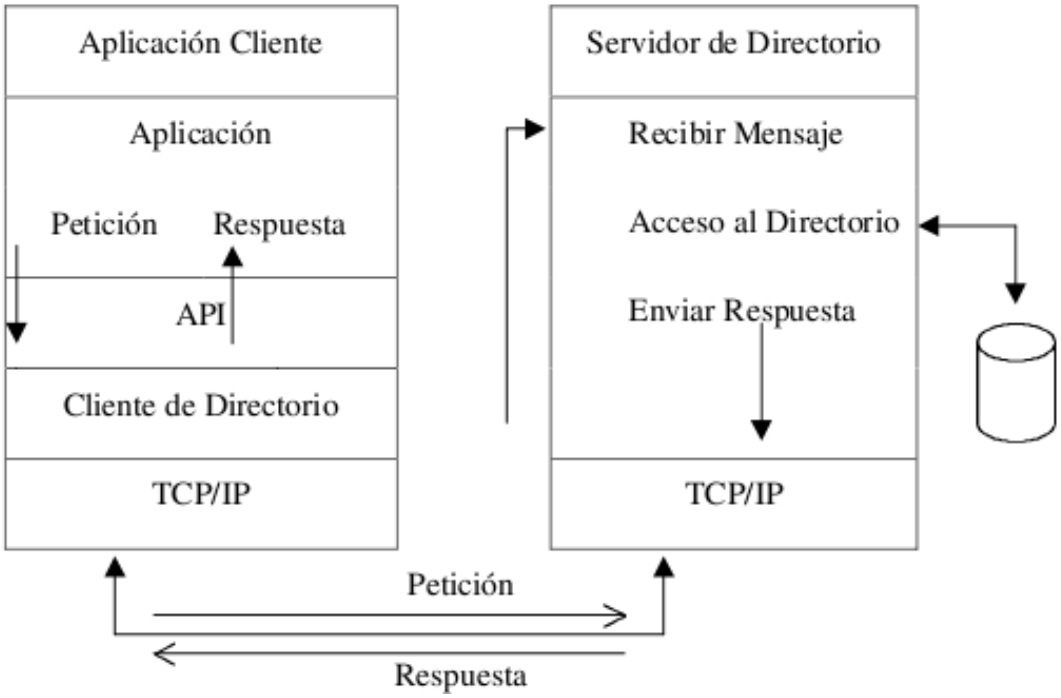


Ilustración 3: Arquitectura Cliente Servidor del Directorio

Siguiendo ésta arquitectura el cliente no depende de la arquitectura del servidor y el servidor puede implementar el directorio de la forma más conveniente.

4.4. SEGURIDAD DE DIRECTORIO

La seguridad de la información almacenada en el directorio es uno de los aspectos fundamentales.

Algunos directorios deben permitir el acceso público, pero cualquier usuario no debe poder realizar cualquier operación.

Cualquier usuario puede buscar la dirección de correo de un empleado, pero solo el empleado o el

administrador deber tener permiso para modificarla. El departamento de Organización y Recursos

Humanos debe tener permiso para buscar el número de teléfono privado de un empleado, pero ninguno de sus compañeros debe tener acceso a esta información.

La política de seguridad define quién tiene qué tipo de acceso sobre qué información.

El directorio debe permitir las capacidades básicas para implementar la política de seguridad. El directorio puede no incorporar estas capacidades, pero debe estar integrado con un servicio de red fiable que proporcione estos servicios básicos de seguridad. Inicialmente se necesita un método para autenticar al usuario, una vez que se ha verificado la identidad del cliente, se puede determinar si esta autorizado para realizar la operación solicitada. Generalmente las autorizaciones están basadas en ACL (Access Control List). Estas listas se pueden unir a los objetos y/o los atributos contenidos en el directorio. Para facilitar la administración de estas listas, los usuarios con los mismos permisos, son agrupados en grupos de seguridad.

Debido a que LDAP nació como alternativa ligera a DAP para el acceso a servidores X.500, sigue el modelo X.500.

El directorio almacena y organiza la información en estructuras de datos denominadas entradas.

Cada entrada del directorio describe un objeto (una persona, una impresora, etc).

Cada entrada tiene un nombre llamado Distinguished Name (DN), que la identifica unívocamente. Un DN consiste en una secuencia de partes más pequeñas llamadas Relative Distinguished Name (RDN), de forma similar a como el nombre de un fichero consiste en un camino de directorios en muchos sistemas operativos (UNIX, por ejemplo).

Las entradas pueden ser organizadas en forma de árbol basándose en los DN, a este árbol de entradas de directorio se le conoce como Directory Information Tree (DIT).

Una clase de objeto es una descripción general de un tipo de objeto.

El Schema define que clases de objetos se pueden almacenar en el directorio, que atributos deben contener, que atributos son opcionales y el formato de los atributos.

LDAP define primitivas de acceso y modificación de las entradas del directorio:

- Búsqueda siguiendo un criterio especificado por el usuario.
- Añadir una entrada.
- Borrar una entrada.
- Modificar una entrada.
- Modificar el DN de una entrada.
- Comparar una entrada.

4.5. ESTRUCTURA CLASICA DE UN DIRECTORIO

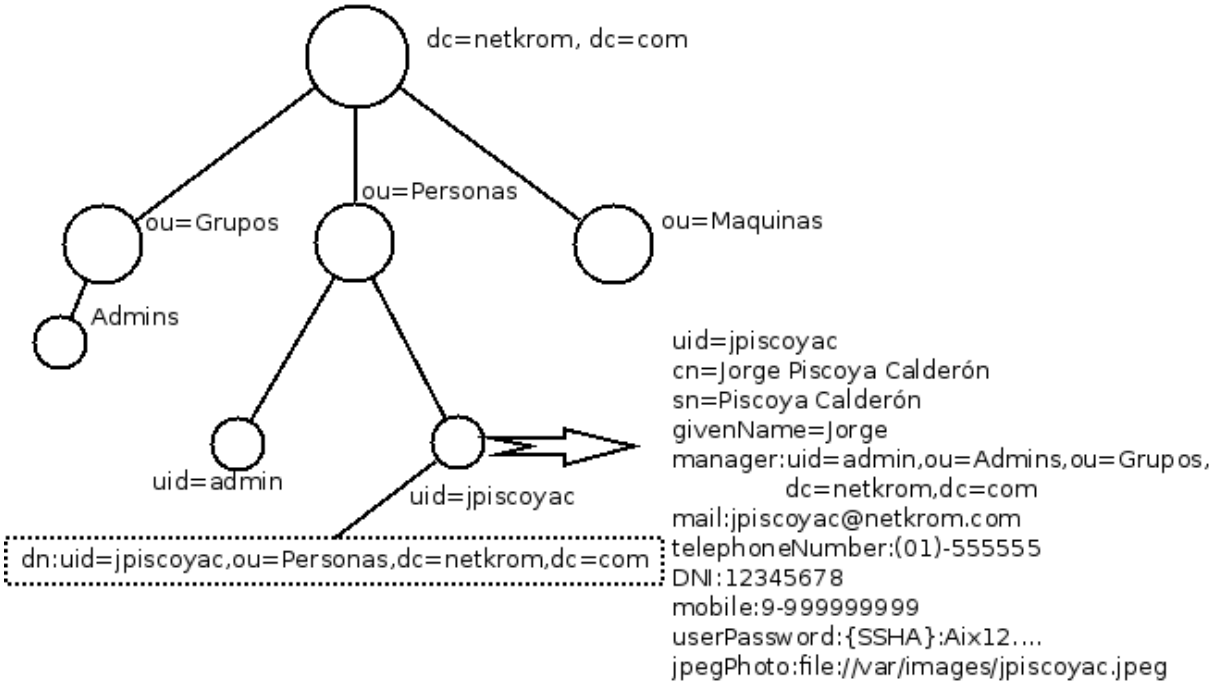


Ilustración 4: Ejemplo esquema de directorio clásico

En la ilustración se muestra una estructura clásica de un directorio activo, donde se diferencia claramente la jerarquía piramidal que existe, desde una cabeza que viene a ser la organización hasta los miembros internos que la conforman.

5. SERVIDOR DNS

5.1. DEFINICIÓN Y ASPECTOS GENERALES

Los servidores DNS son parte de la cadena que queda formada cuando hacemos una petición mediante nuestro navegador de cualquier página web.

Estos servidores no son más que computadoras que en sus discos duros almacenan enormes bases de datos.

Tienen registrada la relación que existe entre cada nombre de dominio y su dirección IP correspondiente.

Los seres humanos identificamos los sitios de Internet mediante nombres, como son Google.com, Yahoo.es, Apple.com, etc. lo que los hace más fácil de recordar y de escribir, estos nombres es lo que conocemos como nombres de dominio.

Las computadoras identifican los sitios web y se conectan a ellos utilizando el formato numérico, algo parecido a la numeración telefónica, pero más complejo y con más recursos, es lo que conocemos como las direcciones IP.

Ahí es donde entran en acción los servidores DNS, ellos son como enormes y complejas guías telefónicas, que a petición nuestra traducen o convierten los nombres de dominio que le solicitemos, en las direcciones IP que les corresponden.

5.2. EMPLEO DE LOS SERVIDORES DNS EN INTERNET

1- Resolución de nombres: Convertir un nombre de host en la dirección IP que le corresponde.

Por ejemplo, al nombre de dominio netkrom.com, le corresponde la dirección IP 50.116.84.40

2- Resolución inversa de direcciones: Es el mecanismo inverso al anterior, de una dirección IP obtener el nombre de host correspondiente.

3- Resolución de servidores de correo: Dado un nombre de dominio (por ejemplo gmail.com), obtener el servidor a través del cual debe realizarse la entrega del correo electrónico.

5.3. COMO SE ESTABLECE UNA CONEXION

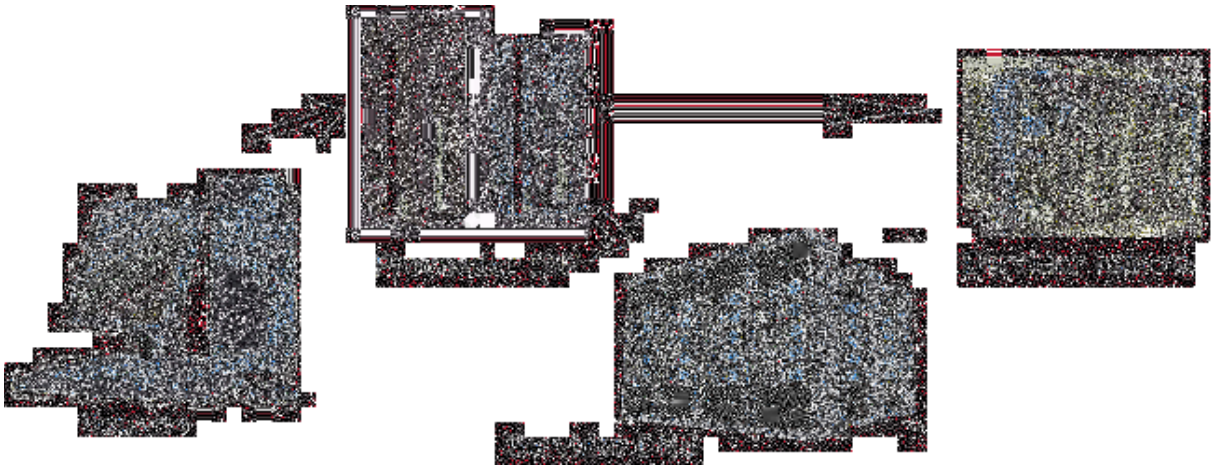


Ilustración 5:

Primer ejemplo, conexión directa:Escribimos en nuestro navegador la dirección de una página web, por ejemplo: http://www.sitio.com,si en otras ocasiones hemos entrado a esta página, en nuestra cache o la del servidor del que depende nuestra conexión, tenemos registrada la dirección IP que le corresponde, por lo que la conexión será directa sin intermediarios.

6. SERVIDOR DHCP

6.1. DEFINICION Y ASPECTOS GENERALES

El protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de nuestra red. El estándar DHCP permite el uso de servidores DHCP para administrar la asignación dinámica, a los clientes DHCP de la red, de direcciones IP y otros detalles de configuración relacionados, siempre que los clientes estén configurados para utilizar un servidor DHCP (en lugar de estar configurados manualmente con una dirección IP, en las conexiones de red de las estaciones de trabajo, activaremos la "configuración automática de IP").

Cada equipo de una red TCP/IP debe tener un nombre y una dirección IP únicos. La dirección IP (junto con su máscara de subred relacionada) identifica al equipo host y a la subred a la que está conectado. Al mover un equipo a una subred diferente, se debe cambiar la dirección IP; DHCP permite asignar dinámicamente una dirección IP a un cliente, a partir de una base de datos de direcciones IP de servidor DHCP de la red local. En las redes TCP/IP, DHCP reduce la complejidad y cantidad de trabajo que debe realizar el administrador para reconfigurar los equipos.

DHCP es el protocolo de servicio TCP/IP que "alquila" o asigna dinámicamente direcciones IP durante un tiempo (duración del alquiler) a las estaciones de trabajo, distribuyendo además otros parámetros de configuración entre clientes de red autorizados, tales como la puerta de enlace o el servidor DNS. DHCP proporciona una configuración de red TCP/IP segura, confiable y sencilla, evita conflictos de direcciones y ayuda a conservar el uso de las direcciones IP de clientes en la red. Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP utilizadas en la red. Los clientes compatibles con DHCP podrán solicitar a un servidor DHCP una dirección IP y obtener la concesión como parte del proceso de inicio de red.

Las estaciones de trabajo "piden" su dirección IP (y demás configuraciones para este protocolo) al servidor, y éste les va asignando direcciones del rango que sirve, de entre aquellas que le quedan libres; si deseamos que a determinados equipos el servidor les sirva siempre la misma, podemos llegar a "forzar" la asignación de la dirección IP deseada a equipos concretos. Además también pueden excluirse del rango de direcciones IP que va a servir nuestro servidor, aquellas que deseamos que estén asociadas de forma estática a determinados equipos o periféricos de red.

Si por error dejásemos algún equipo de la red configurado con un direccionamiento IP estático del rango gestionado por nuestro servidor DHCP, podría ocurrir que cuando nuestro servidor "alquilase" una IP a la estación de trabajo solicitante, dicha dirección IP fuera la que estuviera siendo utilizada por el equipo con direccionamiento estático, provocándose un conflicto de IP; en ese caso el cliente selecciona otra dirección IP y la prueba, hasta que obtenga una dirección IP que no esté asignada actualmente a ningún otro equipo de nuestra red. Por cada conflicto de direcciones, el cliente volverá a intentar configurarse automáticamente hasta con 10 direcciones IP.

En caso de que el cliente DHCP haya obtenido anteriormente una concesión de licencia de un servidor DHCP, cada vez que el cliente arranque de nuevo, se comportará del siguiente modo:

- Si la concesión de alquiler de licencia ha caducado, el cliente solicitará una nueva licencia al servidor DHCP (la asignación del servidor podría coincidir con la anterior).
- Si la concesión de alquiler no ha caducado en el momento del inicio, el cliente intentará renovar su concesión en el servidor DHCP, es decir, que le sea asignada la misma dirección IP.
- Si durante el intento de renovación de su concesión, el cliente no puede localizar un servidor DHCP, intentará realizar un "ping" a la puerta de enlace predeterminada de la concesión; si el resultado del "ping" es satisfactorio, el cliente DHCP supone que sigue ubicado en la misma red en que obtuvo su concesión actual y continuará utilizándola; en caso de que el resultado del "ping" sea erróneo, el cliente supone que ha sido movido a otra red en que los servicios DHCP no están disponibles, y configura automáticamente su dirección IP utilizando una dirección de la red de clase B reservada de Microsoft, 169.254.0.0, con máscara de subred 255.255.0.0 (obviamente el equipo no conectará con la red). Una vez que el cliente se ha configurado automáticamente con una dirección IP del rango indicado, buscará un servidor DHCP en segundo plano cada cinco minutos para obtener una concesión.

En caso de que el cliente nunca haya obtenido una concesión de licencia de un servidor DHCP:

- El cliente DHCP intenta localizar un servidor DHCP y obtener una configuración del mismo.
- Si no puede encontrar un servidor DHCP, el cliente DHCP configura automáticamente su dirección IP y su máscara de subred mediante la utilización de una dirección seleccionada de la red de clase B reservada de Microsoft, 169.254.0.0, con máscara de subred 255.255.0.0; el cliente comprobará la existencia de un servidor DHCP en segundo plano cada cinco minutos. Si posteriormente encuentra un servidor DHCP, el cliente abandonará la información que ha configurado automáticamente. A continuación, el cliente DHCP utiliza una dirección que ofrece el servidor DHCP (así como el resto de información de opciones DHCP proporcionadas) para actualizar los valores de su configuración IP.

Antes de comenzar con los procesos de instalación y configuración de nuestro DHCP, vamos a definir algunos términos que utilizaremos a lo largo de dicho proceso.

Ámbito servidor DHCP.- Un ámbito es un agrupamiento administrativo de equipos o clientes de una subred que utilizan el servicio DHCP.

Rango servidor DHCP.- Un rango de DHCP está definido por un grupo de direcciones IP en una subred determinada, como por ejemplo de 192.168.0.1 a 192.168.0.254, que el servidor DHCP puede conceder a los clientes.

Concesión o alquiler de direcciones.- es un período de tiempo que los servidores DHCP especifican, durante el cual un equipo cliente puede utilizar una dirección IP asignada.

Autorización servidor DHCP.- Habilitación del servidor DHCP instalado para que sirva direcciones IP a los clientes pertenecientes al dominio gestionado por Active Directory.

7. SERVIDOR PROXY

7.1. DEFINICION Y CONCEPTOS GENERALES

Un servidor proxy es en principio un equipo que actúa como intermediario entre los equipos de una red de área local (a veces mediante protocolos, con excepción del protocolo TCP/IP) e Internet.

Generalmente el servidor proxy se utiliza para la Web. Se trata entonces de un proxy HTTP. Sin embargo, puede haber servidores proxy para cada protocolo de aplicación (FTP, etc.).

7.2. PRINCIPIO OPERATIVO.

El principio operativo básico de un servidor proxy es bastante sencillo: se trata de un servidor que actúa como "representante" de una aplicación efectuando solicitudes en Internet en su lugar. De esta manera, cuando un usuario se conecta a Internet con una aplicación del cliente configurada para utilizar un servidor proxy, la aplicación primero se conectará con el servidor proxy y le dará la solicitud. El servidor proxy se conecta entonces al servidor al que la aplicación del cliente desea conectarse y le envía la solicitud. Después, el servidor le envía la respuesta al proxy, el cual a su vez la envía a la aplicación del cliente.

7.3. CARACTERÍSTICAS

En los sucesivo, con la utilización de TCP/IP dentro de redes de área local, la función de retransmisión del servidor proxy está directamente asegurada por pasarelas y router's. Sin embargo, los servidores proxy siguen utilizándose ya que cuentan con cierto número de funciones que poseen otras características.

7.4. ALMACENAMIENTO CACHE

La mayoría de los proxy's tienen una caché, es decir, la capacidad de guardar en memoria (“en caché”) las páginas que los usuarios de la red de área local visitan comúnmente para poder proporcionarlas lo más rápido posible. De hecho, el término "caché" se utiliza con frecuencia en informática para referirse al espacio de almacenamiento temporal de datos (a veces también denominado "buffer").

Un servidor proxy con la capacidad de tener información en caché (neologismo que significa: poner en memoria oculta) generalmente se denomina servidor "proxy-caché".

Esta característica, implementada en algunos servidores proxy, se utiliza para disminuir tanto el uso de ancho de banda en Internet como el tiempo de acceso a los documentos de los usuarios.

Sin embargo, para lograr esto, el proxy debe comparar los datos que almacena en la memoria caché con los datos remotos de manera regular para garantizar que los datos en caché sean válidos.

7.5. FILTRADO

Por otra parte, al utilizar un servidor proxy, las conexiones pueden rastrearse al crear registros de actividad (log's) para guardar sistemáticamente las peticiones de los usuarios cuando solicitan conexiones a Internet. Gracias a esto, las conexiones de Internet pueden filtrarse al analizar tanto las solicitudes del cliente como las respuestas del servidor. El filtrado que se realiza comparando la solicitud del cliente con una lista de solicitudes autorizadas se denomina lista blanca; y el filtrado que se realiza con una lista de sitios prohibidos se denomina lista negra. Finalmente, el análisis de las respuestas del servidor que cumplen con una lista de criterios (como palabras clave) se denomina filtrado de contenido.

7.6. AUTENTICACION

Como el proxy es una herramienta intermediaria indispensable para los usuarios de una red interna que quieren acceder a recursos externos, a veces se lo puede

utilizar para autenticar usuarios, es decir, pedirles que se identifiquen con un nombre de usuario y una contraseña. También es fácil otorgarles acceso a recursos externos sólo a las personas autorizadas y registrar cada uso del recurso externo en archivos de registro de los accesos identificados.

Este tipo de mecanismo, cuando se implementa, obviamente genera diversos problemas relacionados con las libertades individuales y los derechos personales.

8. SER VIDOR ARCHIVOS

8.1. DEFINICION

La función de un Servidor de archivos (o su nombre en inglés: File Server) es permitir el acceso remoto a archivos almacenados en él o directamente accesibles por éste. En principio, cualquier ordenador conectado a una red con un software apropiado, puede funcionar como servidor de archivos. Desde el punto de vista del cliente de un servidor de archivos, la localización de los archivos compartidos es transparente, es decir, normalmente no hay diferencias perceptibles si un archivo está almacenado en un servidor de archivos remoto o en el disco de la propia máquina.

La ventaja de tener un servidor de archivos es que se tiene acceso controlado a los recursos por medio de contraseñas, para mantener la privacidad de los archivos deseados; también con la posibilidad de compartir recursos entre varios usuarios o tener un lugar público de archivos en donde todos puedan almacenar información;todo depende de las necesidades de cada empresa.

Algunos protocolos comúnmente utilizados en servidores de archivos:

- SMB/CIFS (Windows, Samba en Unix)
- NFS (Unix)

9. SERVIDOR WEB

9.1. DEFINICION

Un servidor web o servidor HTTP es un programa informático que procesa una aplicación del lado del servidor realizando conexiones bidireccionales y/o unidireccionales y síncronas o asíncronas con el cliente generando o cediendo una respuesta en cualquier lenguaje o Aplicación del lado del cliente. El código recibido por el cliente suele ser compilado y ejecutado por un navegador web. Para la transmisión de todos estos datos suele utilizarse algún protocolo. Generalmente se utiliza el protocolo HTTP para estas comunicaciones, perteneciente a la capa de aplicación del modelo OSI. El término también se emplea para referirse al ordenador que ejecuta el programa.

9.2. FUNCIONAMIENTO

El Servidor web se ejecuta en un ordenador manteniéndose a la espera de peticiones por parte de un cliente (un navegador web) y que responde a estas peticiones adecuadamente, mediante una página web que se exhibirá en el navegador o mostrando el respectivo mensaje si se detectó algún error. A modo de ejemplo, al teclear www.wikipedia.org en nuestro navegador, éste realiza una petición HTTP al servidor de dicha dirección. El servidor responde al cliente enviando el código HTML de la página; el cliente, una vez recibido el código, lo interpreta y lo exhibe en pantalla. Como vemos con este ejemplo, el cliente es el encargado de interpretar el código HTML, es decir, de mostrar las fuentes, los colores y la disposición de los textos y objetos de la página; el servidor tan sólo se limita a transferir el código de la página sin llevar a cabo ninguna interpretación de la misma.

Además de la transferencia de código HTML, los Servidores web pueden entregar aplicaciones web. Éstas son porciones de código que se ejecutan cuando se realizan ciertas peticiones o respuestas HTTP. Hay que distinguir entre:

- Aplicaciones en el lado del cliente: el cliente web es el encargado de ejecutarlas en la máquina del usuario. Son las aplicaciones tipo Java "applet's" o JavaScript: el servidor proporciona el código de las aplicaciones al cliente y éste, mediante el navegador, las ejecuta. Es necesario, por tanto, que el cliente disponga de un navegador con capacidad para ejecutar aplicaciones (también llamadas scripts). Comúnmente, los navegadores

permiten ejecutar aplicaciones escritas en lenguaje JavaScript y java, aunque pueden añadirse más lenguajes mediante el uso de plugins.

- Aplicaciones en el lado del servidor: el servidor web ejecuta la aplicación; ésta, una vez ejecutada, genera cierto código HTML; el servidor toma este código recién creado y lo envía al cliente por medio del protocolo HTTP.

Las aplicaciones de servidor muchas veces suelen ser la mejor opción para realizar aplicaciones web. La razón es que, al ejecutarse ésta en el servidor y no en la máquina del cliente, éste no necesita ninguna capacidad añadida, como sí ocurre en el caso de querer ejecutar aplicaciones JavaScript o java. Así pues, cualquier cliente dotado de un navegador web básico puede utilizar este tipo de aplicaciones.

El hecho de que HTTP y HTML estén íntimamente ligados no debe dar lugar a confundir ambos términos. HTML es un lenguaje de marcas y HTTP es un "protocolo".

9.3. SERVIDOR WEB LOCAL

Un Servidor Web Local es aquel Servidor Web que reside en una red local al equipo de referencia. El Servidor web Local puede estar instalado en cualquiera de los equipos que forman parte de una red local. Es por tanto obvio, que todos los Servidores Web, son locales a la red local en la que se encuentran, o como mínimo, locales al sistema en el que están instalados.

Cuando un servidor Web se encuentra instalado en el mismo equipo desde el cual se desea acceder puede utilizarse la dirección de Loopback, 127.0.0.1 en Ipv4 y ::1 en Ipv6. El puerto TCP 80 se obvia. Los archivos se almacenan en un directorio determinado por la configuración, generalmente modificable.

Existen numerosas aplicaciones que facilitan la instalación automática de servidores web Apache y aplicaciones adicionales como MySQL y PHP (entre otros), de forma conjunta, como XAMPP, JAMP o EasyPHP. Estas aplicaciones reciben el nombre de LAMP cuando se instalan en plataformas Linux, WAMP en sistemas Windows y MAMP en sistemas Apple Macintosh.

10. SERVIDOR CORREO

10.1. DEFINICION

Un servidor de correo es una aplicación de red ubicada en un servidor en Internet.

El MTA tiene varias formas de comunicarse con otros servidores de correo:

- Recibe los mensajes desde otro MTA. Actúa como "servidor" de otros servidores.
- Envía los mensajes hacia otro MTA. Actúa como un "cliente" de otros servidores.
- Actúa como intermediario entre un "Mail Submision Agent" y otro MTA.

Algunas soluciones de correo que incluyen un MTA son: Sendmail, qmail, Postfix, Exim, Mdaemon, Mercury Mail Transport System, Lotus Notes (IBM) y Microsoft Exchange Server.

Por defecto el protocolo estándar para la transferencia de correos entre servidores es el SMTP, o Protocolo Simple de Transferencia de Correo. Está definido en el RFC 2821 y es un estándar oficial de Internet.

10.2. CARACTERÍSTICAS

Un servidor de correo realiza una serie de procesos que tienen la finalidad de transportar información entre los distintos usuarios. Usualmente el envío de un correo electrónico tiene como fin que un usuario (remitente) cree un correo electrónico y lo envíe a otro (destinatario). Esta acción toma típicamente 5 pasos:

- El usuario inicial crea un "correo electrónico"; un archivo que cumple los estándares de un correo electrónico. Usará para ello una aplicación ad-hoc. Las aplicaciones más usadas, en indistinto orden son: Outlook Express (Microsoft), Microsoft Outlook, Mozilla Thunderbird (Mozilla), Pegasus Mail (David Harris), Lotus Notes (IBM), etc.
- El archivo creado es enviado a un almacén; administrado por el servidor de correo local al usuario remitente del correo; donde se genera una solicitud de envío.
- El servicio MTA local al usuario inicial recupera este archivo e inicia la negociación con el servidor del destinatario para el envío del mismo.

- El servidor del destinatario valida la operación y recibe el correo, depositándolo en el "buzón" correspondiente al usuario receptor del correo. El "buzón" no es otra cosa que un registro en una base de datos.
- Finalmente el software del cliente receptor del correo recupera este archivo o "correo" desde el servidor almacenando una copia en la base de datos del programa cliente de correo, ubicada en la computadora del cliente que recibe el correo.

A diferencia de un servicio postal clásico, que recibe un único paquete y lo transporta de un lugar a otro; el servicio de correo electrónico copia varias veces la información que corresponde al correo electrónico.

Este proceso que en la vida real ocurre de manera muy rápida involucra muchos protocolos. Por ejemplo para ubicar el servidor de destino se utiliza el servicio DNS, el que reporta un tipo especial de registro para servidores de correo. Una vez ubicado, para obtener los mensajes del servidor de correos receptor, los usuarios se sirven de clientes de correo que utilizan el protocolo POP3 o el protocolo IMAP para recuperar los "correos" del servidor y almacenarlos en sus computadores locales.

10.3. SEGURIDAD

Si tiene en cuenta el proceso, hay por lo menos una copia del correo en el servidor de envío y otra copia en el servidor de recepción. Las políticas de funcionamiento de cada servidor, con o sin aviso a los usuarios remitente y/o destinatario, podrían:

- No recibir correos de acuerdo a algún parámetro.
- Destruir las copias de los correos, por ejemplo al trasferirlos satisfactoriamente.
- Copiar los correos a algún otro registro o archivo.
- Enviar una o más copias a otros destinatarios.
- No destruir nunca los correos almacenados.

Es de suma importancia considerar qué entidad, institución y funcionario son los responsables de administrar finalmente los servidores de correo que cada uno usa. Los correos pueden en muchos casos ser fuente de invasión a la privacidad.

10.4. SERVIDORES DE CORREO WEB

Una forma especial de servidor de correo, es aquél que es accedido vía Web usando el protocolo http. En realidad no es servidor, sino un cliente de correo que corre en un servidor web. A través de dicho cliente se puede acceder al servidor de correo sin necesidad de instalar un cliente de correo en la computadora local.

En este tipo de servidor, el archivo de datos del remitente o destinatario puede ser accedido sin requerir un cliente local. En el mismo servidor se integran programas para acceder a los correos del mismo. Ejemplos típicos de este servicio son: www.hotmail.com, www.yahoo.com y www.gmail.com.

10.5. SPAM

Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La palabra spam proviene de la segunda guerra mundial, cuando los familiares de los soldados en guerra les enviaban comida enlatada; entre estas comidas enlatadas estaba una carne enlatada llamada spam, que en los Estados Unidos era y sigue siendo muy común.

Aunque se puede hacer spam por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de Internet que han sido objeto de correo basura incluyen grupos de noticias, usenet, motores de búsqueda, redes sociales, páginas web wiki, foros, web log's (blogs), a través de ventanas emergentes y todo tipo de imágenes y textos en la web.

El correo basura también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea como por ejemplo Outlook, Lotus Notes,Windows live ,etc.

También se llama correo no deseado a los virus sueltos en la red y páginas filtradas (casino, sorteos, premios, viajes, drogas, software y pornografía), se activa mediante el ingreso a páginas de comunidades o grupos o acceder a enlaces en diversas páginas o inclusive sin antes acceder a ningún tipo de páginas de publicidad.

De todas formas, el spam ha tomado una resemantización dentro del contexto de foros, siendo considerado spam cuando un usuario publica algo que desvirtúa o no tiene nada que ver con el tema de conversación. También, en algunos casos, un mensaje que no contribuye de ninguna forma al tema es considerado spam. Una tercera forma de Spamming en foros es cuando una persona publica repetidamente mensajes acerca de un tema en particular en una forma indeseable (y probablemente molesta) para la mayor parte del foro. Finalmente, también existe el caso en que una persona publique mensajes únicamente con el fin de incrementar su rango, nivel o número de mensajes en el foro.

11. VOZ SOBRE IP.

11.1. DEFINICION

Voz sobre Protocolo de Internet, también llamado Voz sobre IP, Voz IP, VozIP, (VoIP por sus siglas en inglés, Voice over IP), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN (sigla de Public Switched Telephone Network, Red Telefónica Pública Conmutada).

Los Protocolos que se usan para enviar las señales de voz sobre la red IP se conocen como protocolos de Voz sobre IP o protocolos IP. Estos pueden verse como aplicaciones comerciales de la "Red experimental de Protocolo de Voz" (1973), inventada por ARPANET.

El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo las redes de área local (LAN).

Es muy importante diferenciar entre Voz sobre IP (VoIP) y Telefonía sobre IP.

VoIP es el conjunto de normas, dispositivos, protocolos, en definitiva la tecnología que permite comunicar voz sobre el protocolo IP.

Telefonía sobre IP es el servicio telefónico disponible al público, por tanto con numeración E.164, realizado con tecnología de VoIP.

11.2. FUNCIONALIDAD

VoIP puede facilitar tareas que serían más difíciles de realizar usando las redes telefónicas comunes:

- Las llamadas telefónicas locales pueden ser automáticamente enrutadas a un teléfono VoIP, sin importar dónde se esté conectado a la red. Uno podría llevar consigo un teléfono VoIP en un viaje, y en cualquier sitio conectado a Internet, se podría recibir llamadas.
- Números telefónicos gratuitos para usar con VoIP están disponibles en Estados Unidos de América, Reino Unido y otros países con organizaciones de usuarios VoIP.
- Los agentes de call center usando teléfonos VoIP pueden trabajar en cualquier lugar con conexión a Internet lo suficientemente rápida.
- Algunos paquetes de VoIP incluyen servicios extra por los que PSTN (Red Pública Telefónica Conmutada) normalmente cobra un cargo extra, o que no se encuentran disponibles en algunos países, como son las llamadas de 3 a la vez, retorno de llamada, remarcación automática, o identificación de llamada.

11.3. VENTAJAS

La principal ventaja de este tipo de servicios es que evita los cargos altos de telefonía (principalmente de larga distancia) que son usuales de las compañías de la Red Pública Telefónica Conmutada (PSTN).

El desarrollo de codec's para VoIP (aLaw, G.729, G.723, etc.) ha permitido que la voz se codifique en paquetes de datos cada vez más pequeños. Esto deriva en que las comunicaciones de voz sobre IP requieran anchos de banda muy reducidos. Junto con el avance permanente de las conexiones ADSL en el mercado residencial, éste tipo de comunicaciones están siendo muy populares para llamadas internacionales.

Hay dos tipos de servicio de PSTN a VoIP: "Discado Entrante Directo" (Direct Inward Dialling: DID) y "Números de acceso". DID conecta a quien hace la llamada directamente con el usuario VoIP, mientras que los Números de acceso requieren que este introduzca el número de extensión del usuario de VoIP. Los Números de

acceso son usualmente cobrados como una llamada local para quien hizo la llamada desde la PSTN y gratis para el usuario de VoIP.

11.4. DESVENTAJAS

Calidad de la llamada. Es un poco inferior a la telefónica, ya que los datos viajan en forma de paquetes, es por eso que se pueden tener algunas perdidas de información y demora en la transmisión. El problema en si de la VoIP no es el protocolo sino la red IP, ya que esta no fue pensada para dar algún tipo de garantías. Otra desventaja es la latencia, ya que cuando el usuario está hablando y otro usuario está escuchando, no es adecuado tener 200ms (milisegundos) de pausa en la transmisión. Cuando se va a utilizar VoIP, se debe controlar el uso de la red para garantizar una transmisión de calidad.

Robos de Datos. Un cracker puede tener acceso al servidor de VoIP y a los datos de voz almacenados y al propio servicio telefónico para escuchar conversaciones o hacer llamadas gratuitas a cargo de los usuarios.

Virus en el sistema. En el caso en que un virus infecta algún equipo de un servidor VoIP, el servicio telefónico puede quedar interrumpido. También pueden verse afectados otros equipos que estén conectados al sistema. Suplantaciones de ID y engaños especializados. Si uno no está bien protegido pueden sufrir fraudes por medio de suplantación de identidad.

11.5. BENEFICIOS

- Reducción en los gastos de telefonía.
- Enrutamiento de llamadas según destino y tarifa: Fijo, celular, Nextel, RPM, RPC, internacional.
- Asterisk "interopera" con sistemas de telefonía tradicional así como cualquier sistema de llamadas por Internet (telefonía IP).
- Costo cero en comunicación telefónica entre sucursales.
- Operadora automática (IVR)
- Cantidad ilimitada de anexos y usuarios
- Anexo extendido. Lleve consigo a cualquier parte del mundo, el numero de anexo de su oficina
- Transferencia de llamadas
- Contraseñas por Usuario
- Buzón de voz
- Correo de Voz integrado al correo electrónico
- IVR o Audio Respuesta con conectividad a Bases de Datos
- Identificación del llamante en pantalla
- Conferencias
- Música en espera configurable en diversos formatos

- Monitoreo y estadísticas de todas las llamadas: Números marcados, duración, destino, anexo desde donde se efectuó la llamada, grabación de llamadas, interceptación de llamadas ,etc.
- Acceso remoto al PBX a través de Internet
- Reportes detallado de Llamadas
- Call Center con sistemas de supervisión y estadísticas de colas
- Funcionalidad de Tarjeta Prepago y Postpago
- Lógica de extensiones flexible, con control de llamadas por perfiles
- Soporte a Fax e integración Fax / e-Mail

12. SERVIDOR DE ANTIVIRUS Y ANTISPAM

Un servidor de antivirus y antispam, conjuntamente con un servidor de correo forman un complemento ideal en cuanto a seguridad en el filtrado de correo entrante y saliente. Se puede instalar en el mismo servidor de correo o como Relay de éste.

12.1. FUNCIONALIDAD

- Escaneo de tráfico entrante y saliente.
- Escaneo por asunto, cuerpo y adjunto.
- Filtrado de contenido.
- Protección ante envío masivo de correo.
- Bloqueo de correo con direcciones predefinidas.
- Consulta en tiempo real de listas antispam.

12.2. BENEFICIOS.

- Ideal para medianas y grandes compañías.
- Filtro antispam.
- El filtro de contenido resuelve los problemas de seguridad de la información.
- Descarga automática de listas de virus.
- Configurable según necesidades.

CAPITULO III: Desarrollo e implementación del Proyecto

13. DEFINICION DE LA ESTRUCTURA DE LED.

La falta de una red que permita su administración total era una necesidad inmediata debido a que la infraestructura física y lógica era netamente empírica y hecha para red en el rango de 2 – 10 máquinas.

Para lograr una red balanceada, se empezó haciendo un estudio de cuanto ancho de banda (tráfico LAN) se usa en promedio cada día por cada máquina. Para ello se usó simplemente las estadísticas de la propia interfaz de red de cada máquina ya que hasta el momento no se encontraba centralizada por lo que no había la manera de analizarlo sin recurrir a verificar cada máquina.

El resultado en promedio daba entre 20 y 50 Mbps, generando hasta un 20% de pérdida de paquetes de datos debido a los cuellos de botella hacia el servidor web, servidor de archivos y hacia internet.

Los archivos compartidos que se encontraban en una máquina que hacía las veces de file server muchas veces se corrompían debido al acceso indiscriminado de lectura – escritura, por lo que se tuvo que realizar un script para que realice backup's cada una hora del mismo archivo, generando la reducción masiva de espacio en disco y por lo tanto disminuir su rendimiento de acceso lectura – escritura.

Ahora se empezará por implementar un servidor de autenticación para poder centralizar todos los usuarios y máquinas de red en un sólo directorio y que nos permita una mejor gestión de los mismos.

14. ADQUISICIÓN DE EQUIPOS PARA IMPLEMENTACION DE SERVICIOS

14.1. SERVIDOR DHCP, DNS, PROXY.

Para poder realizar la instalación de los servicios DHCP, DNS, PROXY se procedió a repotenciar el equipo que ya se encontraba presente, el POWER EDGE 3200. Se adquirió una tarjeta de red multiport gigabit ethernet de 5 puertos con lo que se ganó 5 puertos para poder realizar balanceo de carga en los diferentes servidores DNS, DHCP y PROXY. La ventaja de esta tarjeta es que posee su propio núcleo de gestión de datos por lo que no saturaría al procesador.

Se incrementó la capacidad de memoria RAM de 2GB a 16GB 4x4GB Dell PowerEdge 2850 PC2-3200 Memory ECC REG.

El procesador se mantiene ya que es un INTEL Xenon de hasta 2.66 GHZ de 4 núcleos.

14.2. SERVIDOR WEB Y FILE SERVER Y MENSAJERIA INSTANTANEA

Se utilizará el servidor IBM X3500 para implementar el servicio web donde estará alojada la página WEB corporativa así como la intranet y el file server donde se alojarán los archivos compartidos de la compañía.

Se adquirió un servidor de backups de archivos para los backups de la compañia. El modelo es el Iomega StorCenter ix4-200d 4TB (4 x 1TB) Network Storage Cloud Edition – 35436 cuya capacidad permite guardar los proyectos de multimedia que la empresa realiza a sus clientes así como los videos de vigilancia de las mismas oficinas.

Las capacidades de virtualización de este hardware permiten que se instale más de un sistema operativo reduciendo así el consumo energético y el espacio físico.

14.3. SERVIDOR DE AUTENTICACION OPENLDAP

Se adquirió un servidor IBM X3500 con capacidad de virtualización por hardware para poder realizar virtualización de discos RAID. Aquí se instalará el servidor de autenticación OPENLDAP.

14.4. SERVIDOR ASTERISK

Se adquirió un servidor IBM X3500 con capacidad de virtualización por hardware así como tarjetas DIGIUM para la implementación del servidor de telefonía IP Asterisk y el call center corporativo. Se tiene una conexión contratada con el proveedor ISP Claro para la salida a la PSTN que permita sacar las llamadas.

14.5. SWITCH CORE CENTRAL Y BALANCEADOR DE CARGA

Se adquirieron 04 switch's HP ProCurve serie 3000 de capacidades de 1Gbps para interconectar todas las estaciones, servidores, teléfonos y cámaras IP. Estos equipos son administrables y poseen la capacidad de formar VLAN's que serán útiles para la separación lógica de las redes evitando pérdidas por dominios de colisión y broadcast.

El balanceador de carga adquirido es un PepLink380 con capacidades gigabit para la interconexión de los router's de Claro y Movistar.

14.6. TELÉFONOS IP CISCO – AVAYA Y CÁMARAS IP.

Se adquirieron 30 teléfonos IP del proveedor CISCO para las diferentes áreas de la compañia, como las gerencias, jefaturas, almacén, informática y soporte técnico post-venta. Sólo las gerencias poseen la capacidad de videollamada para las comunicaciones con los diferentes clientes externos.

14.7. INFRAESTRUCTURA FÍSICA, CABLEADO Y RACKS.

El servicio de canalización, tendido, instalación y conexión de los diferentes puntos de red, así como la colocación de los racks, tablero eléctrico con puesta a tierra estuvo a cargo de terceros especializados en implementación de datacenters y conexiones de cableado estructurado.

15. INSTALACIÓN, Y TESTEO DE SERVIDORES

15.1. INSTALACION DEL SERVIDOR VIRTUAL EN POWEREDGE.

El servidor de PowerEdge se formateará para realizar una instalación limpia y poder configurar el servidor virtual Oracle VirtualBox donde se instalará el servidor DHCP, DNS y PROXY.

Se ha instalado el sistema operativo DEBIAN GNU/LINUX 6.0 sólo con componentes básicos, kernel y configuración de las interfaces de red.

Una vez instalado el sistema operativo básico, se procede a configurar las tarjetas e red:

##########################

auto eth0

iface eth0 inet static

address 10.1.1.1

netmask 255.255.255.0

gateway 10.1.1.2

#########################

auto eth1

iface eth1 inet static

address 172.16.1.1

netmask 255.255.255.0

#########################

auto eth2

iface eth2 inet static

address 10.1.1.1

netmask 255.255.255.224

#########################

auto eth3

iface eth3 inet static

address 10.1.3.1

netmask 255.255.255.0

Se ha configurado las 4 tarjetas de red del servidor DHCP, DNS,PROXY

15.2. INSTALACIÓN DEL SERVIDOR DHCP, DNS Y PROXY

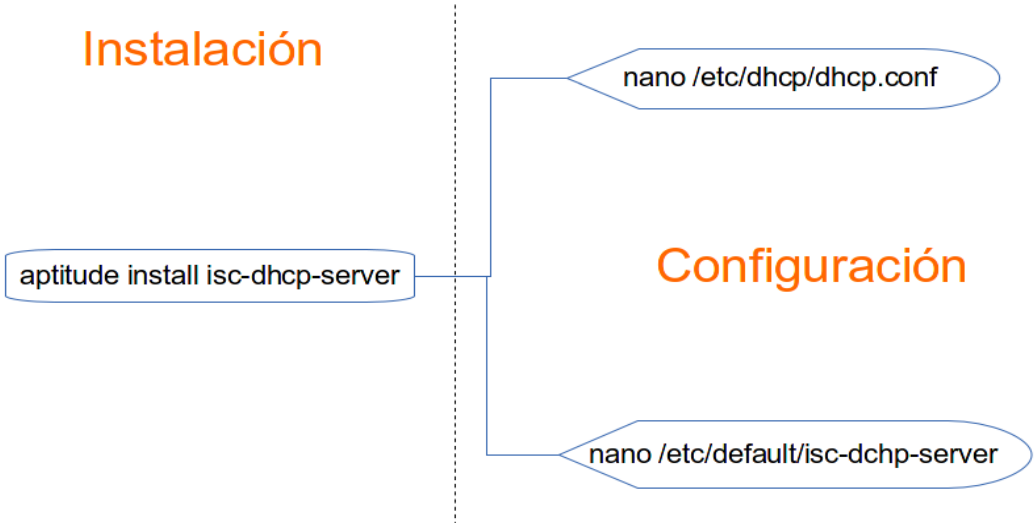
El servidor DHCP será instalado en el servidor DELL PowerEdge donde proveerá de IP's para la red LAN dentro del segmento 172.16.1.0/24.

El servidor será configurado para que junto al servidor DNS se actualice dinámicamente la tabla de resolución de nombres de máquina.

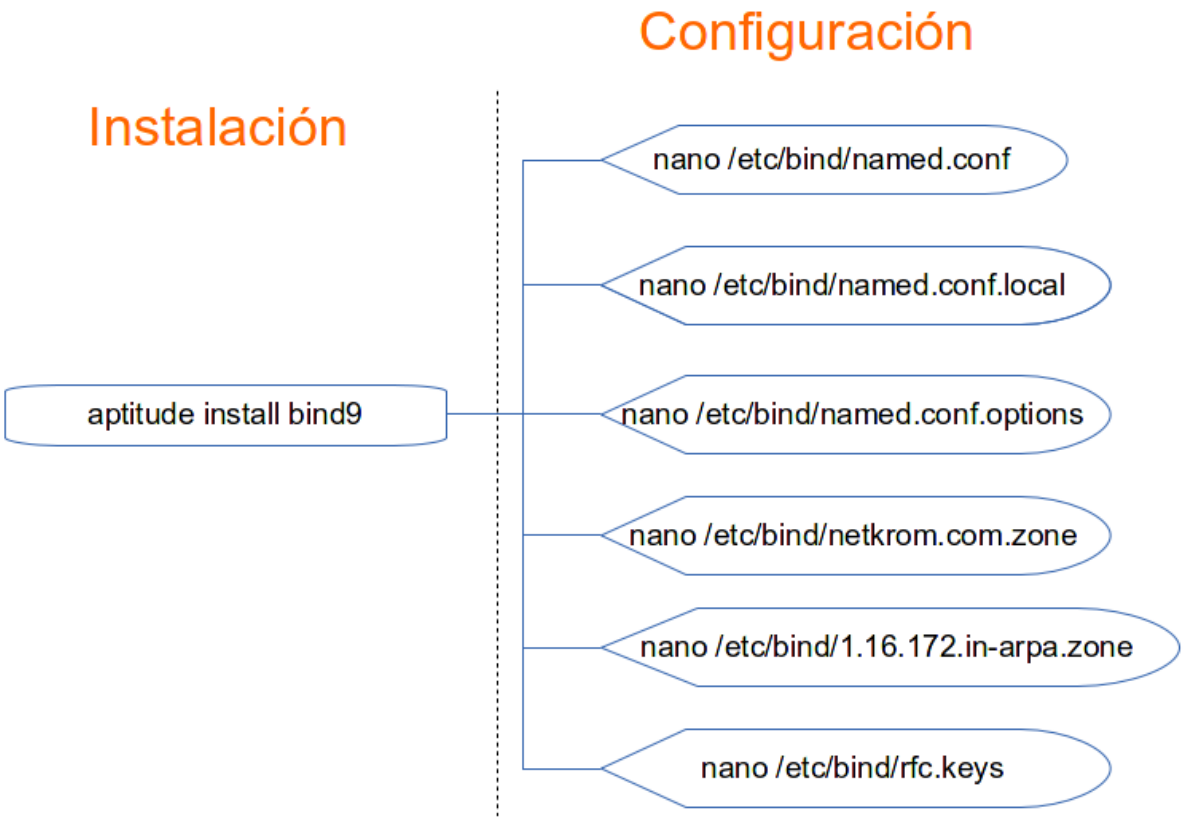
El servidor DHCP usado será el ISC-DHCP-SERVER cuya ventaja es la fácil configuración, abundante documentación disponible, soporte activo por parte del consorcio a cargo, software libre lo que implica cero gastos en licencias.

La versión estable disponible en los repositorios de debian 6.0 es 4.1.1-P1-15, con la actualización de seguridad +squeeze8. Este servicio forma parte de Internet Software Consortium's.

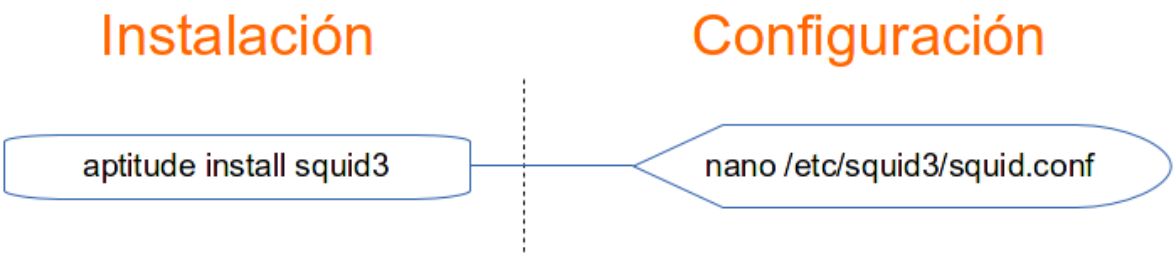
En el sgte diagrama se muestra los pasos para la instalación del servidor DHCP:



Luego procedemos a instalar y configurar el servidor DNS - BIND9, el cual sigue el sgte diagrama:



A continuación, la instalación del servidor proxy SQUID.

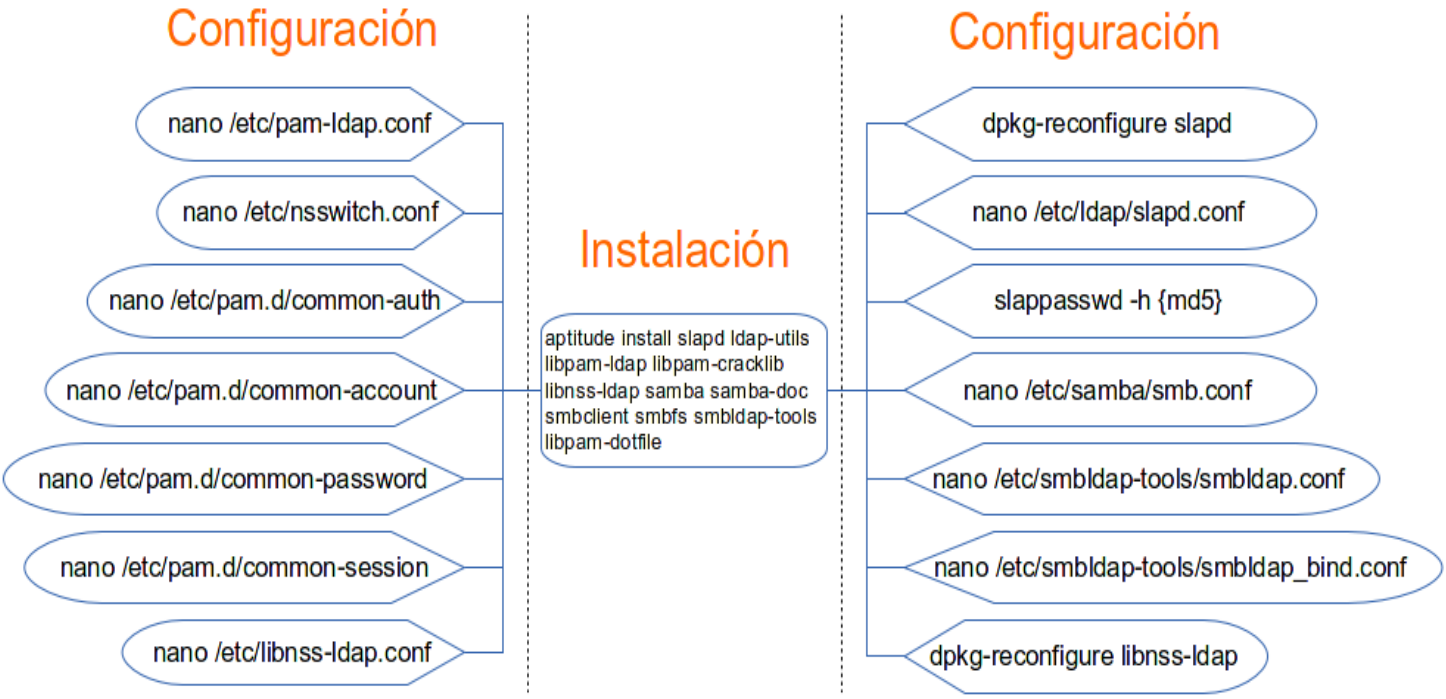


El servidor proxy se configura con autenticación hacia OpenLdap para que cada usuario con las credenciales correctas pueda navegar y así tener un mejor control.

15.3. INSTALACION DEL SERVIDOR OPENLDAP

La instalación de openldap se realizará en el servidor IBM X3500 instalado bajo Debian GNU/Linux 6.0. La dirección IP será 172.16.1.3

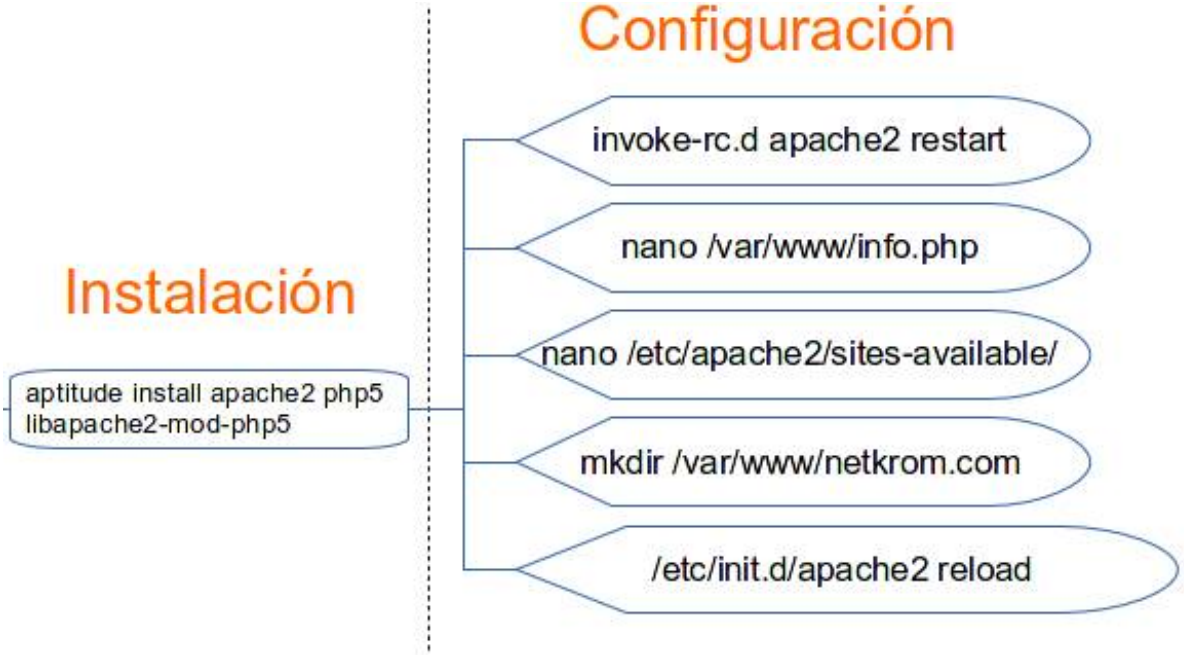
El sgte diagrama muestra los pasos para la instalación:



15.4. INSTALACION DEL SERVIDOR WEB,

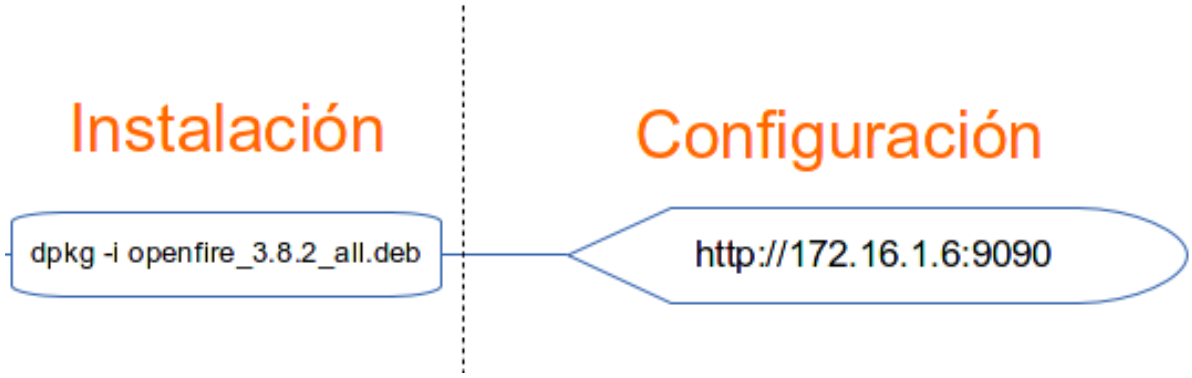
Para el servidor web se utilizará APACHE software, cuya cuota de mercado se mantiene por encima de IIS de Microsoft. Es robusto, modular, estable, de constante actividad de actualizaciones y parches de seguridad, además de ser software libre (bajo la licencia Apache Commons). La dirección IP será 172.16.1.5

La instalación sigue el sgte esquema:



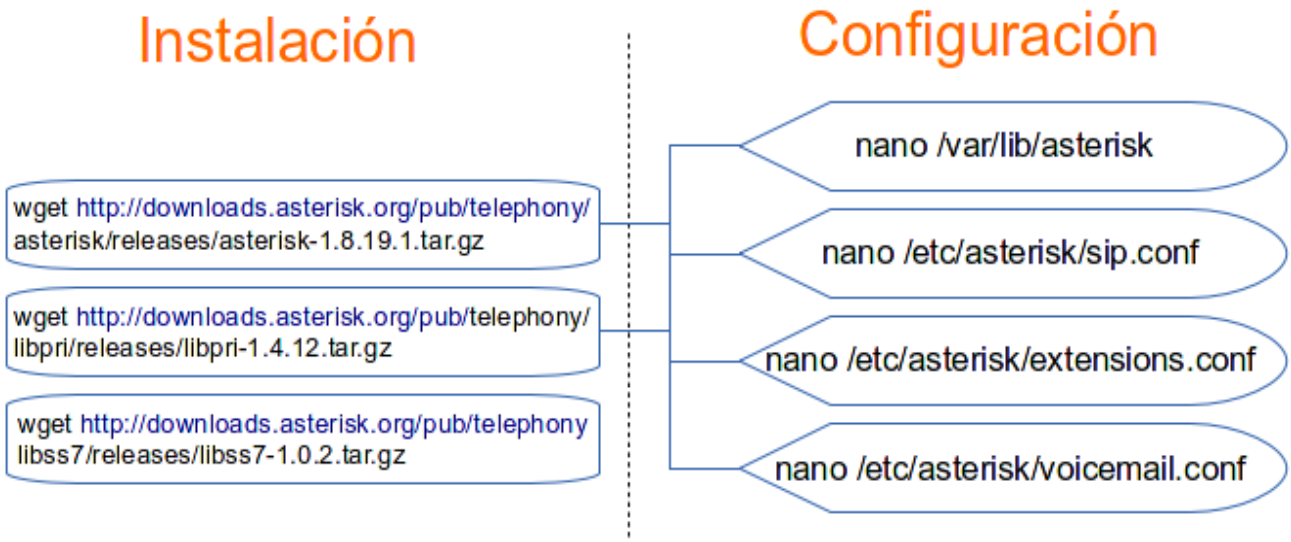
15.5. INSTALACION DEL SERVIDOR MENSAJERÍA INSTANTANEA

La mensajería instantánea se usará para mantener una red de chat interno para poder tener mayor respuesta en consulta entre áreas y sedes. La IP de este servidor será 172.16.1.6. Se usará el servidor OpenFire que permite autenticación con LDAP:



15.6. INSTALACION DEL SERVIDOR ASTERISK

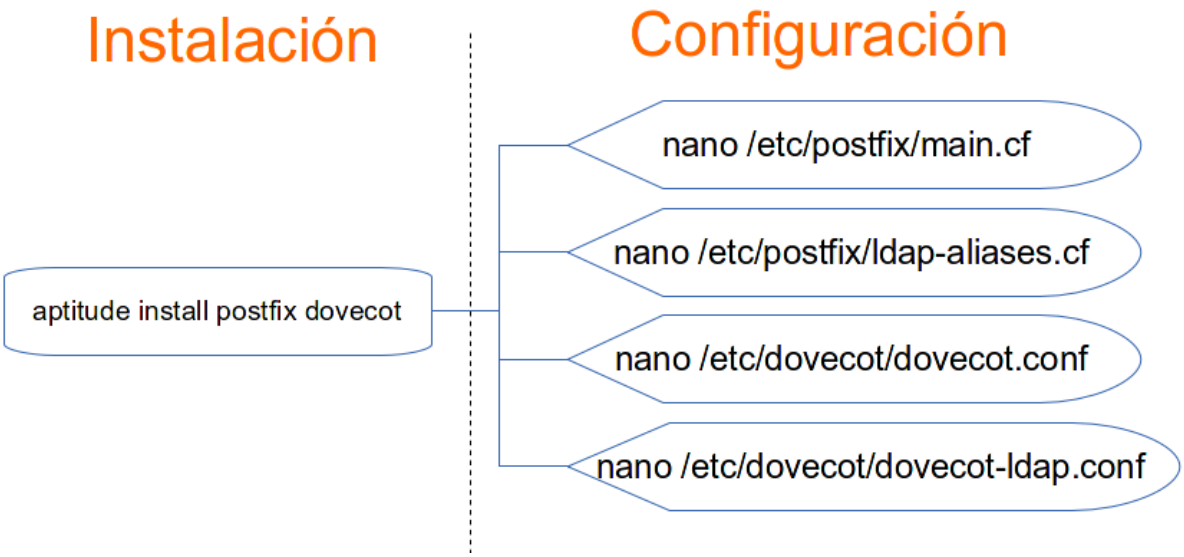
Se instalará sobre el servidor HP Proliant ML110G6 con tarjeta XFO Digium Wildcard AEX1600 8 puertos XFO.



15.7. SERVIDOR DE CORREO POSTFIX-DOVECOT

El servidor de correo usará el software libre POSTFIX, cuya hegemonía en el mercado de este tipo de servicios, su robustez y constantes actualizaciones con parches de seguridad lo hacen ideal para esta implementación. Dovecot es usado como servidor POP e IMAP. Postfix es el agente MTA – para SMTP.

El siguiente esquema muestra como es el proceso de instalación y configuración:



15.8. INSTALACION DEL SERVIDOR DE CÁMARAS.

Las cámaras son de tecnología IP con soporte de PoE. Se instalará en Windows Server 2003 Standar Edition el software de gestión PIXMA con licencia para gestión de 15 cámaras en simultáneo.

Las cámaras se encuentran en el segmento de red 192.168.10.0/24.

16. ANÁLISIS DE TRAFICO.

16.1. VELOCIDAD DE TRANSMISIÓN REQUERIDA PARA INTENET.

Se necesita proporcionarle acceso a Internet a 100 host que conforma la red LAN actual, por lo que es necesario realiza el cálculo del tráfico que se realiza. Sabiendo que cada usuario que acceda a Internet será limitado por las políticas implementadas en el servidor proxy y por servidor de autenticación openldap, se asume que un usuario puede acceder a 5 páginas web en promedio por hora y consumiendo un promedio de 712 KB por página web y adicionalmente a la página de la intranet, tenemos un throughput resultante por navegación web de:

$$Trp_{web} * usuario = \left(\frac{512\ KByte}{página}\right) * \left(\frac{8\ bits}{Byte}\right) * \left(\frac{6\ páginas}{3600\ seg}\right) = 6{,}76\ Kbps$$

$$Trp_{web} * total = 6{,}76\ Kbps * 100\ usuarios = 676\ Kbps$$

Además, considerando que un usuario puede leer 9 correos electrónicos por hora, cuyo tamaño máximo es de 50KB, entonces la tasa promedio de tráfico que genera el correo electrónico es de:

$$Trp_{correo} * usuario = \left(\frac{50\ KByte}{correo}\right) * \left(\frac{8\ bits}{Byte}\right) * \left(\frac{9\ correos}{3600\ seg}\right) = 1.00\ Kbps$$

$$Trp_{correo} * total = 1.00\ Kbps * 100\ usuarios = 100\ Kbps$$

Lo que nos permite calcular el throughput necesario para proveer del servicio de internet a todos los usuarios :

$$Trp_{total} = Trp_{web-total} + Trp_{correo-total} = 676\ Kbps$$

Esta velocidad calculada sería idealmente la que se debería contratar. Pero asumiendo un margen de trabajo del 50% correspondiente al factor de seguridad, la velocidad final sería:

$$Trp_{total} = 676\ Kbps * 1.5 = 1024\ Kbps = 1\ Mbps$$

16.2. DEMANDA TELEFONICA

Considerando las necesidades empresariales de Netkrom Technologies, se tiene que el sistema telefónico deberá gestionar 100 extensiones internas, con un tráfico considerable de 3 minutos entre los departamentos a la hora de mayor tráfico.

Se va a definir el tráfico telefónico en la hora más cargada con un índice de pérdidas del 1%.

Tráfico ofrecido: 100 extensiones

Tiempo promedio de cada llamada: 3 min.

Cantidad de llamadas cursas con 1% de pérdidas. 100/1.01 = 99 llamadas.

$$A = C_A + t_m$$

$$A = \frac{99\,llamadas}{hora} * \frac{3\,minutos}{llamada} * \frac{1\,hora}{60\,minutos} = 5\,Erlangs$$

*Erlangs= El Erlang es una unidad adimensional utilizada en telefonía como una medida estadística del volumen de tráfico.

Con el valor de 5 Erlangs y una probabilidad de bloqueo del 1%, según la tabla Erlang B detalla en los anexos, obtenemos 11 líneas para satisfacer el tráfico interno, además de 10 líneas directas. Por lo tanto se necesitarán 21 pares telefónicos.

16.2.1. Selección del códec a utilizar.

Para determinar el códec de voz a utilizar se determinara la velocidad de transmisión que genera cada uno de ellos, Para lo cual se deberá considerar la cantidad de conversaciones simultáneas que se generarán en el sistema.

Si tomamos en cuenta que se deberá solicitar 21 pares telefónicos la central telefónica deberá manejar el mismo número de llamadas simultáneas en el peor de los casos, lo que nos permite determinar la velocidad de transmisión mínima que deberá soportar la red LAN corporativa.

Velocidad de transmisión códec G711

Para el cálculo de la velocidad de transmisión se tomaran en cuenta el bit rate del códec G711 y 21 llamadas simultáneas que se deberán cursar en un solo sentido sería:

Velocidad de transmisión = (Payload + L3 + L2) * 8 * pps

Donde se tiene:

Payload: En bytes generado por el códec.

L3: Cabeceras de capa 3 y de capas superiores en bytes.

L2: Cabecera de capa de enlace en bytes.

8: Números de bits por byte.

pps: Tasa de paquetes por segundo generado por el códec (pps = bit rate códec / payload (bits)).

Reemplazando los enunciados por los datos tenemos para G711:

Payload = 160 bytes

L3 = 40 bytes [IP (20 bytes) / UDP (8 bytes) / RTP (12 bytes)]

L2 = 14 bytes Ethernet

pps = 50

$$Velocidad\ de\ Tx = 160 + 40 + 14 * 8 * 50 = 85.6\ Kbps$$

Este valor multiplicado por el número de llamadas simultáneas y en sentido full dúplex nos dará como resultado la velocidad de transmisión mínima que deberá soportar la red LAN corporativa.

$$Velocidad\ de\ Tx\ total = 85.6\ Kbps * 2 * 21 = 3.6\ Mbps$$

Velocidad de transmisión códec G729

Para el cálculo de la velocidad de transmisión se tomaran en cuenta el bit rate del códec G729 y 21 llamadas simultáneas que se deberán cursar en un solo sentido lo que determina:

Velocidad de transmisión = (Payload + L3 + L2) * 8 * pps

Payload = 20 bytes

L3 = 40 bytes [IP (20 bytes) / UDP (8 bytes) / RTP (12 bytes)]

L2 = 14 bytes Ethernet

pps = 50

Velocidad de transmisión = (20 + 40 + 14)*8*50 = 29.6 kbps

Este valor multiplicado por el número de llamadas simultáneas y en sentido full dúplex dará como resultado la velocidad de transmisión mínima que deberá soportar la red LAN corporativa:

$$Velocidad\ de\ Tx\ total = 29.6\ Kbps * 2 * 21 = 1.2\ Mbps$$

Entonces comparando los codec's, se usará el G729, además de no tener restricciones de licencia ya que es libre.

16.3.

17. DIMENSIONAMIENTO DE HARDWARE PARA LA RED CORPORATIVA

Los servidores que mantendrán los servicios habilitados como correo web, correo, autenticación, file server y Asterisk se detallan a continuación:

04 unidades del HP Proliant DL160 que alojarán los servicios web, correo, LDAP-SAMBA y Base de Datos SQL SERVER sobre Windows Server 2008.

Carácterísticas	Hp Proliant DL 160
Procesador	2 Xeon X5650 2.66Ghz
Discos Duros	3x500 7.2Krpm 3.5"
Memoria RAM	24 Gb 1333 Mhz
Puertos Pc express	4
Hardware Raid	P410 Smart Array
Puertos RJ-45 10/100/1000	2p 10/100/1000
Unidad óptica DVD Rw	DVD RW
Tarjeta de Video	Si
Puertos Usb	4
Puertos PS2 mouse	No
Puertos PS2 teclado	No
Soporte Linux	Si
Fuente redundante	Si 500 Watts
Garantía 1 año o más	3 años

HP Proliant ML110G6 con tarjeta XFO Digium Wildcard AEX1600 8 puertos XFO para el servidor Asterisk con cancelador de eco en software OSLEC.

Technical Specifications	
Expansion slots	
Expansion slots	5
Memory	
Memory type	PC3-10600E-9
Memory, maximum	48 GB
Memory, Installed	16 GB
Memory slots	12 DIMM slots
Memory protection features	Advanced ECC
Cache	4MB L3
Networking	
Network controller	(1) 1GbE NC107i 2 Ports
Power	
Power supply type	(1) 460 Watt non-hot plug
Processor	
Processor core available	4
Processor	Intel® Xeon® E5504 (4 core, 2.00 GHz, 4MB L3, 80W)
Processor	Intel® Xeon® E5504 (2.00 GHz, 4MB L3, 80W, DDR3-800)
Processor speed	2.00 GHz
Number of processors	1
Storage	
Included hard drives	(1) Hardrives (1) 250 GB
Optical drive type	Half-Height SATA DVD-ROM
Supported drives	Hot plug 3.5-inch SAS; Hot plug 3.5-inch SATA; Non-hot plug 3.5-inch SAS; Non-hot plug 3.5-inch SATA
Storage controller	Smart Array B110i SATA RAID
Internal mass storage	SATA: 4.0 TB

Los teléfonos SIP deben poseer las siguientes características:

Características técnicas	
Conectividad	Lan RJ-45 categoría 5e o superior
	Wan RJ-45 categoría 5e o superior
	PoE IEEE 802.3af class 1 o superior
Características de Voz	
Protocolos	G.711u/A, GSM, G.726, G.729AB
DTMF	In-band, out-of band (RFC2833) and SIP INFO
Características de red	
Protocolos	SIP v1 (RFC2543), v2 (RFC3261)
	IEEE 802.1p/q etiquetamiento (VLAN), Layer 3ToS
	NAT Traversal STUN mode
Asignamiento IP	Estático/DHCP
Router / switch	Estático/DHCP
Interface Administración	Web, telnet

El teléfono Grandstream GX285 cumple con la relación precio / características.

Como switch con capacidad de VLAN's, se tienen 5 HP ProCurve 2610 con 48 puertos Gigabit ethernet y con capacidad PoE.

HP PROCURVE SWITCH 2910AL-48G - CONMUTADOR - 48 PUERTOS - EN, FAST EN, GIGABIT EN - 10BASE-T, 100BASE-TX, 1000BASE-T + 4 X SFP COMPARTIDO (VACÍAS) - 1U - APILABLE

HP ProCurve Switch 2910al-48G - conmutador - 48 puertos

- Tipo de dispositivo: Conmutador - apilable

- Factor de forma: Externo - 1U

- Dimensiones (Ancho x Profundidad x Altura): 44.3 cm x 36.6 cm x 4.4 cm

- Procesador: 2 x ARM ARM1156T2-S 515 MHz

- Memoria RAM: 512 MB SDRAM

- Memoria Flash: 4 MB

- Cantidad de puertos: 48 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T

- Velocidad de transferencia de datos: 1 Gbps

- Protocolo de interconexión de datos: Ethernet, Fast Ethernet, Gigabit Ethernet

- Ranuras vacías: 4 x SFP compartido (mini-GBIC)

- Protocolo de gestión remota: SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, http

- Características: Control de flujo, soporte de DHCP, soporte BOOTP, soporte ARP, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), copia de puertos, activable, soporte IPv6, Quality of Service (QoS)

- Cumplimiento de normas: IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s

- Alimentación: CA 120/230 V (50/60 Hz) y capacidad PoE

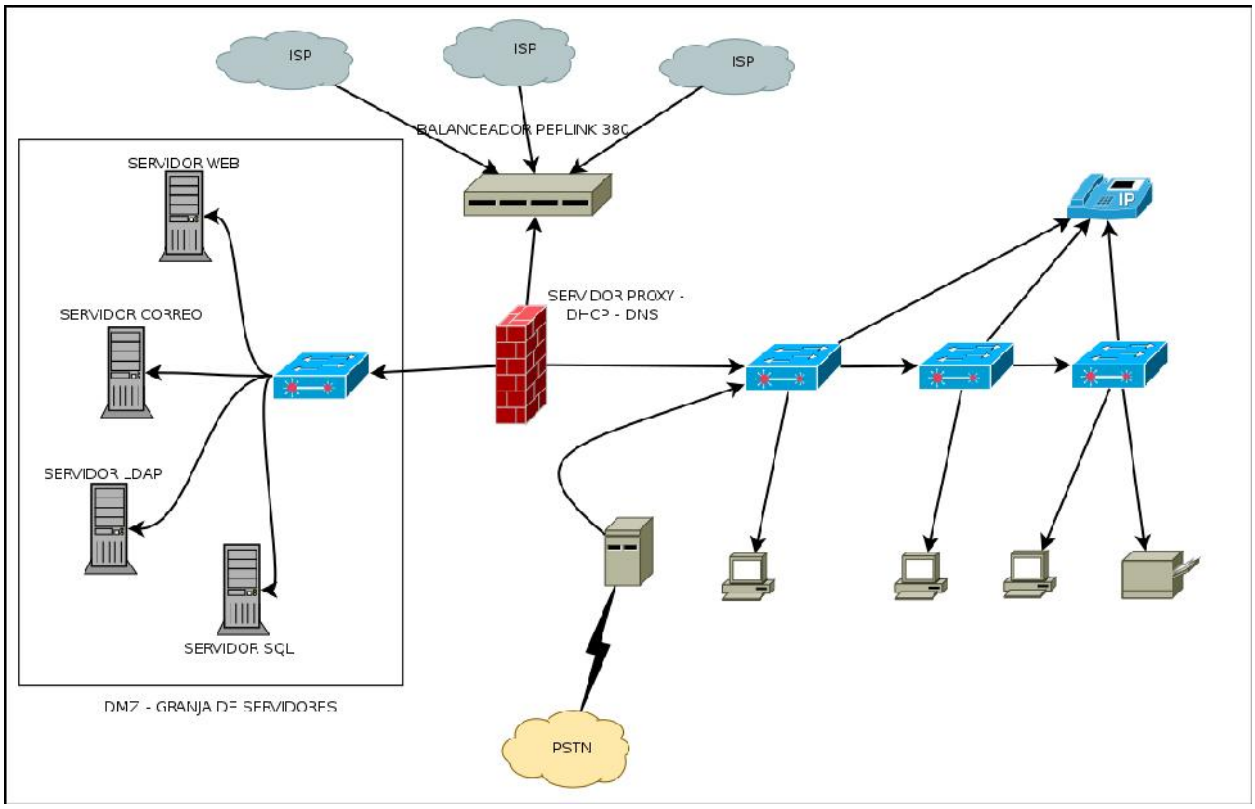
- Garantía del fabricante: Garantía limitada de por vida

- Balanceador Peplink 380 con capacidad de hasta 3 entradas de servicio ISP para poder disponer de redundancia y contingencias ante alguna falla de los servicios.

18. RESUMEN DE COSTOS DE EQUIPOS Y EQUIPAMENTO.

DENOMINACIÓN	CANTIDAD	COSTO UNITARIO	COSTO PARCIAL (SIN IGV)	COSTO TOTAL
HP PROLIANT DL 160	02	$1,500.00	$3,000.00	$3,540.00
HP PROLIANT ML110-G6	01	$1,107.00	$1,107.00	$1,306.26
TARJETA DIGIUM AEX1600	01	$100.00	$100.00	$118.00
TELEFONOS SIP GRANDSTREAM	20	$60.00	$1,200.00	$1,416.00
SWITCH HP V1910-48G	01	$800.00	$800.00	$944.00
BALANCEADOR DE CARGA PEPLINK	01	$500.00	$500.00	$590.00
CABLE UTP CAT. 6 (BOBINAS – 305m)	03	$150.00	$450.00	$531.00
CONECTORES, HERRAMIENTAS	01	$100.00	$100.00	$118.00
			COSTO TOTAL DE EQUIPOS SIN IGV	***$7,257.00***
			COSTO TOTAL DE EQUIPOS CON IGV	***$8,563.26***

19. TOPOLOGIA LOGICA PROPUESTA.



20. CONCLUSIONES Y RECOMENDACIONES

20.1. CONCLUSIONES

Como resultado de la finalización del presente Proyecto de Titulación se concluye:

Al analizar la estructura informática y de telecomunicaciones existente en Netkrom, se determinó las debilidades, vulnerabilidades y necesidades a cumplir para poder implementar una red LAN y Telefonía basada en software libre, evitando así licencias corporativas y por ende el costo de éstas.

Se describió las características, categorías y funcionamiento de las redes LAN para transmitir voz y datos utilizando la misma infraestructura, permitiendo determinar las modificaciones necesarias que se deben realizar en la red LAN para poder transmitir voz y datos utilizando la infraestructura existente en la compañía.

Al estudiar y analizar el estado actual de la red LAN permitió determinar las modificaciones tanto en su topología lógica como física, dando como resultado la necesidad de aumentar puntos de red en áreas en las cuales la red no tiene presencia y que son de suma importancia, además de determina la velocidad de transmisión necesaria para poder brindar el servicio de Internet al 100% de equipos existentes en todas las áreas de la compañía.

Con la realización de nuestro Proyecto de Titulación y el rediseño de la red LAN permitirá mejorar el rendimiento de la misma de manera que pueda soportar sin problemas el trafico adicional que se originará por la implementación del sistema telefónico, además de ofrecer nuevos servicios al administrador de red como son el monitoreo en tiempo real de lo que sucede en la red, el control de contenidos a los que pueden acceder los usuarios, la prevención de intrusos al utilizar como puerta de entrada el sistema Proxy, la implementación de un sistema de correo interno que permitirá agilitar los tramites tanto internos como externos de la compañía, además de mejorar la seguridad de la red con la implementación de Zonas Desmilitarizadas (DMZ).

20.2. RECOMENDACIONES

Se recomienda crear puntos de redundancia de red en gerencias, siendo estos indispensables, ya que el corazón de la compañía recae sobre la administración de la misma a cargo de sus altos mandos,

Se recomienda que por lo menos haya una impresora conectada a la red por área, dado que en la mayoría de casos deben acudir a los compañeros o incluso a otras áreas para realizar impresiones de informes, análisis, reportes y no una impresora compartida por toda la compañía.

Se recomienda la re-estructuración de escritorios y mueblería existentes en oficinas pequeñas, en algunas de ellas hay incomodidad para la atención a los usuarios internos y externo, en otras se da la espalda a las personas que ingresan, en el diseño arquitectónico se debe interactuar con el entorno, punto que vagamente ha sido tomado en cuenta, los escritorios deberían estar de frente a las puertas de cada oficina para de esa manera recibir a quienes ingresan, especialmente refiriéndose a oficinas,

Se deben implementar políticas de acceso al departamento de redes ya que los equipos y la información que se maneja es muy sensible y no debe estar al alcance de los colaboradores de la compañía.

Se debe implementar políticas de acceso restringido a sitios web no acorde con los intereses de la compañía. Estas políticas se definirán en el servidor Proxy para poder realizar un uso eficiente de la velocidad de servicio contratadas.

Se recomienda contar con un sistema autónomo de energía eléctrica a toda la compañía, ya que actualmente se alimenta del servicio de energía comercial.

21. BIBLIOGRAFÍA.

I. CALDERÓN, Ana y PAREDES, María. “DISEÑO DE UNA RED VOIP, UTILIZANDO EL SISTEMA OPERATIVO LINUX, PARA SU IMPLEMENTACIÓN SOBRE LA INFRAESTRUCTURA EXISTENTE DEL ECORAE; PARA BRINDAR TELEFONÍA A ZONAS RURALES ESPECÍFICAS DE LA AMAZONÍA ECUATORIANA” , Tesis EPN Septiembre del 2006.

II. SOLANO POZO, Diego Vinicio. “Estudio y diseño de una red de voz y datos para la Unidad Educativa Municipal Quitumbe utilizando la tecnología Gigabit Ethernet para soportar servicios en tiempo real de VoIP, videoseguridad y videoconferencia”, Tesis EPN Junio del 2009.

III. LOZA, Christian y ORDÓÑEZ, Francisco. “Estudio y diseño de una red privada virtual para brindar el servicio de VOIP, administrado bajo el sistema operativo Linux”. Tesis EPN Octubre del 2008

IV. CASTILLO, Richard y MENDOZA, Carlos “Estudio de "Differentiated Services (Diffserv)" usando el sistema operativo abierto (Linux) para la provisión de calidad de servicio en redes con VoIP”. Tesis EPN marzo del 2007

V. STALLINGS, William. “Comunicaciones y redes de computadoras”, Editorial Prentice-Hall Hispanoamericana, Sexta edición , 740p

VI. TANENBAUM, Andrew. “Redes de Computadoras” Editorial Prentice-Hall Hispanoamericana, Tercera edición,1997 795p

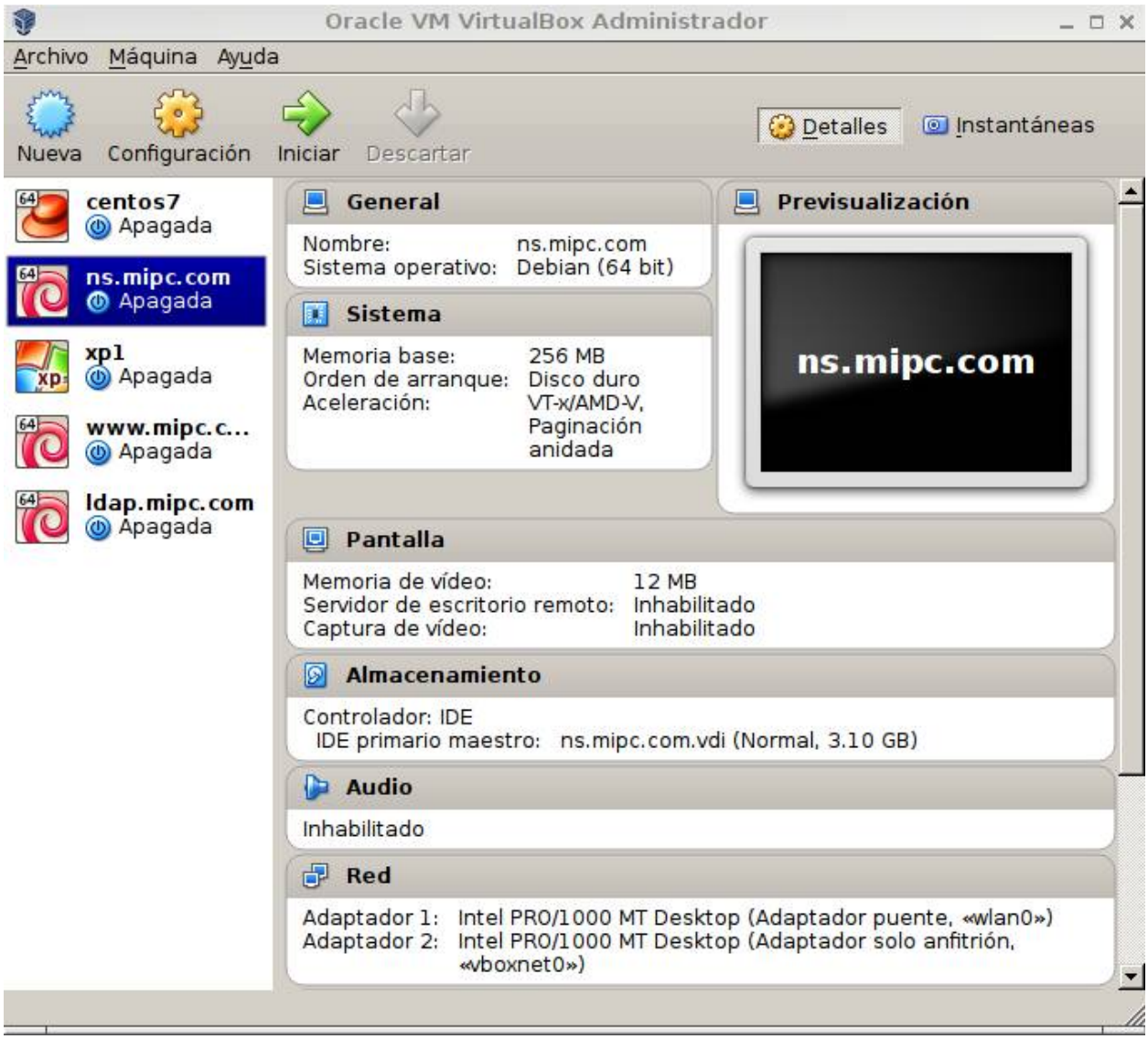
VII. CARRIÓN ROBALINO, Hugo “Ingeniería de Tráfico de Telecomunicaciones”, Carrión&Carrión Consultores, Noviembre del 2006.

VIII. OLALLA Aleix, “Estudio y Diseño para la migración de una red de telefonía tradicional a una red de telefonía IP para una entidad comercial”, Quito, Enero 2002.

ANEXOS

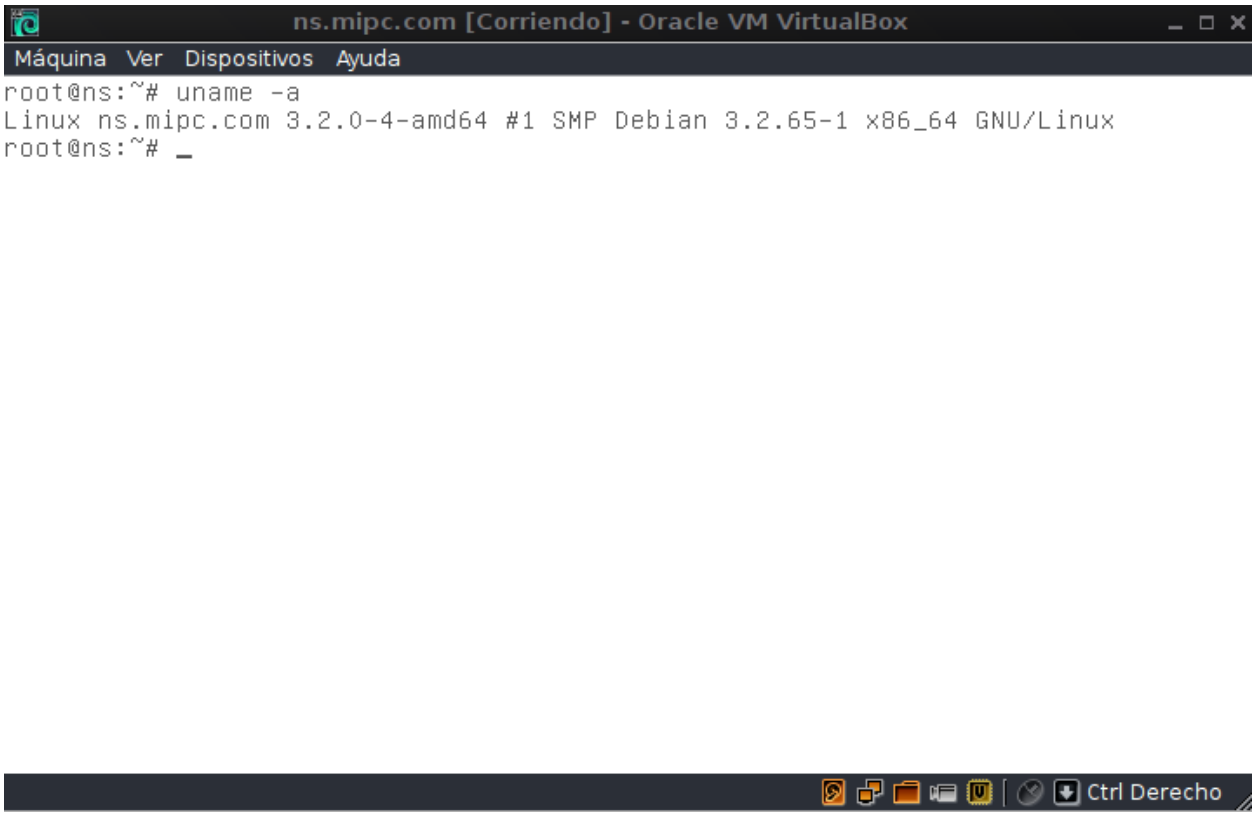
ANEXO 01

ENTORNO DE SIMULACION CON VIRTUALBOX



ANEXO 02

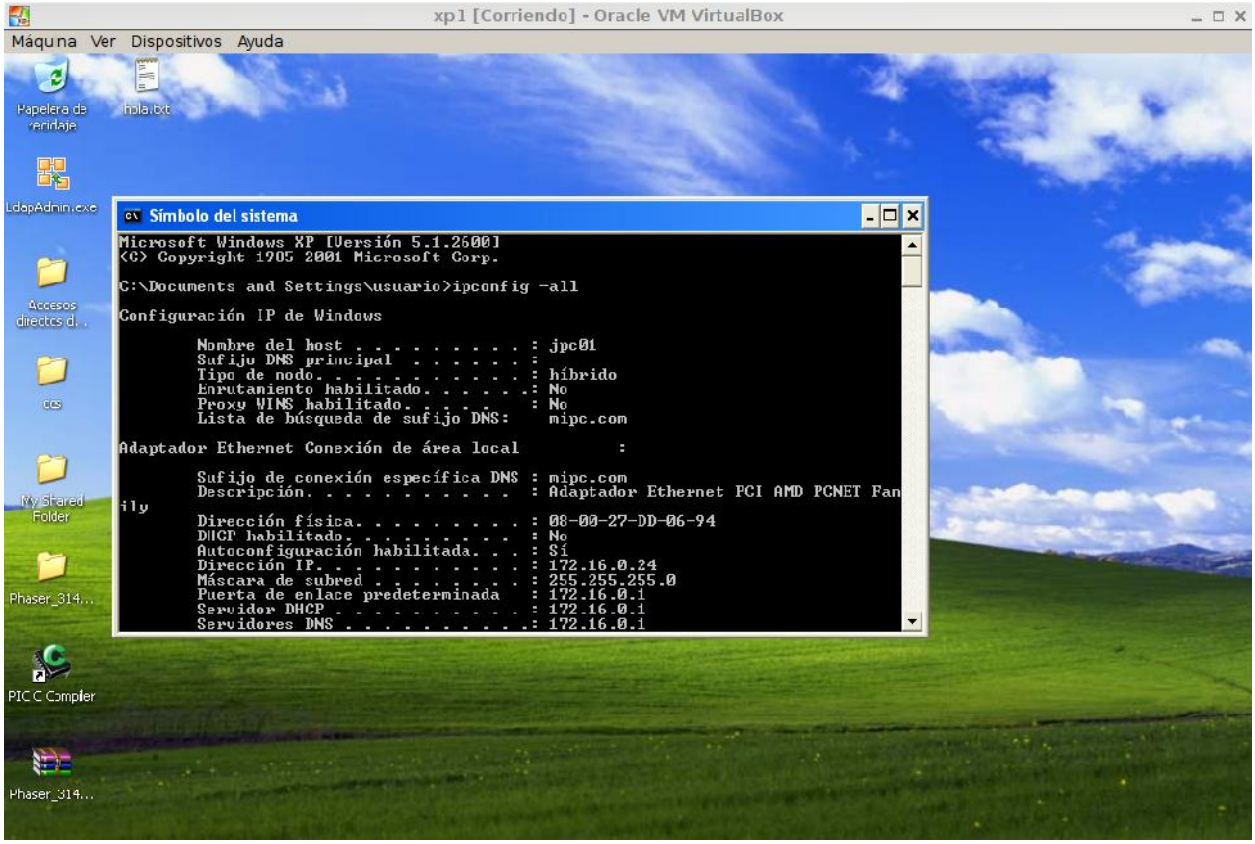
SIMULACION SERVIDOR DHCP – DNS- PROXY – FIREWALL CON DOMINIO MIPC.COM Y NOMBRE DE HOST: NS.MIPC.COM



ANEXO 03

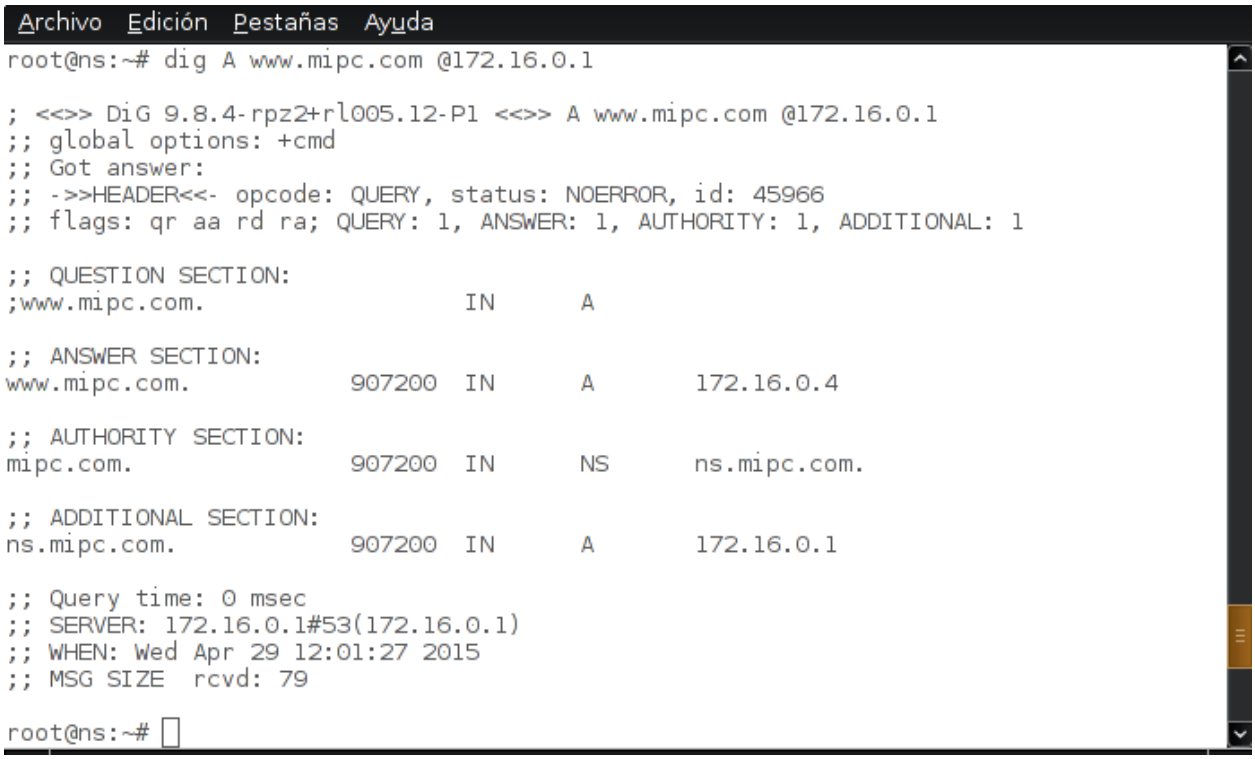
SIMULACION SERVIDOR DHCP – DNS EN ACCION CON MAQUINA WINDOWS XP INGRESADA AL DOMINIO MIPC.COM

```
root@ns:~# tail -f /var/log/syslog
Apr 29 11:45:08 ns dhcpd: All rights reserved.
Apr 29 11:45:08 ns dhcpd: For info, please visit https://www.isc.org/software/dhcp/
Apr 29 11:45:08 ns dhcpd: Wrote 0 deleted host decls to leases file.
Apr 29 11:45:08 ns dhcpd: Wrote 0 new dynamic host decls to leases file.
Apr 29 11:45:08 ns dhcpd: Wrote 3 leases to leases file.
Apr 29 11:45:09 ns squid[2060]: Squid Parent: child process 2064 started
Apr 29 11:45:16 ns kernel: [   12.705039] eth0: no IPv6 routers present
Apr 29 11:45:17 ns kernel: [   13.080325] ip_tables: (C) 2000-2006 Netfilter Core Team
Apr 29 11:45:17 ns kernel: [   13.232344] eth1: no IPv6 routers present
Apr 29 11:45:18 ns kernel: [   14.369739] nf_conntrack version 0.5.0 (1959 buckets, 7836 max)
Apr 29 11:52:24 ns dhcpd: DHCPDISCOVER from 08:00:27:dd:06:94 via eth1
Apr 29 11:52:25 ns dhcpd: DHCPOFFER on 172.16.0.24 to 08:00:27:dd:06:94 (jpc01) via eth1
Apr 29 11:52:25 ns named[1973]: client 172.16.0.1#57102: updating zone 'mipc.com/IN': update unsuccessful: jpc01.mipc.com: 'nar
(YXDOMAIN)
Apr 29 11:52:25 ns dhcpd: DHCPREQUEST for 172.16.0.24 (172.16.0.1) from 08:00:27:dd:06:94 (jpc01) via eth1
Apr 29 11:52:25 ns dhcpd: DHCPACK on 172.16.0.24 to 08:00:27:dd:06:94 (jpc01) via eth1
Apr 29 11:52:25 ns named[1973]: client 172.16.0.1#57102: updating zone 'mipc.com/IN': update unsuccessful: jpc01.mipc.com/TXT:
```



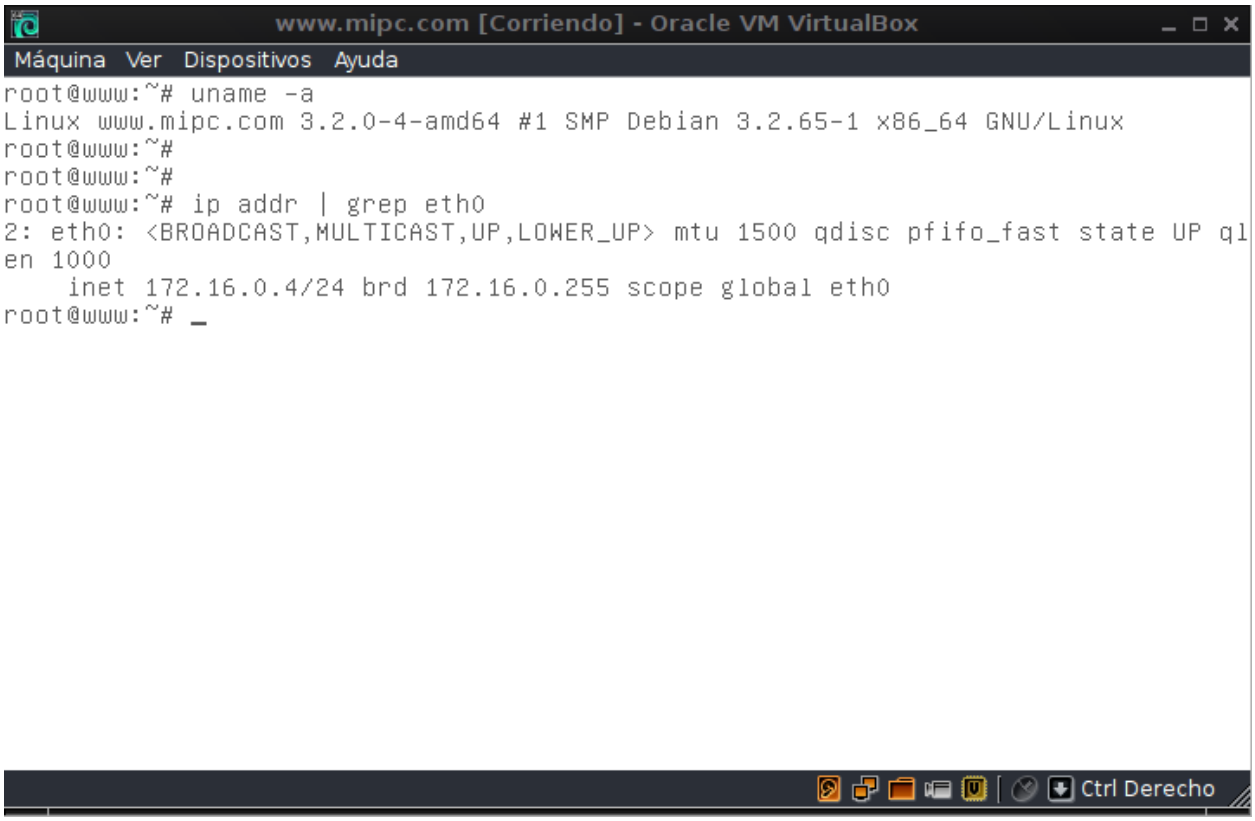
ANEXO 04

SERVIDOR DNS RESOLVIENDO NOMBRE LOCALMENTE AL SERVIDOR WEB LOCAL



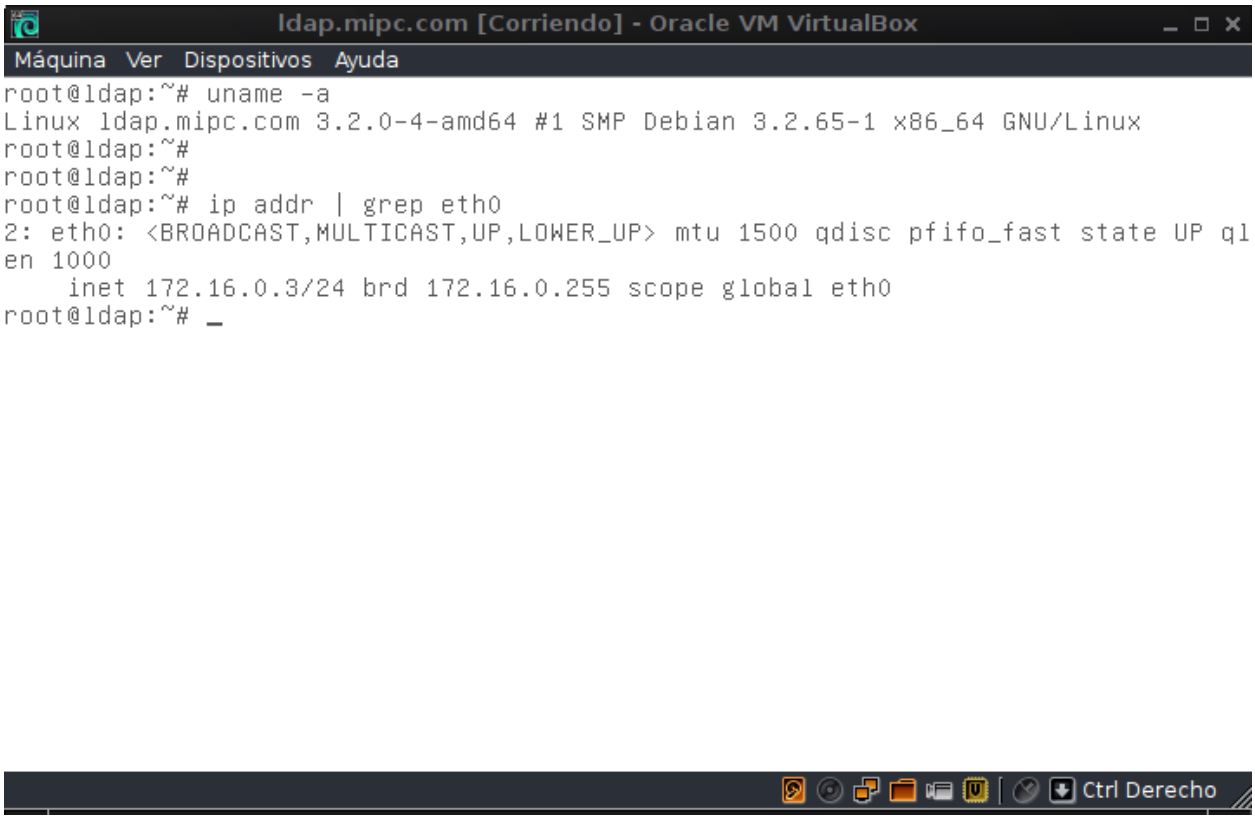
ANEXO 05

SIMULACION SERVIDOR WEB APACHE CON PHP CON NOMBRE DE HOST: WWW.MIPC.COM – IP: 172.16.0.4



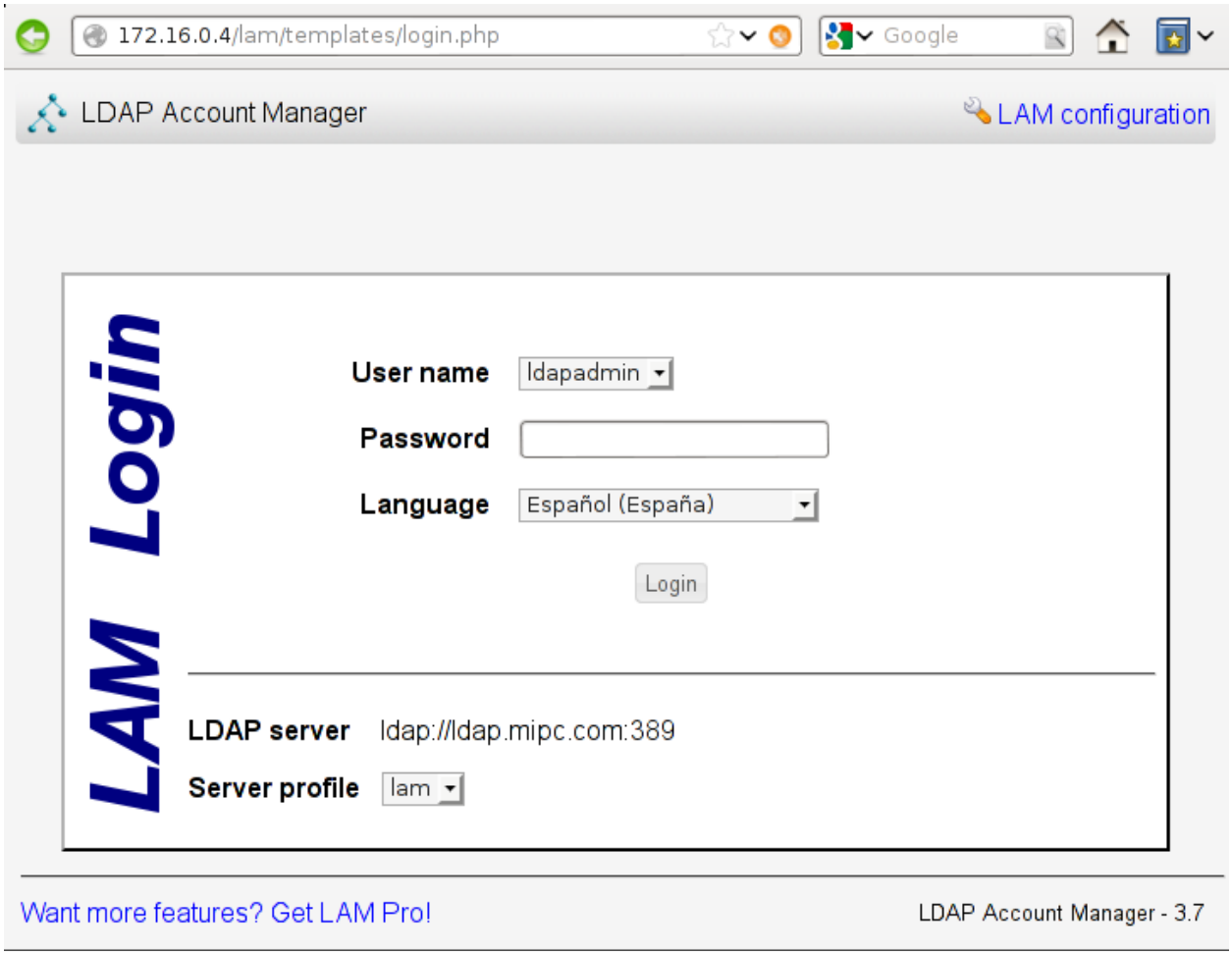
ANEXO 06

SERVIDOR DE AUTENTICACIÓN OPENLAP CON BACKEND SAMBA. NOMRE DE HOST. LDAP.MIPC.COM – IP: 172.16.0.3



ANEXO 07

ADMINISTRADOR DE DIRECTORIO LDAP INSTALADO EN SERVIDOR WEB – LDAP-ACCOUNT-MANAGER



ANEXO 08

ENTORNO DE ADMINISTRACIÓN LDAP-ACCOUNT-MANAGER